COMPUTER SEIZURES AND SEARCHES: RETHINKING THE APPLICABILITY OF THE PLAIN VIEW DOCTRINE*

I. INTRODUCTION

Over the past two decades our society's dependence on computer technology has increased exponentially.[1] With the advent of smart phones, computer tablets, and other portable electronic-storage devices, our society is rarely without access to computers[2] and devices that can store electronic data.[3] This increased dependency has also increased the frequency with which police seek information stored on computers pursuant to search warrants.[4]

The Fourth Amendment generally requires that search warrants only be issued upon a showing of probable cause.[5] Further, a warrant must particularly describe the place to be searched and the items to be seized.[6] Courts have struggled to come to an understanding as to what this means when the objects of the search are a computer's hard drive and files.[7] In particular, problems have arisen in determining how specific the warrant must be in describing the items from the computer to be seized.[8] Due to the sheer volume of data that exists on the average computer, courts have been reluctant to require investigators to specify exactly what folders on a computer's hard drive they will be searching and exactly what type of files they are looking for.[9] Another concern has been, and continues to be, whether the plain view doctrine permits police to seize

* James T. Stinsman, J.D., Temple University Beasley School of Law, 2011. I would like to thank my wife, Chelsea, for her constant love and support. I would also like to extend my most sincere gratitude to the 2010–2011 staff and editors of the *Temple Law Review* for making Volume 83 a great success.

1. *See* U.S. CENSUS BUREAU, COMPUTER AND INTERNET USE IN THE UNITED STATES: 2003, at 1 fig.1 (2005), *available at* http://www.census.gov/prod/2005pubs/p23-208.pdf (noting that between 1984 and 2003 the percentage of American households with computers grew from 8.2% to 61.8%).

2. State v. Evers, 815 A.2d 432, 448 (N.J. 2003) ("Computers are in use in both homes and businesses, and, with the advent of the laptop, in almost every other conceivable place. Business people and students leave their homes with laptops, use them at other locations, and return home with them.").

3. Other possible electronic-storage devices include external hard drives, company servers, network storage devices, digital music players, cell phones, CDs, DVDs, removable USB drives, flash drives, external hard drives, and diskettes.

4. YALE KAMISAR ET AL., MODERN CRIMINAL PROCEDURE: CASES, COMMENTS AND QUESTIONS 319 (12th ed. 2008).

5. U.S. CONST. amend. IV.

6. *Id.*

7. See *infra* Part II.B for a discussion of the challenges courts have faced in attempting to apply traditional Fourth Amendment doctrine to electronic data searches.

8. See *infra* Part II.B.1 for a discussion of the particularity requirements in electronic data searches.

9. See *infra* Part II.B.2 for a discussion about what is included within the scope of a computer search warrant.

data relating to crimes—other than those described in the warrant—if they come across such data while performing a search within the scope of the warrant.[10]

In electronic data searches, the dichotomy between the particularity requirement and the plain view doctrine has sparked concern that such searches are becoming akin to the exploratory rummaging that the Framers of the Fourth Amendment sought to prevent.[11] Commentators, along with the courts, have struggled with how to best balance the protection of privacy interests with law enforcement's legitimate needs to conduct computer searches pursuant to criminal investigations. The two most notable proposed solutions are: (1) requiring investigators to provide ex ante search protocols—detailing the way in which they will conduct the search,[12] and (2) limiting or eliminating the application of the plain view doctrine for electronic data searches.[13] Both approaches, however, have been very slow to gain support among the courts.

This Comment explains how the proposed solutions clash with both Supreme Court precedent and the practical realities of our electronic-driven world.[14] As an alternative, this Comment argues that it is not the *category* of electronic data searches that requires special treatment, but rather, the *manner* in which the searches are carried out. Specifically, whenever the normal two-step process of searching before seizing is reversed, and an over-broad seizure takes place before the search the plain view doctrine should not apply.

