The Physical Computer and the Fourth Amendment

Josh Goldfoot*

INTRODUCTION

Computers can be evidence. Consequently, criminal investigators often need to seize computers and examine them. Computer forensic examination is now a common tool in all types of criminal investigations. The FBI, alone, has more than two hundred full-time computer forensic examiners.[1] Yet, computer forensic examination poses a recurring Fourth Amendment problem. Computer storage media can reveal facts relevant to an investigation, but they can also reveal irrelevant facts that can be embarrassing or inform investigators for the first time about a new crime.

To reveal the relevant while shielding the irrelevant, most courts employ a special fact perspective—that is, a special way to characterize the operative facts. They conceive of storage media as containers of subcontainers, with each subcontainer corresponding to a directory, a file, or something smaller. From this "subcontainer perspective," existing search and seizure law governs forensic

*J.D., University of Virginia, 1999; B.A., Yale University, 1996; Senior Counsel, Computer Crime and Intellectual Property Section, U.S. Department of Justice, 2005-present. All views expressed in this article are my own, and are not necessarily those of the Department of Justice or the United States Government. I wish to thank Matthew Berry, Howard Cox, Jenny Ellickson, Orin Kerr, and Paul Ohm for helpful comments on this article.

[1] *See* U.S. DEP'T OF JUSTICE, THE NATIONAL STRATEGY FOR CHILD EXPLOITATION PREVENTION AND INTERDICTION (2010), http://www.projectsafechildhood.gov/docs/natstrategyreport.pdf.

examination in the same way it governs an officer searching a home. Each subcontainer is a separate "thing" under the Fourth Amendment. The Fourth Amendment limits an examiner's authority to seize that subcontainer in the same way it limits an officer's authority to seize a murder weapon from a home.

The subcontainer perspective transforms search and seizure law. Search and seizure law is heavily premised on physical facts: it governs what places officers can enter and what things they can seize, but not what information they may learn. The subcontainer perspective rejects that premise. Rejecting that premise causes search and seizure rules to cease to make sense. Some physical rules cannot be applied to information at all, others might apply in multiple contradictory ways, and others, when applied, counter-intuitively produce results that barely restrict forensic examination at all. Out of the resulting mess, many have called for departures from search and seizure law, such as requiring magistrate judges to approve how a computer will be "searched" or abolishing plain view. Far from permitting a straightforward application of old law to new facts, the subcontainer perspective leads to the invention of new rules, based on new policy choices.

Rather than use the subcontainer perspective, a better choice is to adopt a perspective, similar to one that the California Supreme Court recently used, that views storage media as physical evidence.[2] Under this perspective, a hard drive is an object, not a place. It does not contain things; it is one thing. Like any other physical evidence, it is examined, not "searched." So long as a storage medium is lawfully seized, the Fourth Amendment does not restrict forensic examination. Just as the Fourth Amendment does not govern the work of the technician analyzing seized blood stains, developing film, or testing suspected drugs, it also does not govern the work of the technician analyzing a lawfully seized hard drive.

Part I discusses how the subcontainer perspective tries to apply physical search and seizure rules to a conceptualized virtual world. That requires "translating" the physical rules to the virtual world. Hence, physical concepts, such as "place," "thing," "search," and "seize" operate only metaphorically. Those metaphors are unclear; it is difficult to agree, for example, on where the subcontainers begin and end. When viewed through those metaphors, some established Fourth Amendment rules can seem to no longer make sense. If taken

[2] *See* People v. Diaz, 244 P.3d 501, 509 (Cal. 2011).

seriously, the subcontainer perspective might fatally cripple computer forensics. Rather than do that, courts have made compromises. Because of those compromises, officers can still look at all data on a storage medium, and, with slam-dunk additional warrants, use any data as evidence. Recognizing this problem, some judges and commentators have sought to fashion special rules for computers.

Part II argues that the physical perspective results in the most faithful application of search and seizure law to computer forensics. Computer storage media are physical evidence. Computers record data by physically changing storage media—magnetizing hard drive regions, for example. Computer forensics thus fits easily into established rules governing the forensic examination of lawfully seized objects, such as drugs, blood, or clothing. Specifically, Fourth Amendment law permits law enforcement to examine lawfully seized objects forensically. The same rule should apply for computer storage media.

Part III considers perhaps the strongest argument for the subcontainer perspective: public policy arguments against routinely authorizing officers to examine entire hard drives based on probable cause to believe that some small part of them is relevant. These arguments call for special treatment for storage media, but storage media does not deserve that treatment. While storage media do store lots of information, some of it very private, the same is true for homes and offices. While computer forensics undeniably threatens privacy, its threat to privacy is roughly equivalent to searching those homes or offices. The policy choices that have permitted searching homes or offices apply with equal strength to examining storage media.

I. THE SUBCONTAINER PERSPECTIVE UNDER THE FOURTH AMENDMENT

A. Computer forensics from two perspectives: subcontainer and physical

1. The Fourth Amendment and recorded information

Search and seizure law treats computers differently from everything else. To see how, consider a paper ledger. A drug testing lab's employees recorded drug test results on the ledger: in one column, the person's name; in another column, the person's drug test results. So the ledger would, for rows and rows, cover more than a hundred people. To a law enforcement officer wishing to investigate drug possession by ten of those people, the ledger is evidence. The

ledger was locked away in the drug testing office. So, the officer obtained a search warrant for that office. The officer had probable cause to believe that ten people had tested positive, so the warrant called for their results only.

At this point, the law is easy to understand. Search warrants can authorize officers to enter premises and search for things. They can seize things that are either contraband or evidence of a crime.[3] That includes seizing papers; the word is in the Fourth Amendment's text, right between "houses" and "and effects." This ledger was evidence of those ten peoples' crimes, and the warrant called for that evidence. The ledger was also evidence of other facts, sensitive facts that had nothing to do with the warrant. However, courts have not faulted seizing the entire ledger; they have explicitly rejected the argument that officers may seize only select pages.[4]

Change one fact. The ledger is a computer file; specifically, a spreadsheet. No printed copy was in the office. The officer must either copy the spreadsheet or seize its only physical embodiment, the computer's hard drive.

Computer searches are now common. Law enforcement officers, usually using a warrant, search a defendant's premises for evidence. Often, that evidence is found on a computer, or other storage medium (a term I use to describe hard drives, floppy disks, cell phones, flash drives, and similar devices).[5] In practice, officers find and copy specific files on-site, take away the entire computer, or make an image copy of the computer's hard drive.[6] The latter two options

---

[3] *See* Zurcher v. Stanford Daily, 436 U.S. 547, 558 (1978) ("Federal Rule Crim. Proc. 41, which reflects the Fourth Amendment's policy against unreasonable searches and seizures, authorizes warrants to search for contraband, fruits or instrumentalities of crime, or any property that constitutes evidence of the commission of a criminal offense.") (citation, ellipses, and quotation marks removed).

[4] *See, e.g.*, United States v. Beusch, 596 F.2d 871, 876 (9th Cir. 1979) (permitting seizure of ledger, and rejecting argument that "pages in a single volume of written material must be separated by searchers so that only those pages which actually contain the evidence sought may be seized").

[5] *See* United States v. Vilar, No. S305CR621KMK, 2007 WL 1075041, at *36 (S.D.N.Y. Apr. 4, 2007) ("[S]ome of the most important evidence of criminal conduct is often found buried in computers. As a result . . . a person who uses a computer, or any electronic device, as an instrumentality of crime might discover that a magistrate judge would find probable cause to search that computer . . . .").

[6] *See id.* at *35 n.22; United States v. Stierhoff, 477 F. Supp. 2d 423, 439 n.8 (D. R.I. 2007); Orin S. Kerr, *Searches and Seizures in a Digital World,* 119 HARV. L. REV. 531 (2005).

are the most common, because examining a computer on-site is difficult.[7]

One could argue that the Fourth Amendment should treat the paper ledger and the hard drive the same. But many would disagree. Consider Judge Bea's separate opinion in *United States v. Comprehensive Drug Testing* (the case from which I draw this example).[8] For Judge Bea, it was crucial that "the agent had to scroll right on the spreadsheet, on to another screen" in order to "see the spreadsheet column containing the [drug testing] results."[9] This scrolling let him view other peoples' results. Viewing those results, Judge Bea seemed to believe, violated the Fourth Amendment. It would have been better, Judge Bea stated, to copy the ten rows to the clipboard, paste them into a new spreadsheet, and look at that new spreadsheet only. Judge Bea described, with surprising detail, how this could be done: "While depressing and holding the Control key, he would click on the numbers on the left side of the spreadsheet . . . then release the Control key[,] . . . click on the 'Edit' menu, and choose 'Copy[,]' . . . click on the 'File' menu at the top of the screen, and choose 'New Blank Workbook[,]' . . . click on the 'Edit' menu in the new blank spreadsheet and choose 'Paste.'"[10]

Judge Bea's approach is unusual in its specificity, but not in its attitude toward applying the Fourth Amendment. His was not the majority opinion, but the majority also faulted investigators for treating the spreadsheet as a unitary whole. They stopped short of writing a tutorial on Excel, but nonetheless treated the spreadsheet as containing distinct zones of privacy.[11]

2. The perspective problem: What are the "facts" of search and seizure?

The disparate treatment of paper ledgers and spreadsheet files illustrates the perspective problem in computer search and seizure. Perspective problems are disputes about how best to characterize and assess the relevant operative facts. They are better-known in Internet

[7] *See* United States v. Hill, 459 F.3d 966, 974-75 (9th Cir. 2006) ("[T]he officers would have to examine every one of what may be thousands of files on a disk—a process that could take many hours and perhaps days.").
[8] United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162 (9th Cir. 2010).
[9] *Id.* at 1180-81 (Bea, J., concurring in part and dissenting in part).
[10] *Id.* at 1181 n.2.
[11] *Id.* at 1171-72.

law.[12] In Internet law, the "internal" perspective views facts as the user experiences them; the "external" perspective views facts as the low-level technology functions. From an internal perspective, the website Amazon.com is a place that one visits; from an external perspective, Amazon.com is accomplished by domain name servers, web servers, clients, program code, routers, and electrons.[13] From an internal perspective, when Alice sends an instant message to Bob, the message is an interstate communication only if Alice and Bob are in different states. From an external perspective, the instant message is an interstate communication if the network happens to carry it outside Alice's state.[14]

Less examined is the perspective problem in computer forensics. The Fourth Amendment generally requires a warrant, and requires a warrant to particularly describe the places to be searched and things to be seized.[15] But, when a storage medium is examined, is that examination a "search?" If it is, what is the "place" and what are the "things?" In answering those questions, one might view computer storage media from one of two mutually exclusive perspectives.

First, one could take an internal perspective and view storage media as the user experiences them: as parcels of information, grouped into files, or even into smaller units such as spreadsheet rows. Under this perspective, those parcels are each their own "thing," independent from each other and from the medium upon which they happen to be recorded. That medium, in turn, begins to look not just like an object, but like a virtual "place" that contains those "things."

Second, one could take an external perspective and view storage media as the computer uses them: as objects, chunks of physical matter whose state is altered to record information. Under this perspective, files are not Fourth Amendment "things" at all. Files are just groupings of data, and data is inseparably tied to the storage medium. The medium is not a "place"; it is an object.

The choice between these perspectives is not a choice between different legal rules; the choice is between the facts to which courts apply legal rules. The same Fourth Amendment rules might require different results depending on the fact perspective. Two recent state

---

[12] *See* Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357 (2003).
[13] *Id.* at 362-63.
[14] *Id.* at 373-74.
[15] *See, e.g.*, Groh v. Ramirez, 540 U.S. 551, 554, 557 (2004).

supreme court decisions illustrate this. Both courts considered whether a cell phone, seized incident to arrest, may be examined without a warrant. The Ohio Supreme Court, in *State v. Smith*, distinguished cell phones from other objects like paper address books and closed containers by pointing to their ability to "store large amounts of private data"; therefore, although police could lawfully seize the phone itself, a warrant was required before accessing the phone's "contents."[16] The California Supreme Court, however, in *State v. Diaz*, explicitly rejected a distinction "between *the cell phone itself* and its *contents*."[17] While recognizing that cell phones could store large amounts of data, the *Diaz* court treated them like any other object found on an arrestee's person, holding, "[T]here is no legal basis for distinguishing the contents of an item found upon an arrestee's person from either the seized item itself or the arrestee's actual person."[18] Both courts applied the same rule that officers may seize things found on an arrestee's person.[19] They simply disagreed about whether data was a "thing."

3. The subcontainer perspective

Between these two perspectives, the most common, by far, is an internal perspective that views a storage medium as a container holding subcontainers of information.[20] It is now common to say an

[16] State v. Smith, 920 N.E.2d 949, 955 (Ohio 2009).
[17] People v. Diaz, 244 P.3d 501, 509 (Cal. 2011).
[18] *Id.* at 115.
[19] *Id.* at 110 ("[T]he key question in this case is whether defendant's cell phone was 'personal property . . . immediately associated with [his] person.'"); *Smith*, 920 N.E.2d at 952 ("Searches may also extend to the personal effects of an arrestee.").
[20] *See, e.g.*, United States v. Mann, 592 F.3d 779, 786 (7th Cir. 2010); Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001) ("[P]assword-protected files are analogous to the locked footlocker inside the bedroom."); *id.* at 410-11 (Michael, J., concurring in part and dissenting in part) (citing cases "drawing analogies between computers and physical storage units such as file cabinets and closed containers"); Marcia Hofmann, *Arguing for Suppression of "Hash" Evidence*, CHAMPION, May 2009, at 20, 22 ("Some courts go a step further, holding that separate files on a computer should be treated as their own closed containers."); Samantha Trepel, *Digital Searches, General Warrants, and the Case for the Courts,* 10 YALE J. L. & TECH. 120 (2007) (describing "the execution of computer searches conducted pursuant to warrants, and the threat of general searches—searches effectively unlimited in scope by the warrant—they raise"); G. Robert McLain, Jr., Casenote, United States v. Hill*: A New Rule, but No Clarity for the Rules Governing Computer Searches and Seizures,* 14 GEO. MASON L. REV. 1071 (2007) ("[A]lthough computers can 'contain' evidence, unlike a traditional container, the evidence is not physical."); Wayne Jekot, *Computer Forensics, Search Strategies, and the Particularity Requirement*, 7 U.

officer "searches" a hard drive, as though the hard drive were a place rather than a thing.[21] A hard drive's subdivisions, like the spreadsheet file or individual folders, can also be subcontainers—that is, places. Yet those subdivisions can also be "things"; files are "seized," according to some. One court, for example, found that a warrant permitted a search of an entire hard drive except for encrypted folders, apparently considering them a separate place.[22] Small portions of files, such as particular spreadsheet cells, can also be "things," and discrete things, at that. Some courts draw an additional distinction based on password-protected user accounts.[23] A spreadsheet, in other words, is a thing (a file), that contains many other things (spreadsheet cells), and is therefore also a place (the file, again), written in another place (the user's password-protected account), which is written in another place (the hard drive), wrapped up into a thing (the hard drive, again), which is found in a place (the building that happens to hold the hard drive).

