Fordham Urban Law Journal

Volume 36 | Number 5 Article 4

2009

How Safe is Your Data: Conceptualizing Hard Drives under the Fourth Amendment

Marc Palumbo
Fordham University School of Law

HOW SAFE IS YOUR DATA?: CONCEPTUALIZING HARD DRIVES UNDER THE FOURTH AMENDMENT

Marc Palumbo[*]

INTRODUCTION

In January 2009, Western Digital Corporation began shipment of the Caviar Green—the world's first two-terabyte hard drive.[1] This drive space

[*] J.D. candidate, Fordham University School of Law, 2010. I would like to thank Professor Deborah Denno for her insight and support as my advisor for this Note, Professor Katherine Strandburg for her immensely helpful comments, and finally my family and friends for their undivided love and support.

1. Press Room – Western Digital Corp., http://www.wdc.com/en/company/glossary.asp (last visited Oct. 8, 2009). A terabyte is equivalent to 1,000 gigabytes.

is roughly equivalent to 129 million pages of Microsoft Word files,[2]—enough to fill the books contained on three floors of a typical academic library[3]—or up to 400,000 digital photos.[4] Far from the room-sized monstrosities of early computer technology, the Caviar Green stands just one inch tall, six inches long, four inches wide, and weighs less than two pounds.[5] Only a few years ago the average hard drive capacity was merely four percent of what is currently available.[6] While a technological marvel, this new massive storage capability also creates interesting and complex problems regarding individual privacy and the Fourth Amendment.

The most pressing issue concerning hard drives and individual privacy is how they are conceptualized within Fourth Amendment jurisprudence. How courts decide to classify hard drives will have dramatic consequences on the security of the information stored on them. Federal courts only began analyzing this problem a decade ago, but during the ten years that have elapsed since the first major decision, computer technology grew exponentially.

The majority of courts treat the entire hard drive as a single closed container.[7] Professor Orin Kerr has deemed this the "physical box" approach.[8] Looking at hard drives in this way renders the zone of a Fourth Amendment search to include the entire hard drive—no matter how large. In other words, a search warrant for one e-mail message has the effect of making everything on that hard drive eligible for investigators to examine. This view has the practical consequence of enabling government agents to access all of the information stored on a hard drive regardless of whether that information has anything to do with the reason the computer is being searched.

Under the minority approach, individual files or folders on a hard drive are treated as separate entities. This approach treats the individual files or folders as the zone of the search and has been described as the "virtual file"

---

2. Lexis Nexis Discovery Services, Fact Sheet, http://www.lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADI_FS_PagesInAGigabyte.pdf (last visited Oct. 8, 2009).

3. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 542 (2005).

4. WD Caviar Green – Western Digital Corp., http://www.wdc.com/en/products/products.asp?DriveID=576 (last visited Oct. 8, 2009).

5. WD Caviar Green, *supra* note 3.

6. *See* Kerr, *supra* note 3, at 542 (noting that in 2005 the average hard drive capacity was eighty gigabytes).

7. *See* United States v. Runyan, 275 F.3d 449, 458 (5th Cir. 2001). *See also* United States v. Hill, 459 F.3d 966, 978 n.14 (9th Cir. 2006).

8. Kerr, *supra* note 3, at 554.

approach.[9] In practice this means that each file or folder, depending on how broad or narrow the proper zone of search was drawn, would constitute a separate container in terms of traditional Fourth Amendment doctrine.

Recently, in *United States v. Crist*, a district court tried to safeguard individual rights by characterizing hard drives in what it believed to be an alternative to the closed container and virtual file approaches.[10] *Crist* dealt with a government search of a computer that had been previously accessed by a private party and the issue of how far, if at all, the government could exceed the scope of the properly conducted private search. The court explicitly held that a hard drive is not analogous to a single closed container and that viewing it as such would impermissibly jeopardize privacy rights.[11] Importantly, however, *Crist* held that the individual platters—or smaller physical subsections of the hard drive—were analogous to closed containers.[12] Accordingly, the court ruled that the government could not search an entire hard drive consisting of multiple platters. While admirable in its effort, the *Crist* court inadvertently advanced the closed container approach with the underlying rationale for its new approach to hard drive searches. If other courts adopt the *Crist* logic, the legal system runs the risk of inadvertently perpetuating the closed container logic in a new doctrine that purportedly seeks to safeguard individual privacy.

Not surprisingly, almost all of the cases dealing with courts' conceptualizations of hard drives revolve around child pornography. Because child pornographers are unsympathetic defendants, this concentration of case law is arguably one of the main reasons the issue has not been thoroughly addressed. One would not expect a large contingent of the legal world to rally around the rights of individuals who possess such disturbing material. It is difficult for any judge to craft a rule that excludes evidence of such despicable acts when the government has a seemingly rational justification for carrying out the search in the manner it does. These vulnerabilities, however, do not only impact child pornographers. Given the increasing technological changes surrounding hard drives and data storage, the child pornographer defendant of today may very well turn into the business executive defendant of tomorrow. Businesses that store massive amounts of sensitive material on central servers or databases are at risk. Professionals

---

9. *See id.*

10. No. 1:07-CR-211, 2008 WL 4682806 (M.D. Pa. Oct. 22, 2008).

11. *See id.* at *10.

12. *See id.* ("[A] hard drive is comprised of many platters, or magnetic data storage units, mounted together. Each platter, as opposed to the hard drive in its entirety, is analogous to a single disk as discussed in *Runyan*.").

who conduct sensitive operations and communicate via e-mail are at risk. In fact, anyone who stores important data on a computer is at risk. That the cases that have so far reached the federal courts have dealt almost exclusively with despicable actions should not serve as a bar to the development of Fourth Amendment doctrine that properly balances the privacy concerns of individuals against the needs of law enforcement officials moving forward.

This Note posits that the majority approach, in which hard drives are characterized as closed containers, is not viable. Such a classification cannot be justified as the amount of data that can be stored on a single hard drive skyrockets and individuals increasingly rely on computer storage for sensitive information. Giving government agents carte blanche authority to sift through enormous amounts of personal information[13] has no parallel in traditional Fourth Amendment practice. When police obtain a warrant to search a home they may not search any and all containers they discover in the process. All further searches of discovered containers must be supported by probable cause.[14] Defining the proper zone of search on hard drives as individual files or folders will better serve to protect the privacy rights of individuals while at the same time giving government authorities enough autonomy to not impair their investigatory duty. As technology grows and more hard drive cases are brought under the Fourth Amendment, criminal defense lawyers will develop stronger arguments in favor of suppressing evidence found as the fruits of these general searches. Moving away from viewing hard drives as closed containers will also protect law enforcement by removing uncertainty as to the future admissibility of evidence uncovered during computer searches.

This Note will examine the history of both the search warrant requirement and private search doctrine, as well as analyze how the conceptualization of hard drives impacts individual privacy in both contexts. Part I ex-

---

13. Proponents of the closed container approach note the fact that a warrant authorizing a search for business records or "writings" permits the search of an entire hard drive. *See* United States v. Hunter, 13 F. Supp. 2d 574, 581 (D. Vt. 1998); Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193, 197-99 (2005) (discussing the broad scope of a document search under Andresen v. Maryland, 427 U.S. 463 (1976), and discussing the courts that adhere to this view). This business records doctrine, however, cannot be extended to computers because of the fundamental difference between a filing cabinet, where papers must be physically examined to ascertain their relevancy, and a computer, where programs and methods are available to limit such intrusion.