Part II reviews the Fourth Amendment requirements for obtaining and executing a valid search and seizure pursuant to a warrant. Part II.A provides an overview of Fourth Amendment warrant requirements for traditional searches of physical spaces and seizures of physical objects. Parts II.B.1 and II.B.2 set forth the current approaches taken by courts in applying Fourth Amendment warrant requirements to searches of electronic-data containers and seizures of electronic evidence. Part II.B.3 acknowledges the dilemmas raised by electronic data searches and discusses the solutions that commentators have proposed and courts have implemented.

Part III.A demonstrates that the current approaches suggested by commentators, and implemented by some courts, fail to strike a proper balance between protecting privacy interests and ensuring police the means to conduct effective criminal investigations. Part III.A also attempts to explain why most courts have not implemented the suggestions. Finally, Part III.B proposes eliminating the plain view doctrine, not only for electronic data searches, but for all situations that require an initial over-seizure to take place before the actual search occurs.

10. See *infra* Part II.B.3 for a discussion of the role of the plain view doctrine in electronic data searches.

11. *See, e.g.*, RayMing Chang, *Why the Plain View Doctrine Should Not Apply to Digital Evidence*, 12 SUFFOLK J. TRIAL & APP. ADVOC. 31, 66 (2007) (noting that electronic-data warrants are turning into de facto general warrants).

12. See *infra* Part II.B.3.a for a discussion of search protocol requirements in electronic data searches.

13. See *infra* Part II.B.3.b for a discussion of suspending the plain view doctrine in electronic data searches.

14. See *infra* Part III.A for a discussion of flaws in the current proposed solutions.

II. OVERVIEW

A. *Traditional Application of the Fourth Amendment*

To understand the rules governing search and seizure of computer data, it is necessary to understand the basic principles of the Fourth Amendment. The Amendment pronounces:

> 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.[15]

The Amendment requires that a search warrant describe the things to be seized with sufficient particularity to prevent "general warrants"[16] akin to "exploratory rummaging" through a person's belongings.[17] This particularity requirement ensures that a search will be carefully tailored to only the specific area in which there is probable cause to search.[18] Once probable cause is demonstrated and the place to be searched is adequately described, investigators may search anywhere within the place where the object of their search is likely to be found.[19]

1. The Particularity Requirement

The particularity requirement has been used to prevent two different problems: (1) ambiguity or generality (i.e., warrants that fail to provide the executing officer guidance as to what exactly should be searched and seized); and (2) overbreadth (i.e., warrants that allow the executing officer to seize more than what is actually supported by probable cause).[20] A warrant satisfies the particularity requirement if it is "sufficiently definite to enable the searching officers to identify the property authorized

15. U.S. CONST. amend. IV.

16. Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971). General warrants have long been considered a violation of fundamental rights. Justice Bradley, writing for the Court in *Boyd v. United States*, explained the history of general warrants in the colonies:

> The practice had obtained in the colonies of issuing writs of assistance to the revenue officers, empowering them, in this discretion, to search suspected places for smuggled goods, which James Otis pronounced "the worst instrument of arbitrary power, the most destructive of English liberty, and the fundamental principles of law, that ever was found in an English law book," since they placed "the liberty of every man in the hands of every petty officer."

116 U.S. 616, 625 (1886).

17. *Coolidge*, 403 U.S. at 467.

18. Maryland v. Garrison, 480 U.S. 79, 84 (1987) (citing Andresen v. Maryland, 427 U.S. 463, 480 (1976)).

19. Unites States v. Ross, 456 U.S. 798, 820–21 (1982) (permitting officers to look for illegal weapons in closets, drawers, chests, and other closed containers within house described in warrant).

20. United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) (citing United States v. Abrams, 615 F.2d 541, 545–46 (1st Cir. 1980) (discussing ambiguity); United States v. Kow, 58 F.3d 423, 427 (9th Cir. 1995) (discussing overbreadth); Davis v. Gracey, 111 F.3d 1472, 1478–79 (9th Cir. 1997) (discussing both problems)).

to be seized,"[21] and "nothing is left to the discretion of the officer executing the warrant" as to what is to be taken.[22] At the same time, courts have been reluctant to strike down broad warrants where the case involves complex criminal schemes that require the assembly of a "paper trail."[23] Courts have recognized that the particularity requirement is satisfied if it is as specific as the circumstances will permit, depending on the type of property to be seized.[24]