I call this perspective the subcontainer perspective. The subcontainer perspective conceptually divides a single hard drive, cell phone, or other storage medium into many subcontainers, each subcontainer requiring justification for its examination. Chief Judge James M. Rosenbaum perhaps described the subcontainer perspective best when he proposed that courts "treat[] separate hard drive files as separate closed containers," so that each container's examination requires separate Fourth Amendment justification.[24] Put another way, "a computer should be viewed as a physical container with a series of electronic 'containers'—that is, directories, folders, and files that must

PITT. J. TECH. L. & POL'Y 2 (2007) ("How comprehensive should a computer search be? In other words, how should the particularity requirement be applied to computer searches?"); Orin S. Kerr, *Search Warrants in an Era of Digital Evidence,* 75 MISS. L.J. 85, 88 (2005) ("[T]he warrant should state the physical evidence that the police plan to seize at the physical stage and the electronic evidence that the forensics analysts plan to search for at the electronic stage.").

[21] *See, e.g.*, *Mann,* 592 F.3d at 786; United States v. Burgess, 576 F.3d 1078, 1089 (10th Cir. 2009).

[22] United States v. Kim, 677 F. Supp. 2d 930, 949-50 (S.D. Tex. 2009).

[23] *See, e.g.*, *Trulock*, 275 F.3d at 403; United States v. Trejo, No. 09-cr-20404, 2010 WL 940036, at *9 (E.D. Mich. Mar. 12, 2010).

[24] James M. Rosenbaum, *In Defense of the Sugarbowl*, 9 GREEN BAG (Autumn 2005), *reprinted in* 2006 FED. CTS. L. REV. 4 (June 2006), *available at* http://www.fclr.org/fclr/articles/html/2006/fedctslrev4.pdf.

be each separately opened. Each separate opening is the examination of a new container."[25]

Among commentators and most courts, this view is widespread and dominant.[26] Whenever a lawyer treats storage media as a collection of information, only some of which may be used in an investigation, that lawyer employs the subcontainer perspective. Courts employ the subcontainer perspective when they hold that warrants must specify particular categories of file as the "things" to be "seized" from storage media.[27] Even those who question whether storage media are properly analogized to containers at all might nonetheless treat storage media as having separate subcontainers of information.[28]

4. Walter v. United States *and the choice of perspective*

This popularity is somewhat surprising, given that the one time the Supreme Court came close to deciding between the subcontainer perspective and the physical perspective, it was divided. In *Walter v. United States*,[29] private parties obtained—thanks to a package delivery mix-up—a box of obscene motion picture films. The private parties unpacked the boxes, but did not successfully view the films.[30] Instead, they called the FBI; and FBI agents, using a standard film projector, viewed the film.[31]

---

[25] Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures*, 75 MISS. L.J. 193, 240 (2005).

[26] *See supra* note 20.

[27] *See, e.g.*, United States v. Potts, 586 F.3d 823, 833 (10th Cir. 2009) ("With respect to computer searches, we have held that the particularity requirement of the Fourth Amendment demands that '[o]fficers must be clear as to what it is they are seeking on the computer and conduct the search in a way that avoids searching files of types not identified in the warrant.'"); United States v. Fleet Management Ltd., 521 F. Supp. 2d 436, 443 (E.D. Pa. 2007); United States v. Vilar, No. S305CR621KMK, 2007 WL 1075041, at *36 (S.D.N.Y. Apr. 4, 2007) ("[U]nderlying information must be identified with particularity and its seizure independently supported by probable cause.").

[28] *See, e.g.*, State v. Smith, 920 N.E.2d 949, 954 (Ohio 2009) (holding that a cell phone is not a closed container for purposes of Fourth Amendment analysis, but also describing cell phones as containing phone numbers); United States v. Burgess, 576 F.3d 1078, 1088-90 (10th Cir. 2009).

[29] 447 U.S. 649 (1980).

[30] *Id.* at 652.

[31] *Id.*

All justices agreed that the film was lawfully in the FBI's possession, but they split, four to four, over whether projecting the film constituted a search. Four justices agreed that projecting the film was a search and that "[t]he fact that FBI agents were lawfully in possession of the boxes of film did not give them authority to search their contents."[32] The contents, in other words, remained private even though they were recorded on film that was in the agents' hands. Four dissenters, however, rejected the notion that projecting the film "was an additional and unconstitutional search," because there was "no remaining expectation of privacy in [the films'] contents" upon their receipt by the FBI.[33] The contents, in other words, ceased to be private when the film came into the agents' possession. Justice Marshall cast the deciding vote without joining any opinion.

Walter illustrates how difficult the perspective problem can be. Yet, its non-computer facts barely hint at the complexities in store when one attempts to figure out how the Fourth Amendment applies to storage media. There, the question is usually not whether officers can look at the media's "contents," but rather which parts. As mentioned, agents generally seize a computer or copy it, and then examine it off-site. This means that the examiner now possesses all the data on that hard drive, including some data that, everyone would agree, has nothing to do with the investigation. They must sift through everything to locate what is relevant. This process, simple to describe, poses difficult questions for lawyers. What, exactly, was "seized"—the computer or the files? Is going through the computer off-site a "search," and, if so, how does the Fourth Amendment limit that search? It is as if the *Walter* court had to answer not just whether FBI agents may project a film, but whether the Fourth Amendment draws distinctions among the film frames, characters, or scenes they may project, and whether it governs how the film might be viewed.

There is a way to choose among these perspectives. Just as applying legal rules to facts requires selecting a perspective, writing those rules in the first place also required selecting a perspective. The choice used to draft the rules should, in most cases, also be the choice used to apply the rules.[34] It is possible to believe this is a sensible rule

[32]*Id.* at 649, 654 (Stevens, J., joined by Stewart, J.); *see also id.* at 660 (White, J., joined by Brennan, J.) ("[P]rojection of the films constituted a search that infringed petitioners' Fourth Amendment interests even though the Government had acquired the films from a private party[.]").
[33]*Id.* at 663 (Blackmun, J., joined by Berger, C.J., Powell, J., and Rehnquist, J.).
[34]*See* Kerr, *supra* note 12, at 392-93.

of interpretation regardless of what one believes generally about deeper questions such as constitutional theory or statutory history's importance. No matter how one decides what the rules are, when those rules presume certain concepts exist, it is reasonable to adopt a fact perspective in which those concepts exist.

5. The physical premise behind search and seizure law

Search and seizure law is a combination of legal authorities, written by different authors at different times; yet, with few exceptions, those authorities assume an external, physical perspective. Federal Rule of Criminal Procedure 41—the federal rule governing issuing and executing search warrants—phrases its commandments with physical terms.[35] It presumes that searches occur in territorial "districts," that "persons" or "property" are searched and seized, that warrants are "executed" at an "exact date and time," which presumptively must be during "daytime," that officers are "present" at the execution of warrants, and that property is "taken" from premises and can be "inventor[ied]."[36] When Rule 41 finally addressed storage media directly, the Rules Committee again opted for a physical approach. Amendments that went into effect in 2009 clarified that inventories of seized storage media "property" need only describe "physical storage media," not information, and that the time for "executing" the warrant covered the time to seize or copy the media, not to examine it.[37] That latter change codified cases holding that seized media need not be examined within the 10 (later, 14) days allotted by Rule 41 for a warrant's "execution."[38]

The Fourth Amendment also employs physical language: persons, houses, papers, effects, places, and things. It is so physical that, for years, it was interpreted only in physical terms,[39] although that

[35] *Cf.* Kerr, *supra* note 12, at 403-404 (arguing that the "external" perspective should apply to the question of whether officers on a premises can download files from a remote location in part because Rule 41 "shows careful attention to the location of the property that can be searched by a particular warrant").

[36] FED. R. CRIM. P. 41(a)(2)(B), (b)(1), (c)(2), (f)(1)(B) & (f)(1)(C).

[37] *Id.* at 41(f)(1)(B).

[38] *See, e.g.*, United States v. Brewer, 588 F.3d 1165, 1172-73 (8th Cir. 2009); United States v. Mutschelknaus, 564 F. Supp. 2d 1072, 1076-77 (D. N.D. 2008), *aff'd*, 592 F.3d 826 (8th Cir. 2010); United States v. Syphers, 296 F. Supp. 2d 50, 58 (D. N.H. 2003), *aff'd,* 426 F.3d 461 (1st Cir. 2005); United States v. Hernandez, 183 F. Supp. 2d 468, 480 (D. P.R. 2002).

[39] *See, e.g.*, Silverman v. United States, 365 U.S. 505, 509-10 (1961) (finding eavesdropping to be a Fourth Amendment violation only because it was accomplished by "a physical intrusion").

is no longer the case. While physical privacy invasions are "the chief evil against which the wording of the Fourth Amendment is directed," that Amendment also protects against intangible privacy invasions, such as wiretaps.[40] Similarly, Rule 41's definition of "property" includes both "tangible objects" and also "information."[41] Yet these are exceptions, notable for departing from the vast bulk of search and seizure cases, which tend to involve entry into physical spaces and seizing physical evidence or persons. Perhaps as a consequence, wiretaps—the most prominent non-physical "searches" under the Fourth Amendment—are governed by their own special code, not by Rule 41 and Fourth Amendment case law that assumes a physical world.[42]

6. "Translating" and "rethinking" the Fourth Amendment

Those who use the subcontainer perspective tend to acknowledge that black-letter search and seizure rules are physical.[43] While some call for creating new, subcontainer-regarding rules,[44] most prefer to render the existing physical rules abstract, and then use them to govern forensic examiners' work. The initial decision to treat storage media as having subcontainers departs from physical moorings; after that departure, metaphors are necessary to apply physical rules to the new virtual world. Hence, for the subcontainer

---

[40] United States v. United States District Court, 407 U.S. 297, 313 (1972) ("Though physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed, its broader spirit now shields private speech from unreasonable surveillance."); *id.* at 302 ("Much of Title III was drawn to meet the constitutional requirements for electronic surveillance enunciated by this Court."); United States v. Villegas, 899 F.2d 1324, 1334 (2d Cir. 1990); *see* Paul Ohm, *The Olmsteadian Seizure Clause: The Fourth Amendment And The Seizure Of Intangible Property,* 2008 STAN. TECH. L. REV. 2 (2008); *see also* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution,* 102 MICH. L. REV. 801, 807 (2004).

[41] FED. R. CRIM. P. 41(a)(2)(A); *see also* United States v. New York Telephone Co., 434 U.S. 159, 169 (1977) ("Rule 41 is not limited to tangible items but is sufficiently flexible to include within its scope electronic intrusions authorized upon a finding of probable cause.").

[42] *See* 18 U.S.C. §§ 2516-18.

[43] *See, e.g.*, Kerr, *supra* note 6, at 533 ("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.").

[44] *See, e.g.*, United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1179-80 (9th Cir. 2010) (Kozinski, C.J., concurring).

perspective to make sense, one must "rethink Fourth Amendment doctrine in order to preserve the function of existing law in light of new facts."[45] Described another way, this is "[t]ranslating Fourth Amendment rules" into "rules that regulate digital investigations,"[46] or even "transfer[ing] our physical world notions of searches to the context of computers."[47]

This rethinking, transferring, and translating project has been underway for at least two decades.[48] Observing its product lets us judge whether the subcontainer perspective permits the application of search and seizure rules in a way that is both administrable and also preserves the Fourth Amendment's function. It does not. As described below, when physical search and seizure rules are viewed through a perspective that treats files or information as "things," they cease to make sense. Part I.B discusses how the fundamental definition of what the new virtual subcontainer "thing" is might be translated in contradictory ways, all of them disconnected from privacy concerns or unworkable. Part I.C discusses how rules governing the reasonableness of searches—that is, rules governing how searches must occur—don't translate clearly, or at all. Part I.D discusses how the rules governing what may be lawfully "seized" produce counterintuitive results: most courts applying the subcontainer perspective have permitted examiners to view every file on a hard drive, so long as examiners comply with cumbersome but pointless formalities. Minus the cumbersome but pointless formalities, this is the same conclusion that the physical perspective came to at the beginning.[49] Part I.E discusses how, in reaction to this result, some have begun to question the translation enterprise altogether. However, the real problem is not how courts have translated the rules, but rather the decision to adopt a fact perspective that was so at odds with search and seizure law that it required translation. The virtual world exists

[45] Kerr, *supra* note 6, at 533.
[46] Trepel, *supra* note 20, at Part I.
[47] Kerr, *supra* note 6, at 551; *see also* Kerr, *supra* note 20, at 126-35 (proposing amendments to Rule 41 to "respond to the specific issues raised by the switch from physical evidence to digital evidence").
[48] *See, e.g.*, United States v. David, 756 F. Supp. 1385, 1390 (D. Nev. 1991) (holding an officer's turning on a "computer memo book" belonging to David "did constitute a search, however, if, under the circumstances, David had a reasonable expectation that when he turned the book off, its contents would remain private").
[49] *See infra* note 112.

only from the subcontainer perspective, but forensics is physical. The physical perspective was the better choice, all along.

B. The problem of drawing subcontainers

1. The file subdivision strategy and its inspiration

The subcontainer perspective is persuasive because it corresponds to the way that lawyers and judges experience computers: as multi-purpose machines that store information in discrete parcels. It seems natural that the law would respect those subcontainers' integrity by requiring police to independently justify intruding into each parcel's privacy. The law becomes a means to "regulate access to information" in a "digital environment" where "physical barriers often are missing."[50]

Regulating access to information, rather than just to storage media, requires a decision: when does the forensic examiner access too much information? From the subcontainer perspective, this question becomes: what are the subcontainers? Or: where do we draw the barriers in the "digital environment" to replace the missing physical barriers? These questions are all equivalent; defining subcontainers defines what information is immune to seizure.[51] For example, to evaluate whether it was proper to seize an entire directory of files when only one file was relevant, we must decide whether the file or the directory formed the relevant subcontainer. To evaluate whether seizing an entire spreadsheet is proper when only some cells were relevant, we must decide whether the relevant subcontainer was the spreadsheet or something smaller.

Courts seldom address head-on what the subcontainers are. But from their holdings, it is possible to glean a dominant strategy: subdividing by file.[52] Doing so allows courts to easily analogize

---

[50] Kerr, *supra* note 6, at 535.

[51] This has also been called the "zone of a search." *Id.* at 554.

[52] *See, e.g.*, United States v. Williams, 592 F.3d 511, 521-22 (4th Cir. 2010) ("[T]he warrant impliedly authorized officers to open each file on the computer . . . to determine whether the file fell within the scope of the warrant's authorization[.]"); United States v. Cartier, 543 F.3d 442, 446-47 (8th Cir. 2008); United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001) ("Officers must . . . conduct the search in a way that avoids searching files of types not identified in the warrant."); Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001) ("[P]assword-protected files are analogous to the locked footlocker inside the bedroom."); *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) (advocating "file-by-file" limitations on search techniques).

computers to filing cabinets. For the most part, the rule for filing cabinet searches is that officers can either search through them on-site or, if that is impractical, seize filing cabinets and review them later.[53] To many courts, filing cabinet searches are directly analogous to computer searches; both filing cabinets and computers intermingle things called "files."[54] The file strategy appears to correlate Fourth Amendment rules with how people actually use computers. People do not, after all, consciously magnetize regions on a hard drive platter; rather, they save files. Moreover, they save particular data in particular files, and sometimes even sort that data into different directories. Basing the subcontainer divisions on users' decisions about how to store data might be a meaningful solution to subdivision problem.[55]

2. The file subdivision strategy's shortcomings

An initial difficulty with the file strategy is that not all electronic evidence is a file. While desktop and laptop computers usually have hard drives, they also have Random Access Memory (RAM). RAM is temporary storage, used by the computer from nanosecond to nanosecond. Like hard drives, RAM also can be imaged and searched for evidence. In fact, RAM can reveal evidence unlikely to be on a hard drive, such as encryption keys.[56] Yet, RAM is not organized into files at all. Even advanced computer users generally have no idea what is in their RAM. RAM also forgets all data once the computer is turned off, a highly un-container-like habit. Moreover, RAM has no user-directed grouping into anything resembling "files," and is not rendered comprehensible by a user interface. Intuitive cues that suggest hard drives are analogous to file cabinets do not hold true for RAM.