14. *See* United States v. Bonitz, 826 F.2d 954, 957 (10th Cir. 1987) ("It is fundamental that, absent some special exception, all containers and packages will receive the full protection of the fourth amendment during a police search." (citing Arkansas v. Sanders, 442 U.S. 753, 762-65 (1979))).

amines the history of how courts have viewed hard drives and provides a brief primer on the technology that operates within hard drives in order to demonstrate that such devices are not simply analogous to closed containers. Part II examines the rationales behind the approaches courts have taken and discusses the problems inherent in both the traditional approaches and the new approach taken in *Crist*.[15] Finally, Part III proposes adopting a modified virtual file approach based on the fact that the closed container approach will grow increasingly problematic as the average size of hard drives increases. The cases treating hard drives as closed containers were decided nearly a decade ago[16] when the average hard drive size was just a fraction of what it is today. Adhering to the general rule that hard drive capacity doubles every two years,[17] it is not beyond the realm of possibility to suggest that the home consumer will be able to purchase ten-terabyte hard drives in the next five years. That means the amount of data left vulnerable to a government search based on a supposedly narrow and particular warrant will be over one hundred times greater than when the first case analogizing a hard drive to a closed container was decided.[18] Adhering to the closed container analogy, or even the virtual file approach as it has been adopted by the federal courts, will expose massive amounts of data to government officials—more data than the courts that first examined the issue could ever have imagined. Moreover, continuing to follow either approach will leave law enforcement officers lost as to what evidence will be admissible or subject to suppression.

I. THE HISTORICAL DEVELOPMENT OF THE PRIVATE SEARCH DOCTRINE AND SEARCH WARRANT REQUIREMENT

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[19] Part I of this Note examines the historical development of this maxim as it applies to modern computer searches. Part I.A discusses the development of the search warrant requirement. Part I.B focuses on the historical development of the Fourth Amendment's private search doctrine.

---

15. *Crist*, No. 1:07-CR-211, 2008 WL 4682806.

16. United States v. Runyan, 275 F.3d 449, 458 (5th Cir. 2001); United States v. Barth, 26 F. Supp. 2d 929, 936 (W.D. Tex. 1998).

17. *See* Kerr, *supra* note 3, at 569.

18. *Barth* was decided in 1998 and the average hard drive capacity in 2005 was 120 gigabytes. Based on a backwards extrapolation of the generally accepted "capacity doubles every two years" theory, the average capacity of a hard drive in 1998 would have been approximately fifteen gigabytes. *See* Kerr, *supra* note 3, at 569.

19. U.S. CONST. amend. IV.

Finally, Part I.C briefly introduces the technology behind contemporary computer hard drives.

A. The Search Warrant Requirement

In 1967 the Supreme Court decided *Katz v. United States*[20] and set forth the modern idea that the Fourth Amendment "protects people, not places."[21] In his oft-quoted concurrence, Justice Harlan explained this adage to mean that the Fourth Amendment protects an individual when she has a "reasonable expectation of privacy" in whatever is being searched.[22] He articulated a two-prong test for determining whether or not an individual has a reasonable expectation of privacy. First, the defendant must have exhibited an actual expectation of privacy—the subjective prong—and second, that expectation must be one that society is prepared to recognize as reasonable—the objective prong.[23] The test as currently articulated by the Supreme Court states that "a Fourth Amendment search does *not* occur . . . unless 'the individual manifested a subjective expectation of privacy in the object of the challenged search,' and 'society [is] willing to recognize that expectation as reasonable.'"[24]

Government agents must obtain a valid search warrant in order to search an area in which an individual has manifested an objective privacy interest that society recognizes as reasonable.[25] Although the Court has recognized numerous exceptions to the warrant requirement, this Note assumes that no such exceptions apply in the situations presented.[26] In the context of searching computers, one of the most important aspects of the Fourth Amendment is the particularity requirement.[27] The particularity requirement compels government agents to specifically describe the area to be searched as well as the object to be seized. There is little case law on how

---

20. 389 U.S. 347 (1967).

21. *Id.* at 351.

22. *Id.* at 360 (Harlan, J., concurring).

23. *Id.* at 361.

24. Kyllo v. United States, 533 U.S. 27, 33 (2001) (quoting California v. Ciraolo, 476 U.S. 207, 211 (1976)).

25. *See* U.S. CONST. amend. IV.

26. Some examples of exceptions to the warrant requirement include exigent circumstances, plain view, and search by consent. *See generally* 3 WAYNE R. LAFAVE, JEROLD H. ISRAEL & NANCY J. KING, CRIMINAL PROCEDURE §§ 3.2, 3.5, 3.10 (4th ed. 2004) [hereinafter CRIMINAL PROCEDURE].

27. "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, *and particularly describing the place to be searched, and the persons or things to be seized.*" U.S. CONST. amend. IV (emphasis added).

the particularity requirement applies to virtual searches, but a brief history of its application in the physical realm will be illustrative.

In the context of physical searches, the Supreme Court has construed the particularity requirement to mean, when executing a search warrant, "nothing [should be] left to the discretion of the officer."[28] Further, "knowledge that some objects connected with criminal activity are to be found on certain premises is no basis for permitting an unrestricted search of those premises. Rather, an intrusion upon the occupant's expectation of privacy in those premises should extend no further than is necessary to find particular objects . . . ."[29] Absolute perfection in the description of the area and object to be searched is not required; it "is enough if the description is such that the officer with a search warrant can, with reasonable effort, ascertain and identify the place intended."[30] This explanation is by no means foolproof, and "problems arise when a facially sufficient description is determined to be less precise than was assumed."[31] When officers obtain a seemingly valid warrant, but discover later that the address or apartment number may be incorrect, there is not much controversy in allowing them to make common-sense judgments about the proper location to be searched. For example, if the warrant specifies "John Doe's blue house at 415 Lake Road" and there is a blue house belonging to John Doe at 451 Lake Road, courts are willing to let the officers involved make judgment calls and execute the search warrant accordingly.[32]

These problems are more pronounced in the virtual context. For example, it has been argued that "[t]he particularity requirement reflects a physical concern," the rationale being that government officials cannot engage in general searches if the specific location and physical object targeted are named.[33] In the virtual world of hard drives, however, the traditional particularity concept does not serve to prohibit general searches nearly as effectively. A government official can request a search warrant for "child pornography" on "John Doe's computer." In the physical world this is as particular as possible—the incriminating material is certainly somewhere on the physical device. In the virtual world, however, the same search warrant leaves extensive amounts of information susceptible to a search that would otherwise be outside of the government's reach. For example, if law

28. Marron v. United States, 275 U.S. 192, 196 (1927).

29. 2 WAYNE R. LAFAVE, SEARCH AND SEIZURE 605 (4th ed. 2004) [hereinafter SEARCH AND SEIZURE].

30. Steele v. United States, 267 U.S. 498, 503 (1925).

31. CRIMINAL PROCEDURE, *supra* note 26, at 163.

32. *See id.* at 166-67.

33. Kerr, *supra* note 3, at 568.

enforcement officers were to carry out a search of John Doe's home for Polaroid pictures containing child pornography, they would not be entitled to open locked containers discovered in the process without a further showing of probable cause. In the virtual context, however, any encrypted folders or files can be accessed pursuant to the original warrant. A search warrant will rarely misidentify the physical object to be searched. It is how the search is performed within the virtual boundaries of that physical device that creates the problems when dealing with search warrants for computers.

Although the particularity requirement compels government officials to specifically define the place to be searched and the anticipated fruits of the search, the requirement has never been applied to *how* the search will be carried out. The particularity requirement has been described as "reflect[ing] a physical concern: the thinking is that the law can limit searches by confining where in the physical world the police search and by naming the object of the search."[34] In the world of computers, however, specifically naming the location and object of the search still leaves vast amounts of data available for the government to inspect. Reinterpreting the Fourth Amendment to require ex ante search protocols in the computer search context may provide the means to safeguard the huge amounts of information stored on individual hard drives. While few courts have ventured to undertake this task, the Northern District of Illinois held in *In re Search of 3817 W. West End* that the government was required by the Fourth Amendment to submit a search protocol prior to the issuance of a warrant.[35] In accordance with a Ninth Circuit ruling, the court reasoned that the degree of specificity imposed by the particularity requirement "varies depending on the circumstances of the case and the type[s] of items involved."[36] A key factor in *West End* was the court's determination that modern computer technology enables government agents to specifically tailor searches.[37] While this technology may not be as precise as some would like, it does enable the government to set forth some type of search protocol that it will adhere to in order to prevent general searches.

Conversely, other courts have held that the Fourth Amendment does not require ex ante search protocols. In *United States v. Hill*, the Ninth Circuit refused to require such a protocol noting that the reasonableness of the searching officer's actions would be sufficient to protect the defendant's Fourth Amendment rights.[38] The court in *Hill* did mention, however, that it

---

34. *Id.*
35. 321 F. Supp. 2d 953 (N.D. Ill. 2004).
36. *Id.* at 958 (citing United States v. Spilotro, 800 F.2d 959, 963 (9th Cir. 1986)).
37. *See West End*, 321 F. Supp. 2d at 959.
38. 459 F.3d 966, 978 (9th Cir. 2006).