The "paper trail" argument was put forth by the government in *United States v. Tamura*.[25] In *Tamura*, the government was authorized to seize evidence of certain payments received by the defendant, but was presented with a daunting three-step process for identifying the pertinent materials.[26] Realizing that this process would take too long, the government requested the help of the defendant's employees.[27] After the employees refused this request, the government seized several boxes and file drawers containing a large number of documents not specified in the warrant, which were stored at a different location.[28] The Eighth Circuit disapproved of the wholesale seizure of the documents, specifically disapproving the government's failure to return documents that were not part of the warrant after they were segregated.[29] Although the court did not find it necessary to suppress the material that was properly seized, they did recommend that "[i]n the comparatively rare instances where documents are so intermingled that they cannot feasibly be sorted on site, . . . the Government and law enforcement officials generally can avoid violating fourth amendment rights by sealing and holding the documents pending approval by a magistrate of a further search."[30]

21. United States v. Horn, 187 F.3d 781, 788 (8th Cir. 1999) (citing United States v. Strand, 761 F.2d 449, 453 (8th Cir. 1985)).

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

23. *See* Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976) (recognizing that in some document paper searches, "it is certain that some innocuous documents will be examined, at least cursorily," in order to decide if they are among the items to be seized); United States v. Wuagneux, 683 F.2d 1343, 1349 (11th Cir. 1982) (stating that cases concerning complex financial transactions and allegations of widespread fraud called for flexible interpretation of warrant due to difficulty in piecing together "paper puzzle" (internal quotation marks omitted)).

24. *See* United States v. Lowry, 675 F.2d 593, 595 (4th Cir. 1982) (holding that reference to "related correspondence" was precise enough, under circumstances of case, to include documents in connection with package specifically named in affidavit (internal quotation marks omitted)); Spinelli v. United States, 382 F.2d 871, 886 (8th Cir. 1967) (holding that warrant for "bookmaking paraphernalia" was specific enough because circumstances made precise description of things to be seized virtually impossible, and affiant can only be expected to provide description for "generic class of items" sought to be seized (internal quotation marks omitted)), *rev'd on other grounds*, 393 U.S. 410 (1969).

25. 694 F.2d 591 (9th Cir. 1982).

26. *Tamura*, 694 F.2d at 594–95. In order to find the relevant records of payment, the agents had to first review computer printouts, and then locate payment vouchers that corresponded with the particular record found in the printout, and finally the agents had to find the check that corresponded to that voucher. *Id.*

27. *Id.* at 595.

28. *Id.*

29. *Id.* at 596–97.

30. *Id.* at 595–96.

2. The Plain View Doctrine

One of the exceptions to the warrant requirement for seizures is the plain view doctrine.[31] Under this doctrine, police may seize an object without a warrant if (1) the police are lawfully in a position to view the object, (2) the object's incriminating character is immediately apparent, and (3) the officers have a lawful right to access the object.[32] Justice Stewart's plurality opinion in *Coolidge v. New Hampshire*[33] reasoned that requiring police officers to ignore such evidence until they were able to obtain a warrant would often be a "needless inconvenience," and could jeopardize officers' safety in certain situations.[34] Justice Stewart made it clear, however, that "plain view *alone* is never enough to justify the warrantless seizure of evidence."[35] Instead, the officer must have "a prior justification for an intrusion in the course of which he came inadvertently across a piece of evidence incriminating the accused."[36] The doctrine thus serves as a "supplement" to the prior justification, typically a search warrant issued for a different object.[37] The Court also expressly stated that the plain view doctrine was not to be used to extend a "general exploratory search" from one thing to another until something incriminating finally surfaces.[38] In *Texas v. Brown*,[39] another plurality opinion, the Court added an supplementary requirement to the plain view doctrine—the "inadvertency" requirement. The Court explained that the inadvertency aspect of the doctrine required that an officer "not 'know in advance the location of [certain] evidence and intend to seize it,' relying on the plain-view doctrine only as a pretext."[40]