---

[53]*See* United States v. Giannetta, 909 F.2d 571, 577 (1st Cir. 1990) ("[T]he police may look through . . . file cabinets, files and similar items and briefly peruse their contents to determine whether they are among the documentary items to be seized."); United States v. Ochs, 595 F.2d 1247, 1257 n.8 (2d. Cir. 1979) (permitting "some perusal" that is "generally fairly brief"); United States v. Heldt, 668 F.2d 1238, 1267 (D.C. Cir. 1982) (allowing a "brief perusal" of each document).

[54]*See, e.g.*, United States v. Williams, 592 F.3d 511, 523 (4th Cir. 2010); Comm'r v. McDermott, 864 N.E.2d 471, 488 (Mass. 2007). *But see* United States v. Carey, 172 F.3d 1268, 1272 (10th Cir. 1999).

[55]Kerr, *supra* note 6, at 555-56.

[56]*See* Carsten Maartmann-Moe, Steffen E. Thorkildsen & André Årnes, *The Persistence of Memory: Forensic Identification and Extraction of Cryptographic Keys,* 6 DIGITAL INVESTIGATION S132 (2009).

Another problem with the file strategy is its underlying assumption that only files contain evidence. That assumption is a gross simplification. Forensic examiners examine media, not just files.[57] "Files are contingent creations assembled by operating systems and software," blocks of bytes that the computer cobbles together and presents as a single unit.[58] Officers image—that is, copy byte for byte—hard drives, and then examine them with forensic software such as EnCase or FTK.[59] That forensic software looks for evidence, and not all evidence comes in files. Most reported computer storage medium cases involve child pornography prosecutions, and in those cases image and movie files are important evidence. But there is more to forensic analysis than that.

Just as forensic pathologists can examine a cadaver's fractures, bruises, calluses, and scars to determine what happened to that body over a person's lifetime, so too can a computer forensic analyst examine a hard drive to learn how a computer was used. When a computer user accesses a web site, opens a file, launches a program, starts the computer, shuts it down, logs on, logs off, installs software, removes software, or attaches a flash drive, hard drives reflect those actions. Forensic analysts term such evidence "artifacts."[60] Like archaeological artifacts showing how people once lived, forensic artifacts show how computers were used. Log files show what software programs did. Virtual memory paging files can reveal what was once in memory. Temporary files and link files can reveal that someone created, opened, or saved particular files.[61] When a user saves a file in Microsoft Word, for example, eight different files or folders are created, modified, or accessed in sixteen different steps, all occurring in less than a second.[62] In Windows, a vast configuration database, called the "registry," is an evidence treasure chest, showing recent user commands, recent files opened, recent network drives

---

[57] *See* United States v. Crist, 627 F. Supp. 2d 575, 578 (M.D. Pa. 2008) ("Agent Buckwash . . . explained that EnCase does not access the hard drive in the traditional manner, *i.e.,* through the computer's operating system. Rather, EnCase 'reads the hard drive itself.'").

[58] Kerr, *supra* note 6, at 557.

[59] *See* United States v. Vilar, No. S305CR621KMK, 2007 WL 1075041, at *35 n.22 (S.D.N.Y. Apr. 4, 2007).

[60] *See* Coburn v. PN II, Inc., No. 2:07-cv-00662-KJD-LRL, 2010 WL 3895764, at *1 n.1 (D. Nev. Sept. 30, 2010).

[61] *Developments in the Law: Electronic Discovery*, 38 LOY. L.A. L. REV. 1541, 1560 (2005).

[62] Thanks to Ovie Carroll for this analysis.

accessed, recent web sites visited, whether USB flash drives were attached, what Wi-Fi wireless access points have been used, and more.[63]

Constrained to reason only in terms of files, how could a court decide whether an examiner may access this evidence? Virtual memory paging files, web server log files, web browser artifacts, registry databases, configuration files, and operating system link files might all be "files" according to operating system engineers. However, if the reason to emphasize files is that they correspond to a defendant's organizational choices (and thus the defendant's subjective privacy expectations), then placing these system files in the same category as a memo saved by a word processor is unsupportable. These files do not correspond to organizational choices made by computer users. Computer users do not consciously create or modify them. Software engineers, not computer users, decided what these files would contain, what they were named, where they were saved, and whether they existed at all. The Windows registry database, for example, is spread across multiple files. There is no reason why that decision, made by software engineers based on considerations that had nothing to do with privacy, should affect how a court evaluates an examiner's conduct.

The file strategy has an even tougher time when key evidence is not a file. A well-known example is unallocated space. "Empty" space on a storage medium is not, in all cases, empty. A file, or part of a file, might have once been recorded to part of the storage medium, and although the file system now treats that file as deleted, the physical medium still holds its remnants. By examining this space, examiners can find not only deleted files, but sometimes even portions of deleted files.[64]

Consider another example: the file system. A file system is an organizational strategy that an operating system employs to keep track of files saved on a storage medium. The file system keeps track of where the files are physically written on the storage medium, and also tracks information about those files, such as what they are named, who

[63] *See* Harlan Carvey, *The Windows Registry as a Forensic Resource*, 2 DIGITAL INVESTIGATION 201 (2005).

[64] *See, e.g.*, United States v. Angevine, 281 F.3d 1130, 1132 (10th Cir. 2002); United States v. Crist, 627 F. Supp. 2d 575, 578 (M.D. Pa. 2008) (noting that EnCase forensic software can "recover 'deleted' files as long as those files have not been written over"); Commonwealth v. Copenhefer, 587 A.2d 1353, 1355 (Pa. 1991).

created them, and when.[65] File systems set aside a portion of storage media to record this information. Information written in that space is valuable to a forensic examiner.

For example, in *Fharmacy Records v. Nassar*, an examiner knew that the Mac file system keeps a running count of how many files had been saved, and it attached a serial number to every new file.[66] When a user attempted to back-date a file by changing its time stamp, this file system evidence revealed the deception. Even though a file purported to have an older date, its serial number (and the time stamps on files with immediately adjoining serial numbers) showed it had been made later.[67] Thus, three facts—the file's serial number and the time stamps on the other two files—when considered together allowed the examiner to conclude that the time stamp was inaccurate.
How can one evaluate the *Fharmacy Records* examiner's conduct under a legal regime in which "a computer [is] a physical container with a series of electronic 'containers'—that is, directories, folders, and files" and "[e]ach separate opening is the examination of a new container?"[68] Limited to a language of files, it is not only impossible to answer that question, but also impossible to articulate it. The serial number was not saved in any file. The date stamps, though associated with files, also were not files. Indeed, if the examiner were only allowed to examine the backdated file in isolation without also examining the hard drive upon which it was saved, he could not have analyzed the crucial evidence. The evidence was not a file; the evidence was the way the user's actions changed the storage medium. No matter how we try to corral the evidence into files, it is difficult to escape the conclusion that a hard drive is not just a repository of files, but rather an object that changes because of how someone used a computer.

3. Subdividing below the file level

What about devices that undeniably have files, and evidence that undeniably is a file? Even here, the file strategy poses another problem. One file can present the same intermingling problem as hard drives. One file can mix a drop of responsive data into a sea of

---

[65] *See* Alexander G. Tormasov et al., System and Method for Using File System Snapshots For Online Data Backup, U.S. Patent No. 7,047,380 B2, at 17 (issued May 16, 2006).
[66] Fharmacy Records v. Nassar, 379 Fed. Appx. 522, 525 (6th Cir. 2010).
[67] *Id.*
[68] Clancy, *supra* note 25, at 240.

unresponsive material—just as a hard drive can. A SQL database, holding all of a dynamic web site's data, might be a single file. E-mail software is likely to save an e-mail inbox as one file. A diary writer might type every diary entry, spanning years, into one repeatedly edited word processing file. If a single database record, e-mail, or diary entry is responsive, but the entire file is seized, then that seizure replicates, on a different scale, the intermingling problem that the subcontainer perspective was supposed to solve.

To address these problems, it is possible to adopt the file strategy, but then complicate it by subdividing *within* the file. That strategy has its own problems.

The court in the *Comprehensive Drug Testing* case mentioned earlier ("*CDT*") confronted how to treat a single Excel spreadsheet file that "contained both the names of the ten ballplayers who were the subjects of the warrant and the names of many other ballplayers, the records of whom the government did not have probable cause to search and seize."[69] They confronted, in other words, the problem of intermingling within a file. Chief Judge Kozinski's concurring opinion (and, before it was withdrawn and revised, the en banc court's majority opinion) appears to call for redaction—within a single file, a redactor should eliminate facts, leaving for the investigator only facts particularly described in the warrant.[70] Under this view, a file is not one thing, but a collection of facts in the same way that a directory is a collection of files. Following that reasoning, just because an officer found a spreadsheet with the test results he was looking for, that does not mean he may read the whole spreadsheet. Redaction conceptually divides files into smaller fact collections. One must keep dividing until the remaining facts are all safely within the warrant. Judge Bea's tutorial on copying rows from an Excel spreadsheet was, apparently, an attempt to explain how this might be done.[71]

The "fact" subdivision strategy is free of the file strategy's arbitrariness and technological simplicity, but it lacks the file strategy's relative clarity. Where do facts begin and end? How does a redactor know when he has redacted enough? Consider an e-mail,

[69] United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1180 (9th Cir. 2010) (Bea, J., concurring and dissenting).

[70] *Id.* at 1180 (Kozinski, C.J., concurring) ("Segregation and redaction of electronic data must be done either by specialized personnel or an independent third party."); *id.* at 1179 (Kozinski, C.J., concurring) ("Once the data has been segregated (and, if necessary, redacted) . . . .").

[71] *See supra* note 10.

saved to a hard drive, that reads, "Yesterday, John and I delivered the cocaine to Joe's place in Chicago." The warrant was for evidence of that e-mail's author's drug crimes. Can this sentence pass through the redactor unscathed, or does it include facts not particularly described in the warrant? The warrant said nothing about John or Joe, and said nothing about Chicago—indeed, the investigators may have had no idea that John and Joe were involved, or that Chicago was a destination. To protect John and Joe's privacy, perhaps their names should be redacted. Or perhaps those names should remain because they provide helpful context? Or perhaps John and Joe's participation in the transportation is, indeed, evidence of the drug crimes described in the warrant? In answering these questions, the redactor must confront complex questions about context and relevance. He must do this with limited case knowledge. Because redactors cannot work on the case after the redaction is complete, investigative agencies seldom have the resources to equip redactors with the same knowledge as case agents.[72]

Deciding how to subdivide storage media remains a conspicuously incomplete item on the subcontainer perspective's "to-do" list. To some extent, the subdivision question is a battle between different internal perspectives: files and facts are two competing strategies for conceptualizing the "things" that storage media might contain. This competition points to a flaw. Storage media do not naturally divide into parts. Subdivisions must be invented, and every subdivision strategy comes with flaws. The subcontainer perspective's challenges, however, do not end there.

C. The subcontainer perspective and reasonable searches

By characterizing a storage medium's forensic examination as a Fourth Amendment search, the subcontainer perspective promises to use translated search and seizure rules to limit the examination's scope. Yet, those rules do more than just limit evidence acquired in a search. An important part of search and seizure law regulates

[72] *See* Brief of the United States in Support of Rehearing En Banc by the Full Court at 21, United States v. Comprehensive Drug Testing, Inc., Nos. 05-10067, 05-15006, 05-55354 (9th Cir. Nov. 23, 2009), *available at* http://www.wired.com/images_blogs/threatlevel/2009/11/kagan.pdf ("Before a search commences, case agents will need to spend days, weeks, or even months teaching both the underlying law and the specifics of the particular case to members of a filter team. Even after receiving such a crash course, filter team members will be unlikely to know a case as well as the case agents, with the result that at least some responsive and potentially case-critical information will go unrecognized.").

obtaining and executing a warrant. These rules, some going back to English common law, give substance to the otherwise vague requirement that a search not be unreasonable.[73] To give a few examples, search and seizure law governs how officers may conduct a search, who may issue a warrant, to whom it can be directed, whether and when property owners receive notice a search has occurred, the time and manner in which warrants may be executed, who may execute them, and which court has territorial jurisdiction.[74]

The difficulty applying—indeed, even enunciating—what these rules mean from the subcontainer perspective suggests that these rules cannot sensibly be "translated" at all. In his *Walter* dissent, Justice Blackmun presaged these difficulties with a simple question: if a warrant is required before projecting a motion picture film already in the FBI's possession, then "on whom would the warrant be served?"[75] This question about serving a search warrant on a piece of film was more than a complaint about giving officers unsolvable puzzles; it was an argument that selecting an internal perspective was so inconsistent with search and seizure rules that it could not be right.

1. "Search" and "seize" from the subcontainer perspective

Under the subcontainer perspective, Justice Blackmun's simple, as-yet unanswered question multiplies into many simple, unanswered questions.

---

[73] *See, e.g.*, Hudson v. Michigan, 547 U.S. 586, 589 (2006) ("The common-law principle that law enforcement officers must announce their presence and provide residents an opportunity to open the door is an ancient one."); Buonocore v. Harris, 65 F.3d 347, 354 (4th Cir. 1995) ("[A]s early as 1603, it was established in the common law that intrinsic to the validity of the specific warrant was that it had to be executed by a properly commissioned officer to further the *government's purposes*.").

[74] *See* Wilson v. Layne, 526 U.S. 603, 611 (1999) ("[T]he Fourth Amendment does require that police actions in execution of a warrant be related to the objectives of the authorized intrusion[.]"); Shadwick v. City of Tampa, 407 U.S. 345, 349 (1972) (holding that non-lawyer county clerks may issue warrants provided the clerks are detached and neutral); 18 U.S.C. § 3105 (limiting who may serve a search warrant); Lo-Ji Sales, Inc. v. New York, 442 U.S. 319, 326-27 (1979) (holding that the personal participation of a town justice in the execution of his own warrant violated the Fourth Amendment); FED. R. CRIM. P. 41(f)(1)(C) (requiring notice in the form of a receipt); 18 U.S.C. § 3103a(b) (permitting delayed notification of searches in some circumstances); FED. R. CRIM. P. 41(e)(2)(A) (warrants must require execution within 14 days and generally during daytime); FED. R. CRIM. P. 41(b) (territorial jurisdiction to issue a warrant).

[75] Walter v. United States, 447 U.S. 649, 665 n.3 (Blackmun, J., dissenting).