"look[ed] favorably" on the inclusion of a search protocol in the search warrant though the lack of one was not fatal to the government's case.[39] This sentiment is echoed in the Department of Justice's Manual for Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.[40] While the majority of courts have refused to require law enforcement to provide ex ante search protocols, there is considerable movement in the opposite direction and as technology rapidly progresses the rationales and decisions of the past decade must be revisited.

B. The Private Search Doctrine

The foregoing discussion is moot, however, unless the government or one of its agents conducts the search. In *Burdeau v. McDowell*, the Supreme Court noted that the Fourth Amendment protects against unlawful searches and seizures and that protection applies only to governmental action.[41] Further, the evidence obtained by a private party can be lawfully used against a defendant.[42] Though it took almost sixty years, the Court finally articulated additional limitations on the private-search doctrine in *Walter v. United States*[43] and *United States v. Jacobsen*.[44]

In *Walter*, a shipment of eight-millimeter film depicting homosexual activities was accidentally shipped to a third-party rather than the intended consignee.[45] Employees of the company where the shipment was mistakenly delivered opened the boxes and discovered many individual boxes of film.[46] These interior boxes had "suggestive drawings" on one side and "explicit descriptions of the contents" on the other.[47] One of the employees opened "one or two of the boxes" and tried, unsuccessfully, to view the contents of the film by holding it up to the light.[48] There were a total of 871 films in the shipment.[49] The employees then called the Federal Bureau of Investigation, who, after seizing the material, viewed the films on a pro-

---

39. *Id.*

40. *See* COMPUTER CRIME & INTELLECTUAL PROP. SECTION, CRIMINAL DIV., U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, pts. I-II (2002) [hereinafter DOJ MANUAL], *available at* http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.pdf.

41. 256 U.S. 465 (1921).

42. *See* Coolidge v. New Hampshire, 403 U.S. 443, 487-90 (1971).

43. 447 U.S. 649 (1980).

44. 466 U.S. 109 (1984).

45. *Walter*, 447 U.S. at 651.

46. *Id.* at 651-52.

47. *Id.* at 652.

48. *Id.*

49. *Id.*

jector "without making any effort to obtain a warrant."[50] The petitioners in the case were indicted and convicted on obscenity charges and their motion to suppress the evidence of the pornographic films was denied.[51]

The Supreme Court reversed the petitioners' convictions on the grounds that the government search exceeded the scope of the search conducted by the private individuals. Writing for a 5-4 majority, Justice Stevens noted that a limited private search before a government investigation does not grant the government unlimited authority to search without a warrant.[52] Most importantly, the Court noted that the government could not exceed the scope of the initial private search without a warrant even if the private search uncovered material that would provide the government with probable cause to believe that the container held illegal material.[53] Probable cause is a prerequisite to obtaining a search warrant, but does not replace a warrant.[54]

Four years later, in *Jacobsen*, the Supreme Court elaborated on just how far beyond a private search a government search could go. Jacobsen and a partner were the intended recipients of a shipment of cocaine via Federal Express ("FedEx"). The package was damaged by a forklift and subsequently inspected by employees pursuant to a contractual provision in FedEx's insurance policy.[55] The package's exterior appeared ordinary and the inside contained a tube fashioned from duct tape surrounded by crumpled newspaper.[56] The FedEx employees cut the tube open revealing four zip-lock bags filled with white powder.[57] The employees then returned the plastic bags to the tube and the tube to the cardboard box while contacting agents from the Drug Enforcement Administration ("DEA").[58] When the DEA agents arrived they reopened the package and, importantly, cut one of the bags of powder open to perform a field test for cocaine.[59] After the test revealed the substance was in fact cocaine, other DEA agents obtained a warrant to search the address where the package was headed and subse-

50. *Id.*

51. *Id.*

52. *Id.* at 656.

53. *Id.* ("[T]he Government argues that the limited private search justified an unlimited official search. That argument must fail, whether we view the official search as an expansion of the private search or as an independent search supported by its own probable cause.").

54. Katz v. United States, 389 U.S. 347, 357 (1967).

55. United States v. Jacobsen, 466 U.S. 109, 111 (1984).

56. *Id.*

57. *Id.*

58. *Id.*

59. *Id.* at 111-12.

quently arrested Jacobsen and his partner.[60] Jacobsen was convicted after an unsuccessful motion to suppress the evidence at trial based on *Walter*. The Court of Appeals for the Eighth Circuit reversed the conviction, however, on the grounds that the field test for cocaine was "a significant expansion of the earlier private search" and was thus unconstitutional.[61]

Again writing for a majority of the Supreme Court, Justice Stevens reversed the Court of Appeals and reinstated Jacobsen's conviction noting that "[t]he additional invasions of [Jacobsen's] privacy by the government must be tested by the degree to which they exceeded the scope of the private search."[62] The Court concluded that, although the DEA agent's field test of the white powder did exceed the scope of the private search, it was not a search under the standard articulated in *Katz*.[63] The core of the court's reasoning was that the field test could "not compromise any legitimate expectation of privacy."[64] The opinion was careful to note that the fact that the white powder tested positive for cocaine did not factor into the reasonable expectation of privacy decision.[65] What was important was the fact that whatever the white powder turned out to be was no longer a "private fact" and thus there could be no reasonable expectation of privacy in it.[66]

The foregoing decisions demonstrate that the government may only exceed the scope of a private search if there is no longer a reasonable expectation of privacy in the contents of the container or area that was searched. Accordingly, confirmation of prior knowledge obtained during the private search would not seem to implicate any Fourth Amendment concerns.[67] Looking for further direction in the area, however, yields few helpful cases. As one court has noted, "there is a remarkable dearth of federal jurisprudence elaborating on what types of investigative actions constitute exceeding the scope of a private search."[68] Moreover, the few circuit courts to address the issue have provided "only limited guidance about the nature of this inquiry."[69] Two circuits have held that a government search exceeds the scope of a private search when the government agents examine a con-

60. *Id.* at 112.
61. *Id.* (citing United States v. Jacobsen, 683 F.2d 296 (8th Cir. 1982)).
62. *Id.* at 115.
63. *Id.* at 143.
64. *Id.* at 123.
65. *Id.*
66. *Id.*
67. *See* United States v. Runyan, 275 F.3d 449, 463 (5th Cir. 2001).
68. *Id.* at 461 (internal quotations omitted).
69. *Id.*

tainer that was left undisturbed by the private searchers.[70] The Eighth Circuit took a different approach and held that unwrapping similar undisturbed items within the container searched by a private party did not exceed the scope of the private search.[71] It is important to note that the Eighth Circuit did not address whether the undisturbed items (kilogram bricks of cocaine wrapped in towels and other clothing material within a zippered suitcase) were separate containers for the purposes of the private search analysis. The court's reasoning emphasized the language in *Jacobsen* that stated it would be possible for no reasonable expectation of privacy to remain in the contents of a container when it seemed apparent to the trained observer that the container contained nothing but contraband.[72]

Therefore, there is still some debate as to when exactly a government search exceeds the scope of a private one. Both the proper means for measuring the scope of a private search and exactly what factual situations would warrant a determination that there is no further reasonable expectation of privacy remain unaddressed by the Supreme Court. These problems are compounded in the hard drive context due to inescapable tension that results from trying to fit emerging technologies into historical doctrines while remaining faithful to the underlying principles of Fourth Amendment jurisprudence.

C. Hard Drive Technology

Before delving into the complex issue of whether or not the existing closed container framework is appropriate, it is important to have a basic understanding of the technology behind the hard drives at the center of this debate. A hard disk is defined as "[a] magnetic disk consisting of a rigid substrate coated or plated—usually on both sides—with a magnetic material."[73] "The drive itself may contain a number of platters mounted on a

---

70. *See* United States v. Kinney, 953 F.2d 863, 866 (4th Cir. 1992) (noting that a subsequent search of a white canvas bag within a closet that had been opened by a private party exceeded the scope of the private party's search); United States v. Donnes, 947 F.2d 1430, 1434 (10th Cir. 1991) (stating that when police opened an opaque container that was inside of a glove discovered and delivered to them by a private party they exceeded the scope of the private search).