The life of the inadvertency requirement was, however, short-lived. In *Horton v. California*,[41] the Court rejected the need for such a requirement. There, an investigator's affidavit established probable cause to search the defendant's home for the proceeds of a robbery and for guns thought to be used in that robbery; the magistrate's warrant, however, was only issued for the proceeds of the robbery.[42] During the search, the proceeds were not found, but the guns were.[43] The Court rejected the defendant's argument that the seizure of the guns was invalid because the police had expected to find them.[44] Justice Stevens noted that although many plain view seizures were inadvertent, the doctrine did not mandate such a requirement.[45]

31. Texas v. Brown, 460 U.S. 730, 738–39 (1983) (plurality opinion).

32. Minnesota v. Dickerson, 508 U.S. 366, 375 (1993) (citing Horton v. California, 496 U.S. 128, 136–37 (1990)).

33. 403 U.S. 443 (1971) (plurality opinion).

34. *Coolidge*, 403 U.S. at 467–68.

35. *Id.* at 468.

36. *Id.* at 466.

37. *Id.* at 466.

38. *Id.*

39. 460 U.S. 730 (1983) (plurality opinion).

40. *Brown*, 460 U.S. at 737 (alteration in original) (quoting *Coolidge*, 403 U.S. at 470).

41. 496 U.S. 128 (1990).

42. *Horton*, 496 U.S. at 130–31.

43. *Id.* at 131.

44. *Id.* at 130–31.

45. *Id.* at 130.

The Court found two fundamental flaws with requiring inadvertency.[46] First, the requirement was too subjective.[47] It required that courts determine whether the officer subjectively expected to find the object(s) while performing the search, which ran counter to the principle that "evenhanded law enforcement is best achieved by . . . objective standards of conduct."[48] Second, the Court found that an inadvertency requirement did not advance the prevention of general searches.[49] The interest in preventing general searches, the Court reasoned, was already served by the particularity requirement and the rule that any warrantless search be circumscribed by the exigencies which justify its initiation.[50] Because the particularity requirement adequately protected against general searches, mandating inadvertency was unnecessary.

B. Computer Data and the Particularity Requirement

Applying traditional warrant rules to electronic data has been no easy task for the courts, and the difficulties are immediately apparent.[51] Unlike searches for physical evidence, when officers search a computer, they typically seize the entire computer first, taking it off-site to conduct the search, often to a forensic computer lab.[52] Since the data that officers are usually searching for can generally be stored in many places on a computer, courts have struggled to come to a consensus as to how particular the description of the search's object must be.[53] Courts have also struggled to find common ground in determining if such searches can be limited in scope, and if so, what procedures are best for doing so.[54] The application of the plain view doctrine to computer searches has been at the heart of both of these issues.[55]

1. How Particularly Must the Object of the Search Be Described?

The Tenth Circuit has explained that particularity in computer searches "must affirmatively limit the search to evidence of specific federal crimes or specific types of material."[56] Because it is so difficult to describe the specific types of material to be seized from a computer, federal investigators often describe the object of the search in

46. *Id.* at 138.

47. *Id.*

48. *Id.*

49. *Id.* at 139.

50. *Id.* at 139–40.

51. *See generally* Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279 (2005) (noting that the emergence of digital evidence has created new facts that demand new law).

52. *See* United States v. Hill, 322 F. Supp. 2d 1081, 1088–89 (C.D. Cal. 2004) (noting that requiring investigators to search computer on-site would be more invasive to person's home or business than off-site computer search); *In re* Search of 3817 W. West End, 321 F. Supp. 2d 953, 958 (N.D. Ill. 2004) (noting that in case of computers, normal sequence of search before seizure is frequently inverted, with search occurring only after seizure has taken place).

53. See *infra* Part II.B.1 for a discussion of the particularity requirement in search warrants for digital evidence.

54. See *infra* Part II.B.2 for a discussion on the scope of digital evidence searches.

55. *See generally* Kerr, *supra* note 51.