To begin, the very meanings of the words "search" and "seize" are unclear. The Third Circuit recently stated that "[m]ere observation must be distinguished from seizure, a distinction that may become hazy in the digital environment."[76] Hazy, indeed: if pulling data off a hard drive and viewing it is not seizure, then what is?[77] Perhaps data is "seized" when officers walk out the door with the storage medium. Or, perhaps seizure happens when the owner "loses the ability to dispose of or alter" the data—that is, when officers copy data.[78] Or, perhaps the key moment is when an examiner isolates data and selects it for use in evidence.[79]

How are these actions distinct from "search?" It is no longer clear that a search happens before a seizure. Some contend these steps are reversed, because the government first seizes computers and then searches their contents.[80] It is also no longer clear that a search happens in a "place" distinct from the "thing" being searched. Under the subcontainer perspective, the "search" of a hard drive is sifting through the things written on a storage medium to identify those called for by the warrant. But when, precisely, does this virtual search occur, and just as important, when does it not occur? Possibilities include reading or searching it with a computer program, calculating a hash value,[81] copying the file, "opening" the file with a hex editor so that a computer displays the raw bytes that make up the file, "opening" the file so that a computer application displays it on a screen in a manner

---

[76] United States v. Stabile, 633 F.3d 219, 241 n.17 (3d Cir. 2011).

[77] *Cf.* Kerr, *supra* note 6, at 556 (defining the scope of search, but not seizure, as "whatever information appears on the output device . . . "). "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." *Id.*

[78] Paul Ohm, *The Fourth Amendment Right to Delete,* 119 HARV. L. REV. 10 (2005); Orin S. Kerr, *Fourth Amendment Seizures of Computer Data,* 119 YALE L.J. 700, 709 (2010).

[79] *See* United States v. Triumph Capital Group, Inc., 211 F.R.D. 31, 42, 63-64 (D. Conn. 2002).

[80] *See, e.g.*, *In re* Search of 3817 W. West End, First Floor Chicago, Illinois 60621, 321 F. Supp. 2d 953, 958 (N.D. Ill. 2004) ("[I]t is frequently the case with computers that the normal sequence of 'search' and then selective 'seizure' is turned on its head.").

[81] *See* United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1179 (9th Cir. 2010) (Kozinski, C.J., concurring) ("[T]he government has sophisticated hashing tools at its disposal that allow the identification of well-known illegal files (such as child pornography) without actually opening the files themselves. These and similar search tools may not be used without specific authorization in the warrant . . . .").

that is meaningful for a human examiner,[82] and, finally, reading it by eye.

2. Jurisdiction, execution, and reasonableness from the subcontainer perspective

One feels, painfully, the indeterminate meaning of subcontainer searches and seizures when one tries to consider search and seizure rules other than the particularity requirement. Procedural rules governing warrants' issuance and execution (chiefly, Rule 41) assume "search" and "seize" are understood. Replacing those concepts with hazy substitutes magnifies the subcontainer perspective's uncertainty.

For example, in general, only a local magistrate can issue a warrant to search in a particular district.[83] If, as the subcontainer perspective suggests, a forensic exam virtually "searches" a storage medium, then how does that rule apply? Suppose data is copied in one district and then the copy is moved to another; does examining the data in that other district violate the warrant's command to search only in the first district? Suppose a hard drive is copied in Oklahoma, the copy is put on a forensic file server in Texas, and examiners in both Virginia and West Virginia access it; what court needs to issue that warrant?

For that matter, under the subcontainer perspective, when does a search occur and when may it not occur? Must the examination occur soon after the drive is seized?[84] Can officers repeatedly examine the storage medium, or, as with a premises search, are "second looks" generally prohibited? Can officers examine it during trial? Rule 41 says searches cannot be done at night unless good cause is shown;[85] does that limitation apply to a forensic analyst working late hours the night before a trial or hearing? Can only law enforcement agents perform forensic analysis, or, as with drug testing laboratories, can contractors do it? What if the government subpoenas the computer from its owner—does the Fourth Amendment govern whether the government can turn it on?[86] Suppose a prosecutor, during trial, seeks

[82] *See* Kerr, *supra* note 6, at 557-62.
[83] FED. R. CRIM. P. 41(e)(2)(A), (b).
[84] *See supra* note 38.
[85] FED. R. CRIM. P. 41(e)(2)(A)(ii).
[86] United States v. Triumph Capital Group, Inc., 211 F.R.D. 31, 37 (D. Conn. 2002) ("After obtaining possession of the laptop computer [with a grand jury subpoena], the government obtained a warrant to search and seize its hard drive and obtained certain incriminating evidence.").

to put a physical cell phone into evidence so that a jury can examine it in the jury room without limit—is that a prohibited "search?"[87]

Under the subcontainer perspective, there are no clear answers to these questions. If computer forensic examination is a "search," then it can't be that officers can ignore all these rules. One of those rules—the Fourth Amendment's particularity requirement—is always applied under the subcontainer perspective; but others, such as the requirement that the search be executed within a specified time, are not.[88]

The subcontainer perspective, then, does not faithfully translate all the search and seizure rules. The translator must pick and choose. That necessity demonstrates the subcontainer perspective's unsuitability. One consideration in choosing between competing fact perspectives is what the legal rule's drafters appear to have chosen.[89] Legal rules will always have gray areas, but the subcontainer perspective creates new gray areas where there used to be black and white. The new gray area's size suggests that the subcontainer perspective is the wrong perspective—that it forces search and seizure rules into an extended, implausible analogy. The drafters of search and seizure law assumed a physical world: the law built up by legislatures, courts, and rules committees arose from physical cases, and its substance is, with few exceptions, physical.[90] It is not surprising, then, that so much confusion results when we try to apply search and seizure law from an internal, subcontainer perspective. This is a strong argument for the physical perspective, and the large gray area left by the subcontainer perspective makes that argument stronger.

---

[87] *Cf.* Haniffy v. Gerry, Civil No. 08-cv-268-SM, 2010 WL 347037, at *8 (D. N.H. Jan. 26, 2010) ("Haniffy's cell phone was properly admitted into evidence. The jury was, therefore, entitled to examine it.").

[88] *See supra* note 38.

[89] *See* Kerr, *supra* note 12, at 392-93.

[90] *See supra* text accompanying notes 35-46; *cf.* Kerr, *supra* note 12, at 403-04 (arguing that the "external" perspective should apply to the question of whether officers on a premises can download files from a remote location in part because the language of Rule 41 "shows careful attention to the location of the property that can be searched by a particular warrant").

D. The subcontainer perspective's struggle to regulate forensic examination

1. The particularity requirement

A storage medium intermingles a large amount of information, some of it personal. Judge Kleinfeld, for example, wrote that "for most people, their computers are their most private spaces," more private than a bedroom.[91] The subcontainer perspective owes much of its popularity to a desire to protect that privacy while still allowing investigators access to hard drives. When combined with translated Fourth Amendment rules, the subcontainer perspective promises to limit forensic examination—or, to use subcontainer language, to limit "where" on the medium an officer may "look."[92] This promise comes from the Fourth Amendment's requirement that warrants "particularly describ[e] the place to be searched, and the persons or things to be seized." Viewed through the subcontainer perspective, this clause requires that search warrants specify particular categories of file (or fact) as the "things" to be "seized" from storage media.

A corollary rule faults search warrants for authorizing the seizure of all data on a particular drive. From a physical perspective, "all data" warrants are just being honest: when an officer seizes a hard drive and carries it from a house, his hands hold not only a hard drive, but all data written upon it. From a subcontainer perspective, however, "all data" warrants are anathema, because storage media contain several compartments of privacy and warrants must specify which can be invaded.[93] Thus, warrants authorizing the "seizure" of all data on a hard drive are called "general" or "overbroad," analogous to warrants calling for every object in a home.[94] In response, some law enforcement officers weigh down their search warrant affidavits

[91] United States v. Gourde, 440 F.3d 1065, 1077 (9th Cir 2006) (Kleinfeld, J., dissenting).

[92] *See, e.g.*, United States v. Kim, 677 F. Supp. 2d 930, 949-50 (S.D. Tex. 2009).

[93] *See, e.g.*, United States v. Burgess, 576 F.3d 1078, 1091 (10th Cir. 2009) ("If the warrant is read to allow a search of all computer records without description or limitation it would not meet the Fourth Amendment's particularity requirement."); Kerr, *supra* note 20, at 127 ("[A]gents should be required to describe the property to be seized at both the physical search stage and the electronic search stage.").

[94] *See, e.g.*, United States v. Rosa, 626 F.3d 56, 61-62 (2d Cir. 2010); United States v. Otero, 563 F.3d 1127 (10th Cir. 2009); United States v. Riccardi, 405 F.3d 852 (10th Cir. 2005); United States v. Fleet Management Ltd., 521 F. Supp. 2d 436, 443 (E.D. Pa. 2007).

with boilerplate.[95] Other officers—particularly those who do not have access to training in the law of computer forensics, or are compelled to draft warrants quickly—find the subcontainer perspective to be an unpleasant surprise. One case involved a warrant prepared by an investigator who learned at 2:00 a.m. of ongoing child exploitation and had a search warrant signed by 4:10 a.m.[96] The court faulted the resulting warrant for failing to particularize the data to be taken from storage media.[97]

The "all data" cases are the most prominent result of translating the particularity clause from the subcontainer perspective. They make up most of the cases in which courts have suppressed evidence from storage media. When warrants meet the particularity requirement, in practice courts rarely suppress evidence solely because of the forensic examiner's conduct. As discussed below, this is because courts employing the subcontainer perspective are forced to make compromises to avoid crippling forensic examination.

2. Search limitations and United States v. Carey

Some of the first writers confronting computer forensics played with the notion of using computer programs to limit examiners' work—requiring examiners to look at only certain file types (for example, just files with a Microsoft Word .doc suffix) or only files with a certain keyword inside.[98] Essentially, the idea was to trust a computer program, not a human, to sift through the mass of intermingled data and extract only the things listed on the warrant. That way, other humans would never see embarrassing but irrelevant materials. But, computer forensics is not so easy. Affiants with technological knowledge now routinely swear that automated

---

[95] *See, e.g.*, United States v. Mitchell, 565 F.3d 1347, 1349-50 (11th Cir. 2009) (describing a 23-page-long affidavit that contained less than three pages of "original content," the rest boilerplate); United States v. Comprehensive Drug Testing, Inc., 513 F.3d 1085, 1132-33 (9th Cir. 2008) (Thomas J., concurring in part and dissenting in part) (quoting extensive boilerplate language discussing computer forensic challenges).

[96] *See Rosa,* 626 F.3d at 58.

[97] *See id.* at 61-62.

[98] *See* Raphael Winick, *Searches and Seizures of Computers and Computer Data,* 8 HARV J.L. & TECH. 75, 108 (1994) ("Whenever possible, key word searches should be used to distinguish files that fall within the scope of a warrant[.]"); United States v. Carey, 172 F.3d 1268, 1275-76 (10th Cir. 1999) (citing Winick); *In re* Search of 3817 W. West End, First Floor Chicago, Illinois 60621, 321 F. Supp. 2d 953, 959 (N.D. Ill. 2004).

techniques, alone, will often be insufficient.[99] Clocks can be wrong, dates can be changed, filenames intentionally misnamed.[100] Keyword searches are an important tool, but they are imperfect. They will not catch unanticipated wording, an egregious misspelling, an unexpected foreign language, recently invented slang, or pictures of documents.[101]

Even if software were up to the task, these attempts to limit forensic examination would still miss the point. Computer forensics cannot be mechanized, because forensics is detective work. Like all detective work, it involves applying background knowledge, intuition, and professional judgment. It is a mistake to conceptualize forensics solely as "seizing" or isolating files. When properly done, computer forensics integrates facts from the examination with facts from the rest of the case, building a coherent story about the defendant's conduct. This is iterative; knowledge about the case informs what to seek on the computer, and data from the computer contributes to knowledge about the case. For example, in isolation, the fact that a suspect downloaded tide tables for a particular beach in Oregon at 5 a.m. might mean nothing. But, when combined with the fact that a young woman's body was discovered in the surf on that beach an hour and a half later, an examiner can appreciate that download's importance.[102]

Therefore, humans must do computer forensics, and humans will likely see private evidence not called for by the warrant. That leaves the hope that courts can police how examiners do their jobs.

---

[99]A model search warrant affidavit published by the Department of Justice, for example, states that "[c]riminals can mislabel or hide files and directories, encode communications to avoid using key words, attempt to delete files to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require . . . more extensive searches, such as . . . perus[ing] every file briefly to determine whether it falls within the scope of the warrant." U.S. Dept. of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence*, *available at* http://www.cybercrime.gov/ssmanual/06ssma.html#AppF.

[100]*See* United States v. Burgess, 576 F.3d 1078, 1093 (10th Cir. 2009) ("It is unrealistic to expect a warrant to prospectively restrict the scope of a search by directory, filename or extension or to attempt to structure search methods—that process must remain dynamic.").

[101]*See, e.g.*, United States v. Evanson, No. 2:05-CR-805-TC, 2007 WL 4299191, at *5 (D. Utah Dec. 5, 2007) (noting that in the search at issue some files "were in 'tiff' format," a "'digital picture of a hard copy document' that has been scanned," and that these files "had numbers as file names, rather than recognizable file names that purportedly described the data in the files"); *Burgess*, 576 F.3d at 1093 ("[I]f the text was an embedded graphic (rather than embedded text) it might not be revealed even in a word search of the entire document.").

[102] State v. Johnson, 131 P.3d 173, 176, 178 (Or. 2006).

The most notable effort was *United States v. Carey*,[103] where, for the first time, a federal circuit court held computer evidence should be suppressed entirely because of the forensic examiner's conduct. In *Carey*, the warrant was for drug evidence; this included image files, because they, too, could be evidence of drug trafficking.[104] While looking through photos on a computer storage medium, the examiner found child pornography.[105] He decided to look for more. Because the court found that the examiner "knew he was expanding the scope of his search," it held the Fourth Amendment required suppression.[106]

Thus, in *Carey,* the Tenth Circuit faulted an examiner for his subjective intent—for *wanting* to find child pornography with a non-child-pornography warrant.[107] This subjective approach was *Carey*'s chief innovation, and also its most prominent defect.[108] Notably, the *Carey* court did not dispute that the examiner had the right to look for evidence of drug offenses in image files.[109] To find them, he had to look at all photos, to see which were evidence of drug offenses. That means he was in a position to see other photos that might show other crimes. The court in *Carey* was able to criticize the examiner only because (it found) he admitted during a suppression hearing that his intent changed from looking for trophy photos to looking for child pornography.[110] The *Carey* court based its holding on this subjective criterion, apparently using it to reject the government's plain view argument.[111]

---

[103]United States v. Carey, 172 F.3d 1268 (10th Cir. 1999).
[104] *Id.* at 1270-71.
[105] *Id.* at 1271.
[106] *Id.* at 1273.
[107] *Id.* ("Detective Lewis made clear as he opened each of the JPG files he was not looking for evidence of drug trafficking. He had temporarily abandoned that search to look for more child pornography[.]").
[108] The Fourth Circuit, for example, rejected *Carey* in part because it "cannot stand against the principle, well-established in Supreme Court jurisprudence, that the scope of a search conducted pursuant to a warrant is defined *objectively* by the terms of the warrant and the evidence sought, not by the *subjective* motivations of an officer." United States v. Williams, 592 F.3d 511, 522 (4th Cir. 2010).
[109] *See Carey,* 172 F.3d at 1270 n.2 (crediting testimony that "image files could contain evidence pertinent to a drug investigation such as pictures of 'a hydroponic growth system and how it's set up to operate'").
[110] *Id.* at 1273 ("[B]ecause of the officer's own admission . . . he expected to find child pornography and not material related to drugs. . . . Under these circumstances, we cannot say the contents of each of those files were inadvertently discovered.").
[111] *Id.* at 1277 ("[T]he fact that Detective Lewis did not inadvertently come across the pornographic files is certainly relevant to our inquiry.").