71. United States v. Bowman, 907 F.2d 63, 65 (8th Cir. 1990).

72. United States v. Jacobsen, 466 U.S. 109, 121 (1984) ("Under these circumstances, the package could no longer support any expectation of privacy; it was just like a balloon 'the distinctive character [of which] spoke volumes as to its contents, particularly to the trained eye of the officer.'" (quoting Texas v. Brown, 460 U.S. 730, 743 (1983))).

73. *Hard Disk*, OXFORD DICTIONARY OF COMPUTING 237 (John Daintith ed., Oxford University Press 5th ed. 2004).

rotating spindle."[74] These platters can be visualized by imagining a stack of compact discs packed tightly together. Data, however, is not neatly stored on these platters the way most people likely envision data being stored on their operating system. The hard disk "stores data in *tracks* of magnetically oriented particles" of which there may be over 10,000 on a high capacity drive.[75] These tracks are divided into smaller units called sectors.[76] Importantly, for purposes of the Fourth Amendment analysis, "[w]hen a file is written to a hard [drive] it is *not written in consecutive sectors. Sectors are scattered all over the disk, organized as a linked list.*"[77] Accordingly, data from a single file may be scattered on different platters in various places on the hard drive.

Another form of hard drive technology that is gaining popularity is solid-state memory ("SSM"). Also known as semiconductor memory, SSM is the technology currently utilized in USB flash drives and other small, portable media. The capacity of SSM has been "increasing by a factor of four every few years"[78] and the technology is now available in certain notebook computers.[79] These solid-state devices ("SSD") are "fabricated principally or entirely from solid material" and contain semiconductors that serve to store the data.[80] In short, SSDs contain no platters or other moving parts; no physical distinction can be made between platters or any other component parts. They are, for all intents and purposes, small pieces of material that store increasingly large amounts of information.

II. DISCUSSION: HOW SHOULD HARD DRIVES BE VIEWED IN THE FOURTH AMENDMENT CONTEXT?

One of the most significant concerns when dealing with computer technology and the Fourth Amendment is how to conceptualize hard drives within the preexisting doctrinal framework. Part II will discuss the current views that courts have adopted regarding this issue. Part II.A will examine the "physical box" approach of equating hard drives with closed containers

74. Stephen J. Rogowski, *Hard Disk*, *in* CONCISE ENCYCLOPEDIA OF COMPUTER SCIENCE 357 (Edwin D. Reilly ed., 2004).

75. *Id.*

76. *Id.*

77. *Id.* (emphasis added).

78. *Semiconductor Memory*, OXFORD DICTIONARY, *supra* note 73, at 471.

79. Apple offers an 128-gigabyte solid state drive for purchase in a notebook computer. *See* MacBook Air – Apple Store (U.S.), http://store.apple.com/us/browse/home/shop_mac/family/macbook_air?mco=MTE3MDc (last visited Feb. 28, 2009).

80. *Solid-State Device*, OXFORD DICTIONARY, *supra* note 73, at 494.

while Part II.B will examine the "virtual file" approach of treating individual files or folders as the proper zone of a search. Part II.C will then examine the new approach set forth by the court in *United States v. Crist.*

After *Jacobsen*, the paradigm inquiry in determining whether a government search exceeds the scope of a prior private search is whether the individual retains any reasonable expectation of privacy after the initial search. Whether or not an individual retains a reasonable expectation of privacy concerning the information stored on her computer's hard drive is predicated exclusively on how that hard drive is classified. If the hard drive is analogous to a closed container, as soon as it is accessed the owner forfeits any reasonable expectation of privacy in the rest of its contents.[81] As mentioned above, this has been described as the "physical box" approach.[82] On the other hand, if a hard drive is imagined to be more like a warehouse containing many individual containers—the "virtual file" approach—additional questions arise as to what expectation of privacy remains after a portion of the information has been accessed. The approach taken in *United States v. Crist* may be deemed a hybrid, though it will become apparent that the rationale mirrors the closed container approach much more than the virtual file counterpart. Federal courts have employed all three views in practice and no consensus has been reached.

A. Closed Containers: The "Physical Box" Approach

In *United States v. Runyan,* the Fifth Circuit employed the physical box approach.[83] Defendant Runyan filed for divorce from his wife, Judith, who subsequently made several trips to Runyan's home to retrieve items that purportedly belonged to her.[84] During one of these visits Judith observed a desktop computer surrounded by various types of disks.[85] Judith then had a friend disassemble the computer and take it, along with the various disks, back to her residence.[86] Back at her home, the friend viewed "approximately twenty" of the disks that had been removed along with the computer, but none of the ZIP disks,[87] and found that they contained child por-

81. *See* Illinois v. Andreas, 463 U.S. 765, 771 (1983) (noting that an individual does not have a reasonable expectation of privacy in a container that had previously been opened by a customs agent); Walter v. United States, 447 U.S. 447, 656 (1980) (noting that the boxes that had been opened by the private parties were subject to a permissible government search).

82. Kerr, *supra* note 3, at 554.

83. 275 F.3d 449, 463-64 (5th Cir. 2001).

84. *Id.* at 452.

85. *Id.* at 453.

86. *Id.*

87. *Id.*

nography.[88] Judith and the friend promptly contacted the authorities and turned over "twenty-two CDs, ten ZIP disks, and eleven floppy disks to the deputy [who responded to the call]."[89] After an investigation, a Customs Service Special Agent was assigned to the case and viewed images from every piece of evidence turned over to the authorities. A subsequently-filed affidavit also stipulated that another officer involved in the case had engaged in a "cursory review" of all the "computer storage media."[90] Runyan was indicted on federal child pornography charges and moved to suppress the evidence obtained in the pre-warrant searches of the media turned over to authorities by his wife.[91]

Runyan's Fourth Amendment challenges were brought on two grounds—first, that the private parties had only searched a random assortment of the disks while the government agents searched all of them, and second, that the government agents examined more images on each disk than the private searchers.[92] The first theory mirrors the physical box approach. Runyan was apparently conceding under this theory that once the private party had accessed a disk, the reasonable expectation of privacy was lost. The second theory Runyan advanced was akin to the virtual file approach in that Runyan was implicitly arguing that he still had a reasonable expectation of privacy in images that were not viewed, but were on the disks accessed by the private search.

The Fifth Circuit noted that each disk[93] was an individual closed container for purposes of Fourth Amendment analysis.[94] The court further explained that the government exceeds the scope of a private search if it examines closed containers that were not opened initially, unless they are "substantially certain of what is inside the container based on the statements of the private searchers, their replication of the private search, and their expertise."[95] The court held that there was no possible way the police officers in question could have been "substantially certain" the unexamined disks also contained child pornography and thus, the subsequent search of all the disks violated Runyan's Fourth Amendment rights under the private

88. *Id.*

89. *Id.*

90. *Id.* at 454-55.

91. *Id.* at 455.

92. *Id.* at 460.

93. The *Runyan* court failed to address the issue of whether the hard drive in the seized desktop computer was a single closed container, seemingly because the incriminating child pornography was located exclusively on the disks and not the computer.

94. *Runyan*, 275 F.3d at 464.

95. *Id.* at 463.

search doctrine.[96] As to Runyan's second theory, the virtual file approach, the court was not as accommodating. The court explicitly stated, "[I]n the context of a closed container search . . . the police do not exceed [a] private search when they examine more items within a closed container than did the private searchers."[97] This rationale was based on the fear of over-deterrence. The Fifth Circuit explained that if the virtual file approach were adopted, government agents would be "disinclined to examine even containers that had already been [privately searched] for fear of coming across important evidence that the private searchers did not happen to see and that would then be subject to suppression."[98]

First and foremost, proponents of the view espoused in *Runyan* claim that defining hard drives as closed containers provides the most workable solution to a potentially massive problem.[99] Because of the numerous practical problems that arise when labeling hard drives as anything other than closed containers, the *Runyan*-doctrine advocates the claim that any other conceptualization of hard drives will lead to absurd results. If a search was deemed unconstitutional every time a government agent stumbled upon something within a closed container that had not been first examined by the private searchers, the government agents would be over-deterred and shy away from conducting searches to the fullest extent of their abilities.[100] If government agents were to exceed the scope of a private search any time they examined something not previously searched by the private party, it could also result in wasting police time and resources.[101] Moreover, when search warrants come into play there are numerous conceptual problems with limiting the zone and scope of search within the virtual environment of the hard drive.

Some scholars echo this view.[102] In particular, Professor Thomas Clancy argues that classifying hard drives as single closed containers will not have the disastrous effect of allowing "wholesale searches of data" on computers under investigation by the government.[103] The underlying assumption with this viewpoint is that all files on a hard drive may be scanned to ascertain their relevancy, though anything outside the scope of the warrant or prior private search will be suppressed. Similar to the rationale invoked by

96. *Id.* at 464.
97. *Id.*
98. *Id.* at 465.
99. *See generally* Clancy, *supra* note 13.
100. *See Runyan*, 275 F.3d at 465.
101. *See id.*
102. *See generally* Clancy, *supra* note 13.
103. *Id.* at 199.

courts in file cabinet cases, this view assumes that there is no better way to separate data than manually examining each and every piece of information to determine its relevancy to an investigation.

While the foregoing distinction may be viable in the physical context of file cabinets and similar objects, it may not withstand scrutiny in the virtual world. Further, this possibility is fraught with potential privacy infringements, regardless of whether the information will be admissible at trial. It is hard to imagine how demarcating the zone of search and conceptualizing a hard drive as one closed container will not allow wholesale searches of the entire hard drive. Indeed, one can easily imagine an overzealous U.S. Attorney seeking a warrant for "financial records" on a large bank's computer system and then engaging in a wholesale search for any and all evidence of criminal activity. Perhaps the only saving grace to privacy rights hidden in this rationale is that incriminating evidence may possibly be suppressed if a judge finds ex post that it was discovered improperly. Whether or not this protection is enough to adequately safeguard privacy rights, however, is debatable.

B. Virtual Warehouses: The "Virtual File" Approach

Not every circuit court to address the issue has discredited the virtual file approach. In *United States v. Carey* the Tenth Circuit held that images of child pornography that were discovered incident to a search for evidence of drug sales were not admissible.[104] Carey had been under investigation for possible sale and possession of narcotics when he consented to a search of his residence.[105] During this initial search the police discovered two computers, which they subsequently seized and obtained a warrant to search for "names, telephone numbers, ledger receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances."[106] After an initial search of file types that would traditionally harbor evidence of drug crimes turned up nothing, one of the detectives began examining JPG files—a file type associated with images.[107] The first JPG file that the officer opened contained an image of child pornography.[108] After discovering this image, the officer downloaded the remaining JPG files—approximately 244—onto nineteen disks and viewed a handful

104. 172 F.3d 1268, 1276 (10th Cir. 1999), *reh'g denied.*
105. *Id.* at 1270.
106. *Id.* at 1272-73 (internal quotation marks omitted).
107. *Id.* at 1271.
108. *Id.*

of files on each disk.[109] Carey was then indicted on child pornography charges as well as drug charges.[110]

Holding that the search of the JPG files exceeded the scope of the warrant, the court stressed that the officer's suspicion changed immediately upon viewing the first file containing child pornography and the subsequent search of all the computer's JPG files was not judicially authorized.[111] In dicta, however, the Tenth Circuit cautioned that "relying on analogies to closed containers or file cabinets may lead courts to oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern computer storage."[112] A central underlying assumption in *Carey* was that the defendant's hard drive was not a single closed container. By ruling that an officer could exceed the scope of a warrant while searching a computer, the Tenth Circuit advanced quite a different view than was espoused in *Runyan*. In terms of the hard drive, "the relevant unit of search, at least in the case of digital images, is an individual file."[113]

The rationale behind the decision in *Carey* was straightforward. The court made it abundantly clear that analogizing Carey's hard drive to one closed container would enable the government to perform a general exploratory search—a result the court was unwilling to allow. And while the general idea motivating the decision appears proper, the implementation of the virtual file approach within the decision presented one glaring problem: the *Carey* court was unwilling to advocate an ex ante search protocol requirement for search warrants issued for hard drives. Instead, the court relied heavily on the subjective intent of the government agent who executed the search in determining the constitutionality of the scope of the search.[114] On the surface, bringing the subjective intent of the searching officer appears to be a workable way to limit the scope of the searches pursuant to a constitutional warrant. The entire realm of Fourth Amendment doctrine can be said to revolve around the subjective component of reasonableness, that is, striking a reasonable balance between individual privacy and the proper power of law enforcement.[115] In the context of executing search warrants, however, the Supreme Court has explicitly noted that the subjective intent of the searching officer cannot be used to invalidate the scope of

109. *Id.*

110. *Id.* at 1270.

111. *Id.* at 1273.

112. *Id.* at 1275 (internal citations and quotation marks omitted).

113. Kerr, *supra* note 3, at 555.

114. *Carey*, 172 F.3d at 1273 ("We infer from his testimony Detective Lewis knew he was expanding the scope of his search when he sought to open the JPG files.").

115. *See generally* SEARCH AND SEIZURE, *supra* note 29, at 4-5 (discussing how courts have used the probable cause requirement to strike this balance).

a search conducted pursuant to an objectively sufficient warrant. In *Horton v. California* the Court explicitly noted that objective standards limit the scope of the warrant and the subjective intent of the officer cannot come into play.[116] Further, in *Whren v. United States* the Court rejected the idea that "an officer's motive invalidates objectively justifiable behavior under the Fourth Amendment."[117] *Carey* failed to address these concerns, as did the Tenth Circuit's subsequent decisions that refined the *Carey* rationale.[118] There was no discussion in *Carey* of whether the warrant involved was objectively sufficient. Without some sort of reformulation or clarification, it does not appear that the virtual file approach in *Carey* can be harmonized with existing Fourth Amendment doctrinal points espoused in *Horton* and *Whren*.

C. A New Approach?: *United States v. Crist*

In the near decade following *Runyan* and *Carey*, courts remained silent on how to properly conceptualize a hard drive in terms of the Fourth Amendment. The issue piqued only minimal interest from scholars despite the seeming enormity of the potential problem.[119] At the time *Carey* and *Runyan* were decided, hard drive capacity was a fraction of what it has become today. Less than a decade ago in 2001, for example, a common home computer would typically have contained a twenty-gigabyte hard drive.[120] As discussed above, earlier this year Western Digital introduced the world's first two-*terabyte* hard drive. With the ever-expanding storage capacities of computer memory, equating a hard drive with a single closed container would apparently enable government officials' to access unprecedented amounts of information based on a private individual viewing one illicit image file or a search warrant for something as simple—and relatively tiny—as an e-mail correspondence.

In late 2008, the issue once again came to the forefront of Fourth Amendment jurisprudence. In *United States v. Crist*, a court delivered

---

116. 496 U.S. 128, 138 (1990).

117. 517 U.S. 806, 812 (1996).

118. *See* United States v. Walser, 275 F.3d 981 (10th Cir. 2001); United States v. Campos, 221 F.3d 1143 (10th Cir. 2000). For an in-depth discussion of the conflict between *Carey* and *Horton*, 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 (2005).

119. *See generally* Clancy, *supra* note 13; Kerr, *supra* note 3.

120. *See* Kerr, *supra* note 3, at 542 (noting that in 2005—four years after *Runyan* and six years after *Carey*—the typical capacity of a hard drive was eighty gigabytes; the twenty gigabyte estimation is based on the assumption that computer storage capacities tend to double every two years).

what on its face appeared to be a victory for privacy advocates.[121] At first glance, it seemed as if the court moved away from the closed container approach, but a closer inspection of the court's rationale makes that conclusion tenuous at best.