Carey now enjoys the peculiar status of being one of the most-cited and least-followed computer examination cases.[112] Reported cases where courts suppressed evidence solely because of the forensic examiner's conduct in executing a warrant are rare. In theory, policing an examiner's motives is attractive; in practice, it is impossible. The Tenth Circuit has repeatedly distanced itself from *Carey*'s odd subjective-intent framework, reducing it to a mere caution against changing the search's "justification," not its purpose.[113] The Tenth Circuit's subjective experiment ended with a whimper in *United States v. Burgess*.[114] The facts of *Burgess* were similar to *Carey*: once again, the warrant was for drug evidence, and, once again, the officer found child pornography while looking for that evidence.[115] But, ten years after *Carey*, the Tenth Circuit acknowledged that it was "unrealistic" to restrict searches "by directory, filename, or extension" and also that "search methods" are a "process" that "must remain dynamic."[116] While holding that an officer might be required to "progressively move from the obvious to the obscure," the Tenth Circuit now acknowledges that "in the end, there may be no practical substitute for actually looking in many (perhaps all) folders and sometimes at the documents contained within those folders."[117]

3. The haystack problem and "necessary over-seizure"

Carey illustrates a recurring problem with the subcontainer perspective: the haystack problem. Searching for electronic evidence is like looking for needles in a haystack. If an officer looks for a needle in a haystack, he must look at a lot of hay. Worse, if he doesn't

---

[112] *See, e.g.*, United States v. Stabile, 633 F.3d 219, 240 (3d Cir. 2011) (finding an examiner's testimony that "he knew that there *may* have been child pornography" irrelevant "because an investigator's subjective intent is not relevant to whether a search falls within the scope of a search warrant"); *Williams*, 592 F.3d at 522; United States v. Mann, 592 F.3d 779, 784 (7th Cir. 2010) ("[I]ntent is not generally relevant when assessing whether a given search falls within the scope of the warrant[.]").

[113] *See* United States v. Grimmett, 439 F.3d 1263, 1268 (10th Cir. 2006) ("*Carey* . . . simply stands for the proposition that law enforcement may not expand the scope of a search beyond its original justification."); United States v. Brooks, 427 F.3d 1246, 1251 (10th Cir. 2005) ("[W]e have not required a specific prior authorization along the lines suggested in *Carey* in every computer search[.]").

[114] *See* United States v. Burgess, 576 F.3d 1078, 1084 (10th Cir. 2009).

[115] *Id.* at 1083-84.

[116] *Id.* at 1093.

[117] *Id.* at 1094.

know how many needles there are, but must find all of them, then he must look through *all* the hay.

The haystack becomes an even bigger problem when the examiner looks for a *lack* of evidence. Sometimes the crucial evidence is "the dog that did not bark." The phrase comes from a Sherlock Holmes story in which Holmes deduces from a dog's failure to bark the conclusion that an intruder was the dog's master.[118] Thus, "the dog that did not bark" evidence is negative evidence—the *absence* of evidence that would be present if something happened, thus suggesting it did not happen. If a defendant claims he is innocent because a computer virus committed the crime, the absence of a virus on his hard drive is "dog that did not bark" negative evidence that disproves his story. If a defendant claimed he sent an e-mail but it cannot be found on his hard drive, that absence is also "dog that did not bark" negative evidence. To prove something is not on a hard drive, it is necessary to look at every place on the drive where it might be found and confirm it is not there.[119]

When the haystack problem collides with the subcontainer perspective, a court must either fatally hobble computer forensics by taking seriously the notion that each file is private, or make compromises. Thus far, courts have chosen to make compromises. Every circuit court to consider the haystack problem—now including the Tenth Circuit, home of *Carey*—has rejected limitations on which files may be examined. They permit human forensic examiners to look at every file, albeit briefly, to determine whether it is in the warrant's scope.[120]

---

[118] ARTHUR CONAN DOYLE, *The Adventure of Silver Blaze*, *in* MEMOIRS OF SHERLOCK HOLMES 22 (1894).

[119] *Cf.* United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1176 (9th Cir. 2010) ("By necessity, government efforts to locate particular files will require examining a great many other files to exclude the possibility that the sought-after data are concealed there.").

[120] *See, e.g.*, United States v. Williams, 592 F.3d 511, 521 (4th Cir. 2010) ("[T]he warrant impliedly authorized officers to open each file on the computer and view its contents, at least cursorily, to determine whether the file fell within the scope of the warrant's authorization."); United States v. Mann, 592 F.3d 779, 782-84 (7th Cir. 2010); *Burgess*, 576 F.3d at 1094; United States v. Khanani, 502 F.3d 1281, 1290 (11th Cir. 2007) (endorsing a search in which "a computer examiner eliminated files that were unlikely to contain material within the warrants' scope"); United States v. Brooks, 427 F.3d 1246, 1251-53 (10th Cir. 2005) (approving "a warrant that authorized officers to search through computer files for particular items specifically related to child pornography"); Guest v. Leis, 255 F.3d 325, 335 (6th Cir. 2001) (law

That legal rule brings us to a second compromise. How, exactly, did the officer get to have access to every file on the storage medium in the first place? Though the definition of "seize" under the subcontainer perspective remains controversial, possibilities include copying data, freezing it, or exposing it to human senses. Under all but the last of these definitions, when officers seize or copy an entire storage medium, they also seize all the subcontainers on that hard drive. But the officers lacked authority to seize all those subcontainers. So, unless the computer was itself a seizable instrumentality,[121] a massive over-seizure occurred. Defendants have protested that seizing or copying an entire storage medium is an over-seizure contrary to the warrant and the Fourth Amendment.[122] If the defendant's diary, for example, was not called for by the warrant, but was among the data carried out the door when officers seized the defendant's computer, then the diary's "seizure" seems inappropriate.

enforcement officers "may legitimately have checked to see that the contents of the directories corresponded to the labels placed on the directories"); United States v. Kernell, No. 3:08-CR-142, 2010 WL 1491873 (E.D. Tenn. Mar. 31, 2010) (search warrant properly authorized the executing agents to search through all of the files in the computer while searching for the items to be seized); United States v. Jack, No. CR.S-07-0266 FCD, 2009 WL 453051, at *4 (E.D. Cal. Feb. 23, 2009) ("[I]t is reasonable for the executing officers to open the various types of files located in the computer's hard drive in order to determine whether they contain such evidence."); United States v. Fumo, 565 F. Supp. 2d 638, 649 (E.D. Pa. 2008) ("[B]ecause of the nature of computer files, the government may legally open and briefly examine each file when searching a computer pursuant to a valid warrant."); Manno v. Christie, Civil No. 08-3254 (RBK), 2008 WL 4058016 (D. N.J. Aug. 22, 2008) ("It [was therefore] reasonable for [agent] to briefly review each electronic document to determine if it is among the materials authorized by the warrant, just as he could if the search was only of paper files."); United States v. Potts, 559 F. Supp. 2d 1162, 1176 (D. Kan. 2008) (warrant did not authorize an overbroad search when it allowed the investigator "to search the computer by . . . opening or cursorily reviewing the first few 'pages' of such files in order to determine the precise content" (internal quotation marks omitted)); United States v. Triumph Capital Group, Inc., 211 F.R.D. 31, 47 (D. Conn. 2002).

[121]*See* Davis v. Gracey, 111 F.3d 1472, 1480 (10th Cir. 1997) (holding that if "the probable cause supporting the seizure of the computer/container related to the function of the computer equipment," then the equipment may be seized as an "instrumentality of the crime").

[122]*See, e.g.*, United States v. Stabile, 633 F.3d 219, 233 (3d Cir. 2011) ("Stabile notes that by seizing six entire hard drives, the Government also seized personal emails and other information not related to financial crimes."); United States v. Hill, 459 F.3d 966, 974 (9th Cir. 2006); *see* Hofmann, *supra* note 20, at 22 (recommending that defense counsel "[a]rgue that imaging a hard drive is a seizure for Fourth Amendment purposes").

Courts applying the subcontainer perspective have an answer: seizing the storage medium is an over-seizure, but it is the "necessary over-seizing of evidence."[123] It is "necessary" because there is no other way for law enforcement to copy a drive; an officer cannot saw off hard drive chunks.

The "necessary over-seizing of evidence" construct hints at another hesitation to take seriously the implications of treating files as independent Fourth Amendment "things." It suggests that officers may seize these "things" without probable cause, do so on a massive scale, and do so as a matter of course. Either these are not truly "things," or the subcontainer perspective requires yet another compromise, one that weakens warrants' role in restricting seizures. It is true that the officer generally has no choice but to copy or physically seize all data; on-site examination would take so long that the officer's continued presence on the premises would itself be unreasonable.[124] But why should that inability to investigate without over-seizing render the over-seizure acceptably "necessary?" Dragnet arrests might be the only way to investigate a rape when all the police know about the rapist is his fingerprints and skin color. However, such dragnet arrests are not constitutionally acceptable "necessary over-seizings" of persons.[125] Ordinarily, over-seizures pass through the narrow reasonableness exception only after a thorough case-by-case factual analysis. Filing cabinet cases, for example, also involve over-seizure, but courts subject them to fact-intensive scrutiny, turning on things such as how well the file cabinets were organized.[126] Here, the rule is categorical.

4. "Plain view" under the subcontainer perspective

The subcontainer perspective, then, does not meaningfully limit what is copied or the places on the hard drive where an examiner

---

[123] *Comprehensive Drug Testing*, 621 F.3d at 1180 (Kozinski, C.J., concurring).

[124] *Hill*, 459 F.3d at 975 ("If the search took hours or days, the intrusion would continue for that entire period, compromising the Fourth Amendment value of making police searches as brief and non-intrusive as possible.").

[125] *See* Davis v. Mississippi, 394 U.S. 721 (1969) (holding unconstitutional the warrantless arrest and fingerprinting of a defendant who was one of dozens of African-American men swept up in a dragnet arrest after a reported sexual assault).

[126] *See, e.g.*, United States v. Hargus, 128 F.3d 1358, 1363 (10th Cir. 1997) (permitting seizure of file cabinets when responsive "records were present in every drawer of both file cabinets"); United States v. Tamura, 694 F.2d 591, 595 (9th Cir. 1982) (permitting court-supervised review in "the comparatively rare instances where documents are so intermingled that they cannot feasibly be sorted on site").

may "look." As the Tenth Circuit acknowledged in *Burgess*, the result is "only the illusion of protecting privacy interests, particularly when the search target is image files."[127] That leaves only the normative hope that the subcontainer perspective could limit the evidence ultimately used in court.

This hope is only partly, and poorly, fulfilled. In "transferring" Fourth Amendment principles to the computer context, an unwelcome guest came along: plain view. The plain view doctrine is an exception to the Fourth Amendment's warrant requirement. It holds that when an officer is lawfully in a place from which an object can be plainly seen and the object's incriminating character is immediately apparent, the officer may seize the object without a warrant.[128] When applied from the subcontainer perspective, plain view means that when an examiner sees a file whose incriminating character is immediately apparent, he may "seize" it despite the warrant's limitations. When combined with the need to look at every file, plain view allows every incriminating file to be used as evidence, so long as its incriminating character is immediately apparent—which it often will be, especially if the file is a child pornography image or movie.

These files can be "seized" immediately, but more often the examiner will obtain a second warrant.[129] Under the subcontainer perspective, a warrant authorizes only some files' seizure. In practice, this means that when examiners find incriminating evidence that is not obviously within the warrant, they freeze. Some are trained to seek a new warrant, even if only out of an abundance of caution.[130]

This second warrant is odd: it does not authorize searching any premises, and does not authorize seizing any object. Formally, it authorizes the officer to search for new things on the same hard drive. Practically, it simply lets the officer examine evidence that he already has, so that he can read what he has already read. Potentially, he

[127]United States v. Burgess, 576 F.3d 1078, 1095 (10th Cir. 2009).
[128]*See* Horton v. California, 496 U.S. 128, 136-37 (1990).
[129]*See, e.g.*, *Burgess*, 576 F.3d at 1094-95 (finding no Fourth Amendment violation in part because the examiner, upon finding unexpected child pornography, "immediately closed the gallery view when he observed a possible criminal violation outside the scope of the warrant's search authorization and did not renew the search until he obtained a new warrant").
[130]*See, e.g.*, *id.* at 1084 (noting that a forensic examiner searching for drug evidence, upon finding one child pornography image, "immediately closed the preview program and secured a new warrant authorizing a search for evidence of child sexual exploitation").

might also read something new, and seize that as well. The second warrant does not change what can be examined, only what can be used for evidence. The probable cause affidavit for the second warrant is usually a slam-dunk; essentially, it reads: "I saw child pornography on that hard drive; therefore, I submit there is probable cause to believe there is child pornography on that hard drive." The requirement to obtain such a slam-dunk warrant is an empty formality and a trap for the unwary. Officers who do not apply for these second warrants generally do not know that the law requires one.[131]

Plain view counters efforts to minimize evidence obtained from storage media. For example, in *United States v. Westerlund*,[132] a child pornography case, the search warrant affidavit provided probable cause to believe the defendant had provided alcohol to minors, but its only facts connecting the defendant to child pornography were stale. Nonetheless, the court did not suppress the child pornography found on the computer, because "[t]he photographs were discovered in plain view within the proper scope of the search for evidence of the crime of providing intoxicants to minors."[133]

So, the predominant way of transferring Fourth Amendment concepts to subcontainers allows the government to examine the entire storage medium and use anything on it, so long as the government complies with empty formalities. It produces burdensome rules that provide the "illusion of protecting privacy interests"[134] by generally requiring only slam-dunk but time-consuming warrants. As a price for that result, the subcontainer perspective condones the "over-seizure" of every file on a medium—an ironic outcome for a perspective many favor for its promise to treat each file as its own self-contained space.

E. Discomfort, disappointment, and departures from "translation"

Given a legal regime that permits extensive forensic analysis in most every case, it is not surprising to find a palpable discomfort with computer forensics. "Just as a conscientious public official may be

---

[131]In one of the few reported cases where a magistrate judge refused to issue such a second warrant, the magistrate judge's probable cause determination was almost certainly wrong. In *United States v. Kim*, 677 F. Supp. 2d 930 (S.D. Tex. 2009), a magistrate refused to issue a second warrant for child pornography even though the affidavit established that files had names "'ForbiddenFruit,' 'Illegal_ Loli# ,' 'Loli# ,' and other similar names." *Id.* at 934.

[132]No. 1:09-CR-154, 2009 WL 3711555 (W.D. Mich. Nov. 4, 2009).

[133]*Id.* at *4.

[134]*Burgess*, 576 F.3d at 1095.

hounded out of office because a party guest found a homosexual magazine when she went to the bathroom at his house, people's lives may be ruined because of legal but embarrassing materials found on their computers," writes Judge Kleinfeld of the Ninth Circuit.[135] "Let's take everything back to the lab, have a good look around and see what we might stumble upon," the Ninth Circuit wrote, facetiously, in a per curiam and en banc *CDT* opinion.[136] Commentators, meanwhile, complain that allowing the government to copy an entire drive and keep the copy indefinitely sounds "Orwellian—and downright creepy."[137] Although some insist that traditional Fourth Amendment rules should apply to computer forensics,[138] others question whether all of those rules make sense in the subcontainer perspective's virtual world.

From the resulting unease, two notable trends have arisen.