The story began when Robert Crist failed to pay his rent on time. After a few months of nonpayment, Crist's landlord hired two men to remove the belongings from Crist's apartment.[122] After taking photographs of the inside of the apartment for documentation purposes, the men moved Crist's scant belongings onto the curb outside for trash pickup.[123] One of the men informed a friend who was looking for a computer that Crist's computer would be outside the apartment; the friend, Seth Hipple, picked up the computer shortly thereafter and took it back to his residence.[124] Upon learning of what was happening at his residence and not being able to locate his computer, Crist called the police and reported the computer stolen.[125] In the meantime, Hipple had brought the computer to his home and tried to "get it running."[126] After Hipple looked through "a 'bunch of songs' on a media folder," he opened "a couple of video files depicting children performing sexual acts."[127] After viewing these files Hipple deleted the entire folder and, a few days later, contacted the local police department.[128] After the computer was entered into evidence, the Pennsylvania Attorney General's Office took custody of the computer in order to conduct a forensic analysis on the hard drive.[129]

The forensic analysis of Crist's hard drive was thorough. The agent took an MD5 hash value of the drive, which is a "'fingerprint' or [kind of] 'digital DNA'" of the drive, and created a copy.[130] The agent then analyzed the copy—not the actual hard drive from Crist's computer—using a program called EnCase.[131] EnCase does not function in the traditional manner of looking through files or folders; instead, it "reads every file—bit by bit, cluster by cluster—and creates an index of the files contained on the hard drive."[132] The agent from the Attorney General's Office then performed a

121. No. 1:07-CR-211, 2008 WL 4682806 (M.D. Pa. Oct. 22, 2008).
122. *Id.* at *1.
123. *Id.*
124. *Id.*
125. *Id.*
126. *Id.*
127. *Id.*
128. *Id.* at *1-2.
129. *Id.* at *2.
130. *Id.*
131. *Id.*
132. *Id.*

signature analysis on *all* the hash values on the hard drive and compared them to a database containing hash values of known and suspected[133] child pornography.[134] After this analysis was complete the agent discovered five video files containing known child pornography and 171 video files containing suspected child pornography.[135] Further analysis turned up almost 1,600 images of known or suspected child pornography.[136] Crist was subsequently indicted on two counts of knowingly receiving and possessing digital images and video files containing child pornography in violation of 18 U.S.C. §§ 2252A(a)(2)(A) & 2252A(b).[137]

The district court ruled to suppress any evidence found that was not uncovered by Hipple.[138] In doing so, the court noted that the EnCase analysis constituted a search that exceeded the scope of the initial private search: "the rationale for authorizing warrantless searches in *Jacobsen* is that the private search was so complete, no privacy interest remained. That is certainly not the case here."[139] The court, however, did not stop there. It rejected the government's contention that a hard drive was a single closed container, justifying this rationale on the fact that hard drives contain many internal "platters" and each of those platters was analogous to a separate container as discussed in *Runyan*.[140]

The district court's opinion in *Crist* seemingly set out to champion privacy rights and serve as a new model for courts to follow when dealing with searches of hard drives. The decision was adamant that the prior private search of a few videos did not compromise the reasonable expectation of privacy regarding the remainder of the hard drive's contents. Moreover, the court was careful to make clear that a hard drive could not be classified as one single closed container.

While the task was admirable and served to protect the instant privacy rights of Crist, the logic appears faulty. As soon as the court made the leap and declared that Crist's hard drive was not analogous to a single closed container, the logic began to unravel. If the court had simply stopped after making this distinction it would have produced another decision in the virtual file camp that could be elaborated-upon by courts in the future. In-

133. "Known" child pornography is pornography in which the name of the victim is known. "Suspected" child pornography includes files which "[contain] depictions of child pornography but the name of the victim is not known." *Id.* at n.3.

134. *Id.* at *2.

135. *Id.*

136. *Id.* at *3.

137. *Id.*

138. *Id.* at *13.

139. *Id.* at *9.

140. *Id.* at *10.

stead, the court delved into the platter discussion and made the mistake of stating "[e]ach platter, as opposed to the hard drive in its entirety, is analogous to a single disk."[141] This platter distinction simply does not comport with the privacy-protecting ideals of the virtual file approach. While protecting privacy rights in hard drives for the time being, the platter distinction creates more questions than it resolves. For example, the court failed to discuss what data was contained on each platter, how much data was contained on each platter, or if it was even possible to make such determinations. In effect, all the court did was adopt the physical box approach of *Runyan*, but instead of a pile of disks sitting on a desk, there was a pile of disks symmetrically mounted inside of a metal casing that was fastened to the interior of a desktop computer. Essentially, all *Crist* does is reaffirm the closed container approach on a micro scale. As soon as it becomes possible to determine with exactitude what information each platter contains, government agents will be able to conduct wholesale searches of each platter. Considering the size of modern hard drives it does not seem radical to suggest that individual platters will at some point contain as much information as entire hard drives did in the recent past.

Lastly, when taken to its logical conclusion, the *Crist* rationale is, effectively, the virtual file approach. The court stated that the entire hard drive could not be a single closed container, so it pared the size of the container down based on a physical distinction it evidently believed would remain constant.[142] As long as manufacturers continue to employ the same hard drive design there will be platters to designate as separate closed containers. The virtual file approach can be viewed as simply paring the *Crist* approach down further, making the singular closed container the individual file or folder on the platter. There are obvious differences—the virtual file being virtual as opposed to physical, for one thing—but the extrapolation is not far-fetched.

In sum, *Runyan* represents the closed container approach formulated in 2001, the practical result of which is to leave enormous amounts of information easily susceptible to government search even if most of that information has nothing to do with what the government is investigating. Conversely, *Carey*, decided in 1999 and reiterated by the Tenth Circuit in 2001, attempts to remove hard drives and computers from the traditional Fourth Amendment realm and adopts a somewhat more advanced approach.[143] By

141. *Id.*

142. *Id.* at *10.

143. *See Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999) (explaining that the traditional file cabinet analogy is inadequate for dealing with hard drives and a more complex standard is needed for computer technology).

holding that it is possible for a government agent to exceed the scope of a warrant to search a hard drive, the Tenth Circuit made clear that a hard drive is not simply a single closed container, but failed to elaborate on exactly how they should be viewed. As would be expected from such a ruling, the result of this approach is a constant uncertainty, at least in the jurisdictions that follow suit, concerning how search warrants regarding hard drives must be specified and when government agents' actions exceed the scope of those warrants or prior private searches. Moreover, it has been almost a decade since a circuit court has ruled on this issue. While in other areas of the law a decade may not seem like much, when dealing with computer technology ten years can make a world of difference. For instance, ten years ago most people still used dial-up connections to get online and "streaming video" consisted of endless waiting for pages to load and then watching choppy and grainy video. Today fiber-optic internet connections are wired directly into the home and streaming high-definition movies are commonplace. The issue of how computer searches should properly be executed is one that must be addressed as quickly as possible considering the speed with which technology develops.

III. ARGUMENT: A NEW APPROACH—VIRTUAL FILES AND SEARCH PROTOCOLS

At this juncture, *Runyan* and *Carey* exemplify the two dominant approaches courts have taken when dealing with the issue of hard drive classification under the Fourth Amendment. *Crist* remains an outlier and, as will be explained below, does not appear to be a feasible doctrinal solution moving forward. The massive storage capacities of modern hard drives coupled with the always-expanding use of personal computers would result in exposure of far too much private information if a closed container approach were to be accepted.

Part III of this Note proposes a modified approach to hard drive classification that attempts to avoid the pitfalls of both the *Carey* and *Crist* formulations. Part III.A will examine the problems inherent in both the physical box and virtual file approaches while Part III.B will propose adopting a modified virtual file approach as a workable solution to these complex problems. Finally, Part III.C will examine the practical effects of applying the proposed approach to the cases discussed above.

A. Two Problematic Approaches

Adopting the physical box approach could have disastrous and absurd results. As described above, conceptualizing hard drives as closed containers can lead to individuals forfeiting their reasonable expectations of pri-

vacy in vast amounts of personal data. A few practical examples highlight this concern. Imagine a network server that provides a large number of workstations with access to network disk drives.[144] These shared disk drives contain the information of countless individuals.[145] Employing the closed container formulation to these drives would effectively extinguish other individuals' reasonable expectations of privacy in their stored data if data from just one user were the subject of a search warrant. The same problem with the closed container approach arises in the context of shared computers. Under the closed container approach, a family man and CEO suspected of conversing electronically about financial improprieties on his family's shared computer would serve to forfeit the expectation of privacy in his wife's personal data stored on the same hard drive.