A first trend is worry about the plain view "problem," namely, the "problem" that law enforcement must be allowed to look at everything even though warrants specify only a few things.[139] Many commentators call for barring or limiting plain view's application to computer forensics.[140] Others, while stopping short of endorsing plain view's abolition, have argued that, given an internal (subcontainer) view of a hard drive as a virtual world full of data without visible boundaries, the Supreme Court's physical justifications for the plain view rule cease to make sense, and therefore plain view should not have been translated in the first place.[141] The Ninth Circuit, at one point, encouraged magistrates to obtain from officers a promise to

[135]United States v. Gourde, 440 F.3d 1065, 1078 (9th Cir 2006) (en banc) (Kleinfeld, J., dissenting).
[136]United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1171 (9th Cir. 2010).
[137]Kerr, *supra* note 6, at 560.
[138]*See* Clancy, *supra* note 25, at 262.
[139]*See, e.g.*, Andrew Vahid Moshirnia, Note, *Separating Hard Fact From Hard Drive: A Solution for Plain View Doctrine in the Digital Domain,* 23 HARV. J. L. & TECH. 609, 622 (2010); Trepel, *supra* note 20, at 120; McLain, *supra* note 20, at 1071; Jekot, *supra* note 20, at 2.
[140]*See, e.g.*, Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues,* 8 MICH. TELECOMM. TECH. L. REV. 39, 97-98 (2002).
[141]*See, e.g.*, Kerr, *supra* note 6, at 535, 583 ("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."); United States v. Comprehensive Drug Testing, Inc., 513 F.3d 1085, 1146 (9th Cir. 2008) (Thomas J., concurring in part and dissenting in part).

"forswear" plain view, although it later withdrew that guidance.[142] Practically, this would mean that when an officer examines a hard drive pursuant to a warrant, he may only "seize" evidence that the warrant specifies. If he finds other evidence, he cannot use it in a prosecution, examine it further, or use it in a new probable cause affidavit.

A second trend involves more innovation. In the last decade some magistrate judges began attaching to computer search warrants conditions and protocols that instructed officers how they may conduct the premises search and subsequent forensic exam.[143] Some specify the steps officers must take before they may determine whether they are permitted to physically seize a computer, some require that the computer be examined within a specified time after seizure, and some try to restrict search techniques. Most prominently, the Ninth Circuit, in *CDT,* dabbled for about a year with imposing new procedures governing search and seizure.[144] Under them, magistrates would have been required to either review data themselves or order the government to "forswear" plain view and review media through a filter team—a team of redactors who would review all the evidence, give the case agents only what the warrant specifies, and then never again work on the case or otherwise act upon what they have learned.[145]

Both these trends are controversial, even if one adopts the subcontainer perspective.[146] But I do not bring them up to criticize

---

[142] *See* United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 998 (9th Cir. 2009) ("[T]he government should, in future warrant applications, forswear reliance on the plain view doctrine or any similar doctrine that would allow it to retain data to which it has gained access only because it was required to segregate seizable from non-seizable data."), *withdrawn and superseded*, 621 F.3d 1162 (9th Cir. 2010).

[143] *See, e.g.*, United States v. Potts, 586 F.3d 823, 827 (10th Cir. 2009); *In re* Search of 3817 W. West End, 321 F. Supp. 2d at 960-63.

[144] *See Comprehensive Drug Testing*, 579 F.3d at 998-1001, 1004-07, *withdrawn and superseded*, 621 F.3d 1162 (9th Cir. 2010); *but see id.*, 621 F.3d at 1178 (Kozinski, C.J., concurring) (describing the procedures, in a concurring opinion, as a non-mandatory "safe harbor").

[145] *See supra* note 142.

[146] *See* Brief of the United States in Support of Rehearing En Banc by the Full Court in *United States v. Comprehensive Drug Testing*, *available at* http://www.wired.com/images_blogs/threatlevel/2009/11/kagan.pdf (Nov. 23, 2009) (criticizing barring plain view and requiring search protocols); United States v. Farlow, No. CR-09-38-B-W, 2009 WL 4728690, at *6 n.3 (D. Me. Dec. 3, 2009) (comparing barring plain view to "demanding that a DEA investigative team engaged in the search of a residence for drugs promise to ignore screams from a

them. Instead, I have discussed these trends because their existence demonstrates, again, the subcontainer perspective's poor fit to rules governing search and seizure generally.

Both these trends are computer-specific innovations—abandoning the original plan to translate physical world rules to computer forensics in a way that "preserve[s] the function of existing law in light of new facts."[147] Few would claim that the Fourth Amendment requires abandoning plain view in non-computer contexts.[148] As for search protocols, they are essentially lawless. When non-judges endorse protocols, they generally endorse them as policy choices, only.[149] Judges who endorse protocols seem to fashion protocols based on their own experiences and policy preferences. They vary depending on who writes the protocol; some protocols have time limits for the examination, some limit forensic techniques, and some require on-scene forensics. One reported protocol prohibited "a search of any kind of unopened electronic mail."[150] The variation in protocols does not spring from different legal conclusions. In fact, judges seldom attempt to persuade that any legal authorities require their particular flavor of protocol. *CDT,* for example, stands as the most prominent and eloquent call for search protocols. Yet, the now-withdrawn *CDT* majority opinion cited no authority at all.[151]

Both these innovations make sense only from the subcontainer perspective: they begin with the assumption officers with warrants should preserve some subcontainers' privacy and invade others. Discussing whether a particular file is in "plain view," for example, is

---

closet or a victim tied to a chair"); Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure,* 96 VA. L. REV. 1241, 1242 (2010) ("[E]x ante restrictions on the execution of computer warrants are constitutionally unauthorized and unwise. The Fourth Amendment does not permit judges to impose limits on the execution of warrants in the name of reasonableness. When such limits are imposed, they have no legal effect.").

[147] Kerr, *supra* note 6, at 533.

[148] An exception is Chief Judge Kozinski, who both wrote the now-superseded majority opinion in *Comprehensive Drug Testing*, 579 F.3d 989 (9th Cir. 2009), and also, in a non-precedential opinion, argued that "[p]lain view is killing the Fourth Amendment." United States v. Lemus, 596 F.3d 512, 516 (9th Cir. 2010) (Kozinski, C.J., dissenting from the denial of rehearing en banc).

[149] *See, e.g.*, Brenner & Frederiksen, *supra* note 140, at 74-82.

[150] United States v. Potts, 586 F.3d 823, 827 (10th Cir. 2009).

[151] *See Comprehensive Drug Testing*, 621 F.3d at 1178-80 (Kozinski, C.J., concurring) (setting forth guidance while citing no cases, other than as illustrations of possible scenarios).

meaningful only if one believes that each file enjoys a zone of privacy separate from the storage medium. A requirement that a filter team isolate evidence before investigators may see it makes sense only if one believes that evidence can be conceptually separated from the hard drive.

To review, the subcontainer perspective sees a virtual world lacking the physical world's privacy-defining boundaries. It was necessary to "transfer" and "translate" the Fourth Amendment's physical rules into that world. Yet, at least two of those rules (plain view and the traditional lack of ex ante restrictions on search methodology) are, many believe, lost in translation. Translating those two rules to the subcontainer perspective rolls the subcontainer perspective back into the physical perspective: the storage medium becomes a single unit, in practice incapable of meaningful subdivision. Thus, the temptation is strong to abandon the translation project and craft original rules uniquely suited to the virtual world—even though these new rules likely will not apply to any other type of object created by man.

Applying the Fourth Amendment to the virtual world has been a disappointment because the virtual world exists only from the subcontainer perspective. Search and seizure law, however, is thoroughly physical. The subcontainer perspective held out hope that we could meaningfully compartmentalize recorded data, permitting some to become evidence while keeping the rest private. But compartmentalizing data really means compartmentalizing the conclusions drawn from analyzing a physical object. That is inherently contradictory: while we can divide physical objects physically, dividing what we learn from them is a different story.

II. THE COMPUTER AS PHYSICAL EVIDENCE

A. Objects as evidence

The physical perspective treats a storage medium as a physical object, and applies to it the same search and seizure rules that apply to all other objects. So, what are those rules?

All evidence conveys information to the jury. Physical evidence is no exception. However, physical evidence usually requires testimony to explain an object's significance. Forensics derives information from objects and permits the examiner to give that explanatory testimony. Many objects become useful as evidence only when examined scientifically: a murderer's clothes might contain

fibers from the crime scene; a driver's blood might contain incriminating alcohol levels. Investigators can also learn information from objects using natural senses, case knowledge, and common intuition. Every object has the potential to disclose facts about people who owned it, kept it, touched it, used it, moved it, or were just near it. Suppose a store clerk reports that the man who robbed her wore blue jeans stained with battery acid, and police obtain a warrant that allows them to seize a single thing: the blue jeans. That one item reveals information that is irrelevant to the investigation, and is also perhaps quite private. Forget the possibility that anything is in the pockets. The blue jeans tell us the man's waist size and let us guess if he is overweight or not. The brand tells us that he shops at Wal-Mart. Grease near the cuffs suggests he has ridden a bicycle. The smell suggests he has been around tobacco smoke. A worn right pocket suggests he favors that hand.

To what extent does the Fourth Amendment prohibit police from examining physical objects, such as those blue jeans? When the objects are not recorded media, such as storage media or the motion picture film in *Walter*,[152] and so long as those objects come into law enforcement's possession lawfully, courts do not require additional Fourth Amendment justification before police subject them to examination.[153]

Blood is a good example of how courts treat physical evidence as objects, rather than containers of information. Like computer storage media, blood contains intermingled information, some irrelevant to an investigation. Examining a man's blood forensically can reveal whose blood it was, what he had been eating, what drugs or medicines he took, and, perhaps, whether he is sick. Yet, once officers lawfully seize blood, they may examine it without obtaining a warrant. In *United States v. Snyder*,[154] police took a blood sample from Snyder, without his consent, incident to a drunk driving arrest. Examining the blood forensically (two days later) proved Snyder was drunk. Snyder conceded that taking the blood was permissible under *Schmerber v. California*,[155] in which the Supreme Court upheld seizing blood incident to a drunk driving arrest. Instead, Snyder argued that

[152]Walter v. United States, 447 U.S. 649 (1980).
[153]*See infra* notes 154-172.
[154]United States v. Snyder, 852 F.2d 471, 474 (9th Cir. 1988) (Kozinski, J.).
[155]Schmerber v. California, 384 U.S. 757 (1966).

forensically examining his blood was a new, unwarranted search.[156] The Ninth Circuit called this reasoning "flaw[ed]," because it attempted to "divide" police conduct "into too many separate incidents, each to be given independent significance for fourth amendment purposes."[157] Instead, the court held, "the seizure and separate search of the blood [was] a single event for fourth amendment purposes."[158] The seizure and "search" of the blood were not really a single event because lab technicians examined Snyder's blood two days after his blood sample was drawn. Nonetheless, the court treated the seizure and examination as a single event "regardless of how promptly the test is conducted."[159]

Camera film is another example of courts treating an object and information derived from it as the same thing. In *State v. Petrone*, officers searched Petrone's residence with a warrant and seized film; they developed the film the next day.[160] The warrant specified "film," though, not photographs.[161] Petrone argued that warrant was sufficient to seize the film, but not to develop it and view the pictures.[162] The Wisconsin Supreme Court disagreed, reasoning that "[d]eveloping the film is simply a method of examining a lawfully seized object," no different from using "a magnifying glass to examine lawfully seized documents."[163] This "method of examining" was not a search separate from the one that brought the film into the officers' possession; rather, it was using "technological aids to assist them in determining whether items within the scope of the warrant were in fact evidence of the crime alleged."[164]

Fourth Amendment challenges to the examination of lawfully seized objects are rare. Normally, defendants do not only seek to suppress the results of a forensic examination; they instead seek to suppress the examined object, with the forensics being consequentially suppressed. However, in the few reported cases in which defendants

---

[156] *Snyder*, 852 F.2d at 473.
[157] *Id.*
[158] *Id.* at 474.
[159] *Id.*
[160] State v. Petrone, 468 N.W.2d 676, 678 (Wis. 1991).
[161] *Id.* at 678.
[162] *Id.* at 679.
[163] *Id.* at 681.
[164] *Id.*; *see also* People v. Patterson, 841 N.E.2d 889, 908 (Ill. 2005) ("[T]here was no need for the authorities to obtain a second warrant in order to develop and view the film seized from defendant's residence.").

sought to suppress examination results while conceding that the examined object's seizure was lawful, they failed. Blood and film are not special cases. The same rule—permitting officers to forensically examine lawfully seized objects—applies to clothing,[165] cars,[166] carpet fibers,[167] purses,[168] paper,[169] videotapes,[170] the defendant's hands,[171] and, it stands to reason, any other object. As the *Petrone* court put it, "A search warrant does not limit officers to naked-eye inspections of objects lawfully seized in the execution of a warrant."[172] Indeed, it is routine for physical evidence to be sent into jury rooms during deliberation; until the advent of the subcontainer perspective, it was never necessary to even consider whether a jury's ability to examine objects, play tapes, and watch films, all outside the court's supervision, might violate the Fourth Amendment.[173] Courts, in other words, treat

[165]*See* United States v. Edwards, 415 U.S. 800, 806 (1974) (search of clothing for paint chips held to be a lawful search incident to arrest); Clarke v. Neil, 427 F.2d 1322, 1325 (6th Cir. 1970) ("We do not consider the laboratory examination of a suit after its seizure by the police to constitute a search within the meaning of the Fourth Amendment[.]").

[166]People v. Superior Court, 59 Cal. Rptr. 3d 633, 642-43 (Ct. App. 2007) (holding analysis of seized car for fingerprints and biological evidence permissible, though warrant did not specify those things).

[167]State v. Pennell, 1989 WL 112555, at *11 (Del. Super. Sept. 12, 1989) (unpublished opinion).

[168]United States v. Guevera, 589 F. Supp. 760, 762 (E.D.N.Y. 1984) (finding that chemical examination of a previously seized purse for drugs did not require a warrant).

[169]Commonwealth v. Copenhefer, 587 A.2d 1353, 1356 (Pa. 1991) (noting in dicta that "a paper tablet, seized pursuant to a valid search warrant, may be subjected to scientific and physical manipulation and analysis without a second search warrant").

[170] State v. Munro, 124 P.3d 1221, 1225 (Or. 2005) ("Once the police seized the videotape under the authority of the warrant, any privacy interest that defendant had in the contents of the videotape was destroyed by the authority of the warrant permitting the examination and exhibition of the contents of the videotape.").

[171]United States v. Johnson, 445 F.3d 793, 795-96 (5th Cir. 2006) (upholding gun powder residue test performed on defendant's hands incident to lawful arrest); *id.* at 796 n.1 (citing cases upholding the collection of fingernail clippings and fingerprints).

[172]State v. Petrone, 468 N.W.2d 676, 681 (Wis. 1991).