The platter rationale adopted in *Crist* is similarly problematic and will fail to protect individual privacy the way the court envisioned. While attempting to protect privacy of individuals' data in the information age, the platter approach fails to safeguard privacy of data in SSM as discussed above, USB drives, CD or DVD media, or any other storage mechanism that has separate and definable parts. Moreover, the rationale is faulty even in the realm of the hard drives it purports to protect. While it may be possible to detect what platter an individual file is stored on, many systems permit file fragmentation. File fragmentation results in individual files being broken down into smaller chunks and being stored in a variety of places across the hard drive.[146] This can result in one file being stored on multiple platters. It would seem to cut against the rationale of the court's decision in *Crist* to say that a user whose computer enabled file fragmentation would lose a reasonable expectation of privacy in multiple platters, but the lucky user whose computer did not, would be entitled to more protection under the Fourth Amendment. Further, with the emergence of solid-state drives and other media that do not fit into the traditional mold, platters may soon become a thing of the past. Once these devices with non-moving parts become widely available, courts employing the *Crist* rationale will have no choice but to resort to the closed container approach and take a huge step back from protecting privacy rights. In a virtual world, simply turning one physical closed container into a series of smaller ones does not solve the privacy problem.

---

144. A server is an administrative computer that controls the access to a computer network and its resources. MICROSOFT COMPUTER DICTIONARY 403-04 (4th ed. 1999).

145. Kerr, *supra* note 3, at 556 (noting how a single physical storage device can contain the private files of thousands of different users).

146. MICROSOFT COMPUTER DICTIONARY, *supra* note 144, at 195.

The foregoing examples highlight a few of the problems presented by the closed container approach. As noted in Part II.B, however, the virtual file approach is problematic in its own ways. Including an ex ante search protocol requirement can adequately handle the subjective intent problems that are thrust into play when implementing the virtual file approach and keep it in line with the fundamental holdings of both *Horton* and *Whren*.

B. Virtual Files and Search Protocols: A Proposal

The virtual file approach is the best way to classify hard drives under the Fourth Amendment. The term "virtual file approach" is worthless, however, unless courts have some practical guidance on how to implement and apply it.[147] This Part proposes a modified two-part approach to the virtual file classification that will hopefully solve the problems created by both *Carey* and *Crist*. First and most importantly, the proper zone of a hard drive search must be the virtual files and folders contained on the drive. Exactly how narrow to draw this distinction on the virtual level can be debated; what cannot, however, is that any distinction on the physical level is simply unworkable if individual privacy is to be adequately protected. Second, courts must re-conceptualize the Fourth Amendment's particularity requirement in the computer context and require ex ante search protocols that lay out exactly how the hard drive will be examined by forensic analysts. The technology to pinpoint data exists.[148] This technology may not be perfect, but using it to search for files without indiscriminately viewing everything on an individual's computer is the best method available at this juncture to safeguard privacy.

This proposal will function to limit the invasiveness of government searches in two ways. First, in the context of the private search doctrine, government agents will not be able to exceed the scope of the prior private search by any means. This development will be consistent with the tenets of *Walter* and *Jacobsen*. Because the proper zone of the search should be

147. The Tenth Circuit declined to extend *Carey* to require a search protocol in *United States v. Brooks*, 427 F.3d 1246, 1251 (10th Cir. 2005). As discussed *infra*, however, simply imposing the virtual file approach without an ex ante search protocol requirement calls for courts to interpret the searching officer's subjective intent. Requiring courts to examine this subjective intent is not only violative of the Supreme Court's holding in *Horton v. California*, but also impractical and difficult to apply ex post.

148. Forensic analysis programs for computers advance with each passing day. For instance, Guidance Software's "EnCase" program advertises "Smart Evidence Collection: No other forensic tool gives organizations the ability to forensically preserve only the relevant evidence without capturing the entire hard drive." GUIDANCE SOFTWARE, ENCASE ENTERPRISE FOR EDUCATION 2 (2006), http://www.bestnetworksecurity.com/images/uploads/guidance-for-education.pdf (last visited Oct. 20, 2009).

limited to the already-examined virtual files, anything beyond that would violate the Fourth Amendment. For example, if the private search uncovered evidence of child pornography, the government agents would ostensibly have probable cause to obtain a search warrant to search that hard drive for further instances of child pornography. The same principle would apply if the private search uncovered a spreadsheet documenting the owner's drug sales. It is in this way that limiting the zone of search to individual files or folders will aid law enforcement as well. Police officers or government agents conducting forensic searches will no longer need to worry about the proper scope of their examination subsequent to a private search or pursuant to a broad warrant. Requiring a search protocol on top of instituting the virtual file approach will assure law enforcement officials that any evidence they obtain will be admissible against the defendant. Second, as mentioned briefly above, interpreting the particularity requirement to necessitate the submission of search protocols will serve to limit the evidence the government can constitutionally view and extract from a hard drive pursuant to a warrant.

C. Application in Practice: How Would a Modified Approach Work?

Exemplifying just how a modified virtual file approach will function in practice will provide insight into its benefits. In terms of the private search doctrine, the application would be straightforward. The fundamental problem that courts encounter when dealing with hard drives that have previously been searched by a private party is the question of proper scope.[149] Once the zone of search is determined to be the virtual file, scope is no longer an issue in private search doctrine cases. The defendant will lose her reasonable expectation of privacy in whatever files were examined by the private party and nothing else. The government agent must obtain a search warrant based on probable cause in order to search anything aside from these previously examined files—a burden that does not impermissibly impede the agent's ability to adequately perform her duty. The application of the proposed new approach to such a search warrant will be discussed below.

Applying the modified virtual file approach in *Crist* would have resulted in an identical district court ruling, albeit based on a quite different rationale. All the evidence obtained by the forensic examination other than the files initially viewed by the private searcher would have to be suppressed.

---

149. *See generally* United States v. Runyan, 290 F.3d 223 (5th Cir. 2002); United States v. Carey, 172 F.3d 1268 (10th Cir. 1999); United States v. Crist, No. 1:07-CR-211, 2008 WL 4682806 (M.D. Pa. Oct. 22, 2008).

As soon as the investigators examined anything else on Crist's hard drive, they impermissibly violated his Fourth Amendment rights. The same logic applies to *Runyan*. Instead of the court suppressing evidence located on disks that had not been accessed by Runyan's wife and her companion, the court would have had to suppress any evidence discovered aside from the actual image files viewed during the course of the private search.

As is evident from these examples, the virtual file approach was not particularly problematic in the context of the private search doctrine. In fact, it serves its purpose with little controversy—individual privacy is protected and government agents are not hamstrung because they will, in most cases, be able to obtain a search warrant based on probable cause from the private search. It is when these search warrants are then executed, however, that the larger problems appear. Requiring an ex ante search protocol is the best way to resolve these problems while remaining faithful to the traditional Fourth Amendment balance between individual privacy from government intrusion and law enforcement agent's ability to adequately perform their investigatory duties.

Looking at *Carey* through the lens of this modified approach will better serve to illustrate its practical effect on the search warrant process. The subjective intent of the officer who conducted the search would not be relevant under the proposed standard. For the sake of the argument, assume that a search protocol was implemented and specified that documents related to Carey's suspected drug sales would be targeted using file names, file extensions, and file headers. Under this hypothetical search protocol all of the image files uncovered would be suppressed. The searching officer in *Carey* saw the incriminating file name and opened the file accordingly—this constitutes a separate search under the virtual file approach. Because the officer opened these image files—which have distinct file headers, names, and extensions from any text, spreadsheet, or other file that could be used to store drug sale information—he impermissibly extended the search beyond what was specified in the protocol. And while this result would seem to let Carey "get away with" a heinous act, it is important to note that the application of the modified virtual file approach would neither frustrate law enforcement operations nor make it easier for individuals who have committed crimes to keep them hidden. For instance, if an officer or analyst were carrying out a search pursuant to the aforementioned hypothetical protocol and discovered a file entitled "childporn.JPG," sufficient probable cause would be apparent for the issuance of a new warrant with a new search protocol. And while this process may seem cumbersome, it is no more so than requiring police officers to obtain a warrant to search a locked container within a home that they are already permissibly searching.