[173] *See* United States v. Placensia, 352 F.3d 1157, 1164-65 (8th Cir. 2003); United States v. Grant, 52 F.3d 448, 449 (2d Cir. 1995) ("[T]he jury hears, watches, or reads the material for a second time outside the judge's presence."); Haniffy v. Gerry, Civil No. 08-cv-268-SM, 2010 WL 347037, at *8 (D. N.H. Jan. 26, 2010) ("Haniffy's cell phone was properly admitted into evidence. The jury was, therefore, entitled to examine it.").

most physical evidence from an external, physical perspective, and do not subdivide conceptually.[174]

Professor Kerr made perhaps the most direct criticism of the physical perspective when he rejected the "physical storage device approach" in part because "[c]omputers are searched to collect the information they contain"; therefore the emphasis should be "on that information rather than the physical storage device that happens to contain it."[175] But all physical evidence "contains" information; lawyers use physical evidence in the courtroom to convey that information. A jury usually learns information from physical evidence by hearing the testimony of someone who found it or examined it.[176] This courtroom presentation requires both a physical exhibit and testimony relating the information learned from the exhibit—or, one could say, relating the information "contained" in the exhibit. This is true for guns, drugs, and hard drives equally. Recall the earlier blue jeans example. By themselves, they are not useful as evidence in a trial against the robber. A prosecutor could wave them before the jury, but that would not establish that they had any more significance to the crime than a pair of jeans purchased at Wal-Mart the day before. But, the victim can examine them and testify that the jeans have the same

[174] The only exception appears to be private searches. The private search doctrine holds that the Fourth Amendment is inapplicable to a search and seizure done by a private individual not acting as a government agent; but once government agents come into possession of the seized item, they are not allowed to exceed the private search's scope. *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984); 1 WAYNE R. LAFAVE ET AL., SEARCH & SEIZURE § 1.8 (4th ed. 2009). As discussed earlier, the Supreme Court case *Walter v. United States*, 447 U.S. 649 (1980), discussed whether the "scope" of such a private search included projecting a motion picture film onto a screen. Similarly, in *United States v. Mulder*, 808 F.2d 1346, 1348 (9th Cir. 1987), the Ninth Circuit held that it was improper for officers to chemically test tablets because officers obtained the tablets through a private search, and the private searchers had not tested the tablets. However, the Fifth Circuit held that when a private searcher does look at a storage medium, that private search permits law enforcement to search the entire storage medium. *See* United States v. Runyan, 275 F.3d 449, 464 (5th Cir. 2001) (rejecting argument that "police exceeded the scope of the private search because they examined more files on each of the disks than did the private searchers").

[175] Kerr, *supra* note 6, at 556.

[176] *See* Michael S. Pardo, *Self-Incrimination and the Epistemology of Testimony,* 30 CARDOZO L. REV. 1023, 1041 (2008) ("With words . . . the fact-finder's knowledge would be dependent on the epistemic authority of the defendant; with blood . . . their knowledge would be dependent on either their own perceptions or on the epistemic authority of another person.").

distinctive stain as the one worn by the man who robbed her. Perhaps testimony from a forensic garment examiner could provide more evidence. The jeans, in other words, are also seized to collect information.

Saying that a hard drive "contains" information assumes an internal perspective. One could take a similar perspective towards any other object; the blue jeans mentioned earlier, for example, could be seen as containing information, with the conclusions about bicycle riding, smoking habits, weight, and fashion sense, each analogized to a separate closed subcontainer within the blue jeans. One could also say a page contains sentences, a tape recording contains syllables, or a doormat contains footprints. Consistent with this perspective, legal rules could require separate Fourth Amendment justifications for learning different facts from a single object. The law could require a warrant to analyze blood, one that specifies that the blood will be "searched" for alcohol only, not for controlled substances, and not for AIDS or other blood-borne diseases. The law could require a warrant before testing a joint chemically, one that specifies a test for tetrahydrocannabinol. The law could even require a warrant before an officer is allowed to read a notebook found in the arrestee's pocket.

As discussed above, the law does not require these warrants; rather, it adopts an external, physical perspective, and scrutinizes the seizure of objects, not information. There are good reasons why. All physical evidence contains information and groups that information physically, not conceptually. One cannot look only at the stain on the blue jeans (evidence of crime) without also noticing their brand (evidence of fashion preferences). So, lawyers must create conceptual subcontainers by drawing dividing lines inside physical evidence. But once drawn, those imaginary subcontainers will differ dramatically from the real, physical containers they are meant to imitate. When investigators examine objects, the available examination methods will not always allow them to stay within the imagined boundaries. Yet, the whole reason behind conceptualizing information as a subcontainer was to keep it contained. Confusion follows.

B. Introducing the physical computer

It is time to give the physical perspective another look. From the physical perspective, a hard drive is not a container of containers. It is an object. Data stored on a hard drive does not exist in a virtual world any more than data on a printed page exists in a "paper world." Computer data does not have independent physical existence. As the

California Supreme Court put it, "[T]here is no legal basis for distinguishing the contents of an item found upon an arrestee's person from either the seized item itself or the arrestee's actual person."[177]

This is a "physical" perspective because it treats data as physical changes made to storage media. This is not a conceptualization, but a technological reality. Data is stored by manipulating physical objects: regions on a hard drive platter are magnetized, photosensitive dye on a CD is darkened, and floating gates in flash memory have voltage applied to them. While reasonable people can disagree over the choice between a physical or subcontainer perspective, the ultimately physical nature of storage media should be beyond dispute.[178] From punch cards and magnetic drums to modern solid-state drives and optical disks, our technology permits us to record data only through physically altering objects.[179] Evidence from these computer storage media objects is, therefore, physical.

Amidst this world of magnetized regions and physical objects, what happened to the familiar landmarks that all computer users are familiar with, such as files and spreadsheet rows? Everything saved to a disk is data, and all data is physical. Files are groupings of data, organized by a plan set out in a file system. When a witness testifies that he found data on a hard drive, he means someone modified the storage medium physically to record that data. A witness might also testify about the foundations behind those conclusions: these magnetized regions represent a byte, these bytes a block, and these blocks a file. Ultimately, this is all inference from physical facts. Usually, these inferences are so uncontroversial that the witness does not bother stating them explicitly; nonetheless, the witness makes them.

Computers spare users these details by creating a user experience that expresses data graphically or audibly. Users do not really read, see, or hear files; they experience them. When a user "opens" a file, an application program translates the file into recognizable objects on the screen, or into sounds through a speaker. A spreadsheet, for example, is a user experience, generated by

---

[177] People v. Diaz, 244 P.3d 501, 510 (Cal. 2011) (internal quotation marks omitted).
[178] *But see* McLain, *supra* note 20, at 1071 ("[A]lthough computers can 'contain' evidence, unlike a traditional container, the evidence is not physical.").
[179] *See, e.g.*, Data Storage System, U.S. Patent No. 2,540,654, at 1-2 (issued Feb. 6, 1951) ("[T]he magnets 27 will be used to determine or create patterns of electrical values corresponding to digits or other code signals.").

software, using data read from a physical disk. When a forensic examiner opens a file, he approximates relevant aspects of the defendant's user experience.[180] That simulated experience permits the examiner to draw conclusions about what the physically recorded data was meant to represent. In court, the jury is rarely presented with raw bytes in a file; instead, a smart lawyer will create a user experience for the jury by presenting a screen shot or playing a movie or sound file. Nonetheless, the evidence is physical all along.

These user experiences are poor bases for Fourth Amendment rules. Courts strongly favor objective Fourth Amendment rules,[181] but user experiences are subjective: an Excel document opened on a defendant's netbook with a 10.1-inch screen may look quite different when opened on an examiner's Mac with a 27-inch widescreen display. Even a text file, when opened with Notepad on a computer running Windows, will present a different user experience when opened with Vim on a computer running Linux. This subjectivity undercuts legal rules that turn on the user experience—such as the view that the scope of permissible "plain view" seizures should be limited to what appears "on the first screen [the examiner] called up."[182] This user experience is also often incomplete, in that information saved in a file might not be displayed at all, or, like the infamous "metadata" that accompanies some files, might be tough to find.[183]

The experiences through which users perceive files on a disk also involve subjectivity. The Windows Explorer and Mac OS X Finder both display only those parts of a hard drive that a user might find helpful: files are displayed, but slack space is not; file modification dates are shown, but file system inode serial numbers are

---

[180] *See* United States v. Comprehensive Drug Testing, Inc., 513 F.3d 1085, 1146 (9th Cir. 2008) (Thomas J., concurring in part and dissenting in part) ("[E]xamination of computer data is a forensic exercise. It necessarily involves the application of software to interpret the data; without external software aid, the data would appear only as binary numbers.").

[181] *See* Brendlin v. California, 551 U.S. 249, 260 (2007) (citing cases).

[182] *Comprehensive Drug Testing*, 621 F.3d at 1180-81 (Bea, J., concurring and dissenting).

[183] *See* District of Columbia Bar Legal Ethics Committee, Opinion No. 341, *Review and Use of Metadata in Electronic Documents* (Sept. 2007) *available at* http://www.dcbar.org/for_lawyers/ethics/legal_ethics/opinions/opinion341.cfm ("Metadata is electronically stored information, typically not visible from the face of the document as printed out or as initially shown on the computer screen, but which is imbedded in the software and retrievable by various means.").

not. Examiners skip this watered-down experience and instead use specialized software (such as EnCase or FTK) that creates a user experience with more information about the physical storage medium.

C. Applying the Fourth Amendment to physical computers

Under the physical perspective, there is far less need for analogies. Storage media are not analogous to objects; they *are* objects, such as disks, RAM chips, flash memory cards, and cell phones. Data is recorded upon those objects, but data is not a separate thing. The terms "search," "seize," "place," and "thing" have their familiar physical meanings. Only premises, not media, are "places" that are "searched." Officers search the premises where storage media sit, and then officers might seize storage media—in that order.

Once a storage medium is lawfully in law enforcement's possession, a forensic examiner may study it to learn facts. From the subcontainer perspective, this forensic examination is an off-site search; from the physical perspective, it is not a search at all. From the physical perspective, a storage medium is examined, not searched.[184] When a computer forensic examiner works quietly in his fluorescent-lit government office, examining a copy of a copy of a defendant's hard drive, he is not intruding on any private premises. There is no confrontation between officer and citizen, no abrupt disruption in any person's right to be alone, and no danger that an officer will physically seize any property as evidence. His activity is like a search only in that he learns facts that he previously did not know. Merely learning facts is not a search: a blood alcohol test does not "search" blood, and developing camera film does not "search" the film.

The physical perspective frees an examiner from worrying about whether his next mouse click will violate the Bill of Rights. Storage media are not subdivided by file, by fact, or by anything else. Directories, files, partitions, user accounts, spreadsheet rows, and hard drives are neither "places" nor subcontainers. Information is learned, recorded, transmitted, communicated, appreciated, and sometimes forgotten, but information is not seized.[185] Data, files, e-mails,

---

[184] *See* People v. Diaz, 244 P.3d 501, 509 (Cal. 2011).

[185] *See* United States v. Hinojosa, 606 F.3d 875, 885 (6th Cir. 2010) ("The officers . . . did not violate Defendant's constitutional rights by *observing* the decor of his residence." (emphasis added)); United States v. Jackson, 131 F.3d 1105, 1108 (4th Cir. 1997) ("Viewing an article that is already in plain view does not involve an invasion of privacy and, consequently, does not constitute a search implicating the Fourth Amendment[.]"); Ohm, *supra* note 40, at 30-31 (reviewing how early wiretap cases suggested that intangible property could be seized, but concluding that "courts

pictures, deleted files, artifacts, logs, cell phone address books, and "dog that did not bark" negative evidence are not "things," but facts. They are not seized from storage mediums, but learned from them through examination.

The physical perspective also permits the straightforward application of existing search and seizure law. For example, when an agent seizes or images a hard drive, he does not "over-seize" all of the files on it. Because only physical things are seized, files are not seized or over-seized. If a forensic examiner learns of a new crime during his examination, reading or seeing or isolating that data is not a plain view seizure, or, indeed, a seizure at all. From the physical perspective, there is no plain view "problem," because plain view seizures simply do not happen: files are not things, are never in view (plain or otherwise), and are not seized.

Under the physical perspective, the key legal event is the storage medium's seizure. A storage medium's lawful seizure permits its lawful examination to the same extent that any other lawfully seized object can be examined. The same rules that apply to forensically testing any other object—blood, film, clothing, cars—also apply to storage media.

Whether a seizure occurs is, perhaps, the most difficult question for a lawyer working from the physical perspective. The most common scenario is easy to analyze: physically carrying a computer off a premises is a seizure. But, what about bringing blank storage media to a premises, copying a computer's hard drive, and leaving the original drive behind, intact and functional? What about operating a computer to display data on the screen, while making no copy other than the investigator's personal memory? What about viewing data the owner left on the screen, touching nothing?

From the physical perspective, the Fourth Amendment prohibits seizing storage media and computers in the same way that it prohibits seizing all other personal property. Under current law, "[a] 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property,"[186] or, stated another way, "a seizure deprives the individual

have found all of the following acts not to be a seizure: photographing the scene of the execution of a search warrant; photocopying several file cabinets worth of documents; and copying the VIN from a car").

[186]United States v. Jacobsen, 466 U.S. 109, 113 (1984).

of dominion over his or her person or property."[187] "Meaningful interference" with possessory interests includes more than the obvious case of taking property off the premises and putting it into an evidence locker. Merely physically manipulating an object can also seize it. In *Arizona v. Hicks*, for example, the Supreme Court held that merely moving an object so that an officer could read its serial number constituted a seizure of the object.[188]

Seizure rules require scrutiny of how law enforcement copies storage media. If, as is usually the case, making the copy requires physically manipulating a defendant's property, then that physical manipulation incident to the copying seized the defendant's storage medium.[189] Relying upon the "interference" definition of seizure, for example, the Eleventh Circuit concluded that disassembling a computer to access its hard drive "seized" the computer.[190] If disassembling a computer interferes with possessory interests, it is reasonable (though perhaps controversial) to conclude that touching the computer to operate it also meaningfully interferes with its owner's possessory interest.

The vast majority of reported computer forensics cases involve these unambiguous seizures of storage media, either through physical seizure or on-site copying. What about exotic cases, involving obtaining information from a computer without physical manipulation? The answer to this question depends on what "seize" means under the Fourth Amendment, and that question is independent from perspective choice. There is a debate about whether a possessory interest includes "control of the data itself, including any copies."[191] There is also a debate about whether defining seizure only in terms of

---

[187]United States v. Williams, 592 F.3d 511, 521 (4th Cir. 2010) ("[A] seizure deprives the individual of dominion over his or her person or property.") (quoting Horton v. California, 496 U.S. 128, 136-37 (1990)).

[188]Arizona v. Hicks, 480 U.S. 321, 325 (1987).

[189]*See* Ohm, *supra* note 40, at 33 ("[A]s *Hicks* exemplifies, we live in what I call an *atoms-before-bits* world. . . . [I]n order to copy the bits from a hard drive, the government must open the physical case of the computer containing the hard drive.").

[190]United States v. Mitchell, 565 F.3d 1347, 1350 (11th Cir. 2009) ("While the disassembling of the CPU did not constitute a search of a container in which Mitchell had a reasonable expectation of privacy, it did constitute an interference with his possessory interest.").

[191]*See* Kerr, *supra* note 78, at 705; *id.* at 724 ("Copying is a seizure when it interferes with the intended course of possession or transmission of data that has not been observed by government actors.").

"possessory" interests is too narrow.[192] The physical perspective is compatible even with an expansive seizure definition that includes "touchless" copying. Under the physical perspective, if an officer effects a "seizure" by remotely copying data, then the officer "seized" the storage medium that data came from. The physical perspective's only contribution to that debate is to clarify that the entire storage medium, not just some data, was seized.

III. THE PHYSICAL COMPUTER AND PUBLIC POLICY

There are compelling arguments for the subcontainer perspective. These arguments' strength comes from describing a seemingly undesirable result that would come from routinely authorizing officers to examine entire hard drives based on probable cause to believe that some small part of them is relevant. Some writers have even treated the physical perspective as the *absurdum* in a *reductio ad absurdum* argument.[193]

At some point, the debate between the subcontainer and physical perspectives becomes a public policy debate. The subcontainer perspective's best defense is not a legal argument that the Fourth Amendment requires special treatment for hard drives, but rather a policy argument that only the subcontainer perspective can promise to preserve some storage media privacy. Yet, as presently applied, the subcontainer perspective breaks that promise. Both the physical and subcontainer perspectives end up permitting law enforcement to examine every byte. The physical perspective arrives at that result directly, while the subcontainer perspective detours through the haystack problem and plain view. Even banning plain view or requiring magistrate-approved search protocols would not avoid a broad privacy invasion: examiners or filter teams will still

[192] *See* Ohm, *supra* note 40, at 59.

[193] *See, e.g.*, Recent Cases, United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989 (9th Cir. 2009) (en banc)*, 123 HARV. L. REV. 1003, 1008 (2010) (suggesting that if "the relevant unit of an electronic search is the entire hard drive of a computer" then the "physical analogue would be that a warrant for a gun would allow police to upend a suspect's entire house and seize absolutely anything that was immediately apparent evidence of a crime"); Moshirnia, *supra* note 139, at 622-23 ("[T]his approach could prove disastrous in the medical or corporate contexts because it is likely allow [sic] searches of individuals' private information that is only tenuously related to the criminal investigation."); Marc Palumbo, Note, *How Safe is Your Data?: Conceptualizing Hard Drives Under the Fourth Amendment,* 36 FORDHAM URB. L.J. 977, 1001 (2009) ("[A]ny distinction on the physical level is simply unworkable if individual privacy is to be adequately protected.").

invade privacy by seeing irrelevant information. Although the evidence would not be used in a prosecution, government agents would still see it, and that by itself would invade privacy. The subcontainer perspective provides only the "illusion" of privacy,[194] yet it demands burdensome formalities.

That is not the end of the subcontainer perspective, however. One can adopt the subcontainer perspective without arguing that physical search and seizure rules cleanly "translate" to the virtual world. Instead, one could argue that legislatures (or even courts) should require the subcontainer perspective as a policy matter and draft new rules just for computer "searches." That is what happened with wiretaps. After the Supreme Court took a rare departure from the external perspective and treated wiretaps as searches under the Fourth Amendment, the response was to enact a special-purpose procedural code for wiretaps, not to attempt to translate physical rules.[195]

I am skeptical that policy makers, even working from a blank slate, could rewrite search and seizure law from a subcontainer perspective without either compromising administrability or compromising privacy policy goals. Adopting those rules would mean deciding to treat storage media specially. Only storage media would be treated like miniature places-within-places, protected with an additional layer of Fourth Amendment protection; notebooks, scraps of paper, drugs, blood, film, and other physical objects would not.

Such a policy decision requires a justification. If courts use special, more restrictive rules for computer evidence than for all other evidence, that could have a disparate impact on some defendants. To generalize only slightly, many cases where computer evidence is crucial are child pornography cases;[196] traditional physical evidence plays a more prominent role in other crimes, especially drug crimes. Available statistics suggest that child pornography offenders are better educated and older than drug offenders; there is also a notable racial

[194] United States v. Burgess, 576 F.3d 1078, 1095 (10th Cir. 2009).

[195] *See* United States v. United States District Court, 407 U.S. 297, 302 (1972) ("Much of Title III was drawn to meet the constitutional requirements for electronic surveillance enunciated by this Court.").

[196] *See* Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today (PROTECT) Act, Pub.L. No. 108-21, § 501(6), 117 Stat. 650, 677 (2003) ("The vast majority of child pornography prosecutions today involve images contained on computer hard drives, computer disks, and/or related media.").

disparity.[197] Before giving electronic devices what one court called "preferred status,"[198] policy makers should demand a justification for why that status is preferred.[199]

Consider the argument that computer storage media should receive special treatment because they intermingle relevant information with a large amount of irrelevant and personal information. This is a policy argument. Even if one were to conceive of the Fourth Amendment as a mechanism to filter the "flow" of abstract "information . . . between individuals and the state,"[200] exactly how precisely that information flow should be filtered is a policy choice. The prevailing policy choice permits information to flow to the government in large intermingled chunks; specifically, in object- and premises-sized chunks. Arguing that those chunks of information should be broken into smaller pieces is a policy argument.

The intermingling argument is difficult to square with the policy choices that prevail over searches of premises. It is true that hard drives reflect many parts of peoples' lives. But criminal investigations occur in an intermingled world, and searches of all

---

[197]*See* United States Sentencing Commission, *Sourcebook of Federal Sentencing Statistics,* tbl. 4 (2009), *available at* http://www.ussc.gov/ANNRPT/2009/Table04.pdf (reporting that 26.2% of defendants sentenced for "Drugs-Trafficking" were white, while 85.4% of defendants sentenced for "Pornography/Prostitution" were white); *id.* at tbl. 8, *available at* http://www.ussc.gov/ANNRPT/2009/Table08.pdf (reporting that 2.5% of defendants sentenced for "Drugs-Trafficking" were college graduates, while 19.5% of defendants sentenced for "Pornography/Prostitution" were college graduates); *id.* at tbl 6 (age); National Center for Missing and Exploited Children, *Child-Pornography Possessors Arrested in Internet-Related Crimes*, *available at* http://www.missingkids.com/en_US/publications/NC144.pdf, at 15 ("Virtually all of the arrested CP possessors were men (Table 1). They were predominantly white (91%) and older than 25 (86%).").

[198]*Burgess*, 576 F.3d at 1090.

[199]*See* People v. Diaz, 244 P.3d 501, 508 (Cal. 2011) ("If, as the high court held in *Ross*, 'a traveler who carries a toothbrush and a few articles of clothing in a paper bag or knotted scarf [has] an equal right to conceal his possessions from official inspection as the sophisticated executive with the locked attaché case' . . . then travelers who carry sophisticated cell phones have no greater right to conceal personal information from official inspection than travelers who carry such information in 'small spatial container[s].'") (citing United States v. Ross, 456 U.S. 798, 822 (1982)); Clancy, *supra* note 25, at 216-17 ("The bankruptcy of an analytical structure based on distinguishing between types of containers soon became evident, at least to a plurality of the Court: it had no basis in the language of the Amendment[.]").

[200]Kerr, *supra* note 6, at 535.

kinds have always uncovered facts irrelevant to the investigation. For example, consider home searches. When an officer, armed with a warrant, enters a house or apartment and conducts a search, he can turn his head in any direction he chooses. He can see things in a room, remember that they are there, and later use that information in his investigation without having "seized" anything under the Fourth Amendment. The officer can open any container reasonably likely to contain something that he is authorized to seize,[201] so if he is searching for drugs or a small object, he can see, smell, and hear everything. Using intuition, he can turn this raw data into confident conclusions about the people who live there. There are cigarettes in the garage? The owner is probably a smoker, but might be trying to break the habit. There is medical equipment, a small twin bed, and children's toys all in one bedroom? The family probably has a chronically sick child. There are two sets of men's clothing, in different sizes and styles, but just one double bed? The residence is probably occupied by two gay men. Wall decorations reveal tastes in art, favorite pastimes, and memorable life events; book spines reveal literary interests; CDs reveal tastes in music; magazines reveal hobbies, political outlook, or tastes in pornography; papers on a desk show what the occupants were recently reading or writing; cupboards and refrigerators reveal dietary habits and nutrition; medicine cabinets reveal that the occupants suffer from depression, allergies, or hemorrhoid inflammation.

Most would agree that this is a terrifyingly vast body of private information exposed to law enforcement. Some will be relevant to the investigation: perhaps the information will confirm an alibi, or match a victim witness description. In one case, an officer's ability to recognize a room from a child pornography photograph proved to be crucial evidence that the photograph was taken in the defendant's home.[202] Most information learned from seeing a home's interior, however, will have no use in the investigation, and will not come close to being described in a warrant among things to be seized. Searches like this are not limited to homes or small spaces either; one warrant

[201] *See* 2 WAYNE R. LAFAVE ET AL., SEARCH & SEIZURE § 4.10(d) (4th ed. 2009).

[202] *See* United States v. Hinojosa, 606 F.3d 875, 884-85 (6th Cir. 2010) (finding the "officers' observations of the hardwood floors, bathroom tiling, and French doors" was not a "seizure" even though those observations were used to confirm that a child pornography photograph was taken in that home).

can authorize searching every building in a corporate campus, or a warehouse filled with paper files.[203]

Recall Judge Kleinfeld's complaint that "legal but embarrassing materials" found on a computer could humiliate a public official, humiliation equivalent to "a party guest [finding] a homosexual magazine when she went to the bathroom at his house."[204] Yet the Fourth Amendment authorizes officers with warrants to enter those bathrooms and find embarrassing items. The Fourth Amendment sharply limits an officer's opportunities to conduct such a search. However, once a search occurs, the prevailing public policy choice has been to tolerate this unpleasant cost to privacy and accept that the officer's intrusion into private affairs will usually exceed what was necessary for the investigation.

Computer searches threaten privacy about as much as home searches—that is, quite a bit. Yet, under prevailing public policy, homes are not subdivided into conceptual subcontainers based on what investigators can learn. Homes also are not protected by search protocols nor exempted from plain view. The law does not govern where an officer, conducting a lawful search, may turn his head; it governs whether his head gets to be in the premises at all. There is no reason to better protect a homeowner who moves his private information away from paper and onto a storage medium. To answer Judge Kleinfeld, protecting computers the same as bathrooms makes sense; but protecting them *more* does not.

A second argument for special treatment is that modern storage media do not merely intermingle information, but store information in very large quantities. Because computers hold "immense amounts of information," comparable to a library, some argue they require commensurately immense privacy protection.[205] This does not make

---

[203] *See, e.g.*, Affidavit and Application for Search Warrant, Case No. 08-MJ-110 (N.D. Iowa, May 9, 2008), *available at* http://www.eyeonagriprocessors.org/docs/Application and Affidavit for Search Warrant.PDF (authorizing the search of several buildings associated with a single corporation); United States v. Pelullo, 399 F.3d 197, 204 (3d Cir. 2005) ("[T]he FBI executed a search warrant for a 2400-square foot warehouse in Miami . . . . The FBI seized 904 boxes, 114 file cabinets, and 10 file cabinet drawers of corporate and financial records.").

[204] United States v. Gourde, 440 F.3d 1065, 1078 (9th Cir. 2006) (Kleinfeld, J., dissenting).

[205] *See, e.g.*, United States v. Payton, 573 F.3d 859, 861-62 (9th Cir. 2009) ("There is no question that computers are capable of storing immense amounts of information and often contain a great deal of private information. Searches of computers

sense as a legal argument, even from a subcontainer perspective. Fourth Amendment protections do not shrink and expand with the size of the premises or container. Someone who moves from a studio apartment into a mansion does not gain additional Fourth Amendment protection, even though the mansion could conceivably hold many more personal and sensitive items.

The capacity argument is better understood as a policy argument, one that argues that storage capacity presents a categorically different risk to privacy and therefore justifies special treatment. This argument misconceives the relationship between storage capacity and the privacy of information. Personal information can be found in even small containers.[206] This argument also confuses storage capacity with privacy. Hard drives have gotten bigger; private lives have not. Yes, a modern hard drive could hold a library's worth of data. But, the human capacity to write a library's worth of private information does not exist—the "library" on the average hard drive is stocked mostly with blank books, or, at least, books everyone has already read. The typical hard drive is mostly empty, with large portions of the rest taken up by operating system and program files. Identical copies of those files can be found on millions of other computers. These files could cover multiple gigabytes, but none of that information will be private, interesting, or even embarrassing. While hard drive capacity has grown, the consumer demand driving that growth has more to do with a need to store software, music, and video files than a need to store sensitive or private information. Finding ten downloaded Battlestar Galactica episodes on a defendant's hard drive will not reveal more private information than finding one downloaded episode.

A stronger argument is that the increase in how useful computers have become has led people to make more physical records of more of their private lives than they did previously. Computers' growing utility may well cause individuals to structure more of their

---

therefore often involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches of other containers."); United States v. Burgess, 576 F.3d 1078, 1090 (10th Cir. 2009) (speculating that storage media might have "preferred status because of their unique ability to hold vast amounts of diverse personal information"); Kerr, *supra* note 6, at 542 (comparing eighty gigabytes of storage to "forty million pages of text—about the amount of information contained in the books on one floor of a typical academic library").

[206] *See* People v. Diaz, 244 P.3d 501, 508 (Cal. 2011) ("Even 'small spatial container[s]' . . . that hold less information than cell phones may contain highly personal, intimate and private information, such as photographs, letters, or diaries.").

private lives around computer use, thus creating more physical evidence of what they do from hour to hour. It is not that private lives have grown larger; people communicated with friends and kept secrets before the invention of computers, too. It is that private lives have become more visible to computer forensic techniques. For example, a conversation that, decades ago, might have occurred face-to-face or over the telephone now might be carried out by computer. Unlike the telephone, the computer will likely leave behind physical evidence of what was said. One could well argue, as a public policy matter, that this suggests that there should be stricter limitations on computer forensics. However, computers' growing utility has an ambiguous affect on public policy arguments. Computers' increased utility has also meant an increase in threats to public safety. Child exploitation, in particular, has skyrocketed since the mid-1990s with the advent of the Internet and digital cameras.[207] Computers give criminals access to secret communication, relative anonymity, access to online communities of criminals, access to more victims, and new ways to evade law enforcement. Considered solely as a public policy question, this development might warrant no change in the balance between privacy and law enforcement needs; or, it might warrant a change in law enforcement's favor.

CONCLUSION

This article presented an argument about what the law should be, not what it is. The physical perspective should be the only perspective used when applying search and seizure rules to computer forensics. Practicing lawyers, unfortunately, must understand both the subcontainer and physical perspectives. Increasingly, the law of search and seizure reflects both. While the subcontainer perspective dominates court opinions discussing computers seized with search warrants, the physical perspective dominates the new "storage medium" rules in Rule 41, and also dominates the rest of search and seizure law.[208] This complicates the practitioner's job.

Fortunately, the brain can appreciate two mutually incompatible perspectives at once. When a person sees a painting, the brain on one hand recognizes the painting as a flat surface, while on the other hand recognizes that the painting depicts objects, albeit with

[207] *See* NATIONAL STRATEGY FOR CHILD EXPLOITATION PREVENTION AND INTERDICTION, *supra* note 1, at 11.

[208] *See supra* notes 35-41 and accompanying text.

contradictory spatial properties and relations.[209] The ability to simultaneously perceive wholly contradictory worldviews is, unfortunately, also a useful skill for practitioners applying the Fourth Amendment to computer forensics. Unaware of what perspective will ultimately apply, practitioners may need to perceive multiple potentially conflicting realities simultaneously, phrasing legal arguments that make sense when viewed from either perspective.

[209] *See* Rainer Mausfeld, *Conjoint Representations and the Mental Capacity for Multiple Simultaneous Perspectives*, *in* LOOKING INTO PICTURES: AN INTERDISCIPLINARY APPROACH TO PICTORIAL SPACE 27 (2003).