Outside of a few longstanding exceptions, courts do not allow police to enter and search an area because of their subjective "certainty."

While it has been stated that "the particularity requirement does less and less work as the storage capacity of computer devices gets greater and greater,"[150] the call for an ex ante search protocol requirement has been muted. One of the foremost scholars on computer technology and the law has expressly rejected the idea as "serv[ing] little purpose."[151] Those opposed to a search protocol requirement state numerous reasons in support of their case. The most pervasive arguments are that: ex ante regulation is more costly and time consuming;[152] defendants may have taken steps to disguise incriminating evidence; forensic analysts rarely know ahead of time exactly how they will attack a hard drive; and federal judges are ill-equipped to determine what search protocol will be the most effective and least invasive.[153] While compelling, these reasons do not tip the scales so far against ex ante search protocols as to make them wasteful or inappropriate.

Technology is constantly evolving. Forensic investigation programs become more refined with each passing version. While defendants may indeed disguise incriminating evidence, there is technology to identify files even when the extensions and names have been altered.[154] Forensic analysts can conduct searches at both the logical and physical levels[155] without opening the files involved.[156] Searching based on file headers or hash values enables analysts to find the evidence sought without indiscriminately opening and sifting through the mountains of personal data that may be completely irrelevant to the ongoing investigation. For instance, the Spanish Guardia Civil Computer Crime Unit has developed a search engine to find known hash values of illegally shared files on peer-to-peer file sharing networks.[157] Similar to the database of hash values used in the *Crist* investigation, these search engines can be used to narrowly tailor searches of computers suspected of containing illegal material.

---

150. Kerr, *supra* note 3, at 565-66.

151. *Id.* at 576.

152. *See* SEARCH AND SEIZURE, *supra* note 29 (internal quotations and citations omitted).

153. Kerr, *supra* note 3, at 575-76.

154. For example, even if a defendant had changed the filename and extension of a known image of child pornography, a hash value comparison would uncover the image regardless.

155. *See* Kerr, *supra* note 3, at 544.

156. *See id.* at 544-45 (discussing how analysts can conduct file name searches, file extension searches, and file header searches—all of which may search files for specific instances of criminality without viewing the contents of those files).

157. *See* United States v. Cartier, 543 F.3d 442, 444 (8th Cir. 2008).

Further, while forensic analysts may not know ahead of time the precise course of action they will take in examining a hard drive, asking them to collaborate with government officials in preparing a guided search protocol does not require perfection. It is true that there is no "perfect tool" that can pinpoint exactly what government officials are searching for while at the same time keeping other information free from inspection.[158] A lack of such a tool should not, however, result in wholesale searches of computers simply because a perfect system cannot be implemented. If seeking pirated music and video files, the government can submit a protocol specifying that hash values of known pirated media be compared to hash values on the defendant's computer. If, on the other hand, the government is searching for an incriminating e-mail correspondence between two members of a company's board of directors, they can specify that they will target specific words and phrases as well as the types of files that traditionally contain e-mail. The fact remains that even if these tailored searches reveal unexpected information, there will still be ex post judicial review available to deal with these unforeseen issues. Requiring the search protocol ahead of time will limit the discretion of the searching officer or forensic analyst and curb the chance of general exploratory searches.

As for the concern about judges being ill-equipped to deal with the investigatory process, it appears to be a matter of perspective. One should not assume that judges are ignorant of new technologies and the effect they have on existing constitutional standards. Judicial institutes exist across the country where judges can register for seminars and classes to keep themselves abreast of cutting-edge developments in the judicial world.[159] These institutes deal with topics ranging from how to handle alternative dispute resolution to the growing use of transnational legal authority and the impact on courts in the United States.[160] It is true that judges are not as technically skilled as forensic computer analysts and computer scientists. Judges, especially in the context of authorizing search warrants, are protectors of constitutional rights. Requiring search protocols does not also require members of the judiciary to hold advanced degrees in computer science any more than the introduction of DNA evidence require judges to be experts in

158. The "perfect tool" is what Orin Kerr entitled a theoretical forensic analysis program that could locate exactly what a warrant is looking for without compromising any other information on the computer. *See* Kerr, *supra* note 3, at 570.

159. *See, e.g.*, Colo. Judicial Inst., http://www.coloradojudicialinstitute.org (last visited July 27, 2009); Flaschner Judicial Inst., Inc., http://www.flaschner.org (last visited July 22, 2009); Mich. Judicial Inst., http://courts.michigan.gov/mji (last visited July 22, 2009); N.Y. State Judicial Inst., http://www.courts.state.ny.us/ip/judicialinstitute/index.shtml (last visited July 22, 2009).

160. Mich. Judicial Inst., *supra* note 159.

biochemistry. The government officials involved can prepare a brief description of the process that will be employed and what that process entails. It may take time to acclimate to such a procedure initially, but as the practice becomes more commonplace judges will become more accustomed to the practice and better prepared to deal with the situations presented. Just a few years ago, the practice of electronic discovery also perplexed many judges. As the practice exploded in prevalence and importance, however, judges became more and more familiar with the requirements and processes involved. The same approach can be employed with search protocols. The introduction of a search protocol standard is by no means the end of the line for computers and the Fourth Amendment. Just as any major development in the legal world, defining the "right" approach to searching hard drives under the Fourth Amendment is a continuing process that will inevitably change as the technology involved evolves. The court in *West End* started the process and others can now follow accordingly.

This ex ante search protocol requirement may seem revolutionary when examined in light of Fourth Amendment jurisprudence in the physical context, but in the *virtual* context it is simply extending the same protections that individuals are afforded through a different framework. The complexities and technological issues behind computers and hard drives make these search protocols necessary in order to extend Fourth Amendment protections for physical information to its virtual counterpart. Requiring search protocols is certainly not an uncontroversial decision. It is, however, a decision that can adequately strike a balance between the need for law enforcement to obtain evidence and the privacy rights of this nation's citizenry. That balance is, and always has been, at the crux of any Fourth Amendment inquiry.[161]

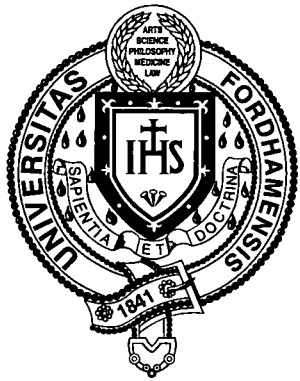
CONCLUSION

Conceptualizing hard drives under the Fourth Amendment has proven to be anything but an easy task. Contrary to what closed container approach advocates would have people believe, there is too much private information at stake to allow police or forensic analysts to conduct wholesale searches based on a warrant that is constitutionally required to specifically describe the nature of the evidence to be seized. Just because it is not feasible for a "perfect tool" to be developed by forensic analysts does not mean that there

161. *See* United States v. Knights, 534 U.S. 112, 118-19 (2001) ("The touchstone of the Fourth Amendment is reasonableness, and the reasonableness of a search is determined by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." (internal quotation marks omitted)).

should be no check against general exploratory searches in the virtual setting. Providing ex post judicial review of computer searches is not enough; the private information on the computer is still compromised—even if only viewed by the government officials and analysts involved. With the ever-expanding range of sensitive information individuals store on their computers, compromising the information to just one party is enough to lead to identity theft or a bevy of other unsavory results.

While the virtual file approach spelled out in *Carey* has its challenges, the alternative of classifying hard drives as single closed containers is fraught with constitutional problems. Adhering to the physical box model neglects the fact that computer technology is fundamentally different than anything the Fourth Amendment has been applied to in the past. Relying on determinations made by courts over a decade ago seems counterintuitive when one realizes the staggering speed at which computer technology evolves and improves. Modifying the virtual file approach to require search protocols, and thus rid itself of the inquiry into the searching officer's subjective intent, provides a workable model courts can employ—a model that will protect individual privacy while at the same time aiding law enforcement with proper guidance to carry out searches and ensuring that evidence discovered will be admissible at trial.


ARTS
SCIENCE
PHILOSOPHY
MEDICINE
LAW
IHS
SAPIENTIA
ET
DOCTRINA
1841
UNIVERSITAS
FORDHAMENSIS