56. United States v. Riccardi, 405 F.3d 852, 865 (10th Cir. 2005).

terms of the specific federal crime at issue. For example, in *United States v. Upham*[57] U.S. Customs agents monitoring a chat room received images depicting child pornography from a computer later discovered to be owned by a Kathi Morrissey and used by her then-boyfriend, Troy Upham.[58] The warrant authorized the seizure of "[a]ny and all computer software and hardware, . . . computer disks, disk drives," as well as "[a]ny and all visual depictions, in any format or media, of minors engaging in sexually explicit conduct [as defined by the statute]."[59] The agents conducted a search of Morrissey's home and took a computer and a number of diskettes.[60] The court upheld the particularity of the material to be seized, stating that the limiting language "of minors engaging in sexually explicit conduct" left little latitude to the executing officers.[61] Similarly, in *United States v. Campos*,[62] the Tenth Circuit upheld the seizure of a computer under a warrant which particularized only items directly related to child pornography.[63] In *United States v. Adjani*,[64] the Ninth Circuit upheld the search of defendant's computer where the warrant specifically authorized the seizure of evidence to show violations of a specific federal extortion statute.[65]

However, in *United States v. Hunter*,[66] where the search warrant of a home called for the seizure of "'[a]ll computers[,] . . . [a]ll computer storage devices[,] . . . [and all] computer software systems,'" without providing any detailed information relating the sought items to a specific federal crime, the court held that the warrant lacked sufficient limitation, and was more akin to the general warrants that the Fourth Amendment sought to prevent.[67] The court criticized the warrant's language as a "catch-all paragraph," and held that a warrant must specify the purpose for which computers are to be seized and specify the limitations for any subsequent search.[68]

Although the federal circuit courts that have addressed the issue generally apply a "federal crime or specific types of materials" particularity standard,[69] some federal

57. 168 F.3d 532 (1st Cir. 1999).

58. *Upham*, 168 F.3d at 533.

59. *Id.* at 535 (third alteration in original) (omission in original) (quoting warrant at issue).

60. *Id.* at 533.

61. *Id.* at 536 n.1 (internal quotation marks omitted).

62. 221 F.3d 1143 (10th Cir. 2000).

63. *Campos*, 221 F.3d at 1147–48 (noting that other jurisdictions have upheld similar warrants on same grounds) (citing United States v. Hall, 142 F.3d 988, 996–97 (7th Cir. 1998); United States v. Lacy, 119 F.3d 742, 746 (9th Cir. 1997)).

64. 452 F.3d 1140 (9th Cir. 2006).

65. *Adjani*, 452 F.3d at 1147.

66. 13 F. Supp. 2d 574 (D. Vt. 1998).

67. *Hunter*, 13 F. Supp. 2d at 584; *see also* United States v. Clough, 246 F. Supp. 2d 84, 87 (D. Me. 2003) (holding insufficient particularity where there was no mention of statutes, crimes, or illegality in affidavit); Burnett v. Florida, 848 So. 2d 1170, 1173–74 (Fla. Dist. Ct. App. 2003) (finding warrant application insufficient because it contained no crime-specific facts regarding likelihood that child pornography would be found on computer).

68. *Hunter*, 13 F. Supp. 2d at 584.

69. *See* United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) (upholding warrant issued for "[a]ny and all computer software and hardware, . . . computer disks, disk drives," and "[a]ny and all visual depictions, in any format or media, of minors engaging in sexually explicit conduct [as defined by the statute]" (third alteration in original) (omission in original)); United States v. Lacy, 119 F.3d 742, 746 (9th Cir. 1997)

district courts and some state courts have allowed for even less specificity.[70] For example, in *Maine v. Lehman*,[71] the particularity requirement was found to be met where the warrant authorized the seizure of "[a]ll computer equipment and computer related equipment . . . which [Defendant] would have been able to access" based on the nature of the criminal offense (child pornography) under investigation.[72]

2. What Is Within the Scope?

A warrant is overbroad if it includes items for which there is no probable cause to search.[73] It is the role of the reviewing court to "measur[e] the scope of the search . . . against the ambit of probable cause established by the affidavit upon which the warrant [was] issued."[74] However, in practice, this rule does very little to regulate computer searches.[75] As Professor Orin Kerr explains:

> Digital evidence alters the relationship between the size of the space to be searched and the amount of information stored inside it. In physical space, the particularity requirement limits the scope of a search to a place on the order of a house or apartment. . . . That limitation does not hold in the case of a computer search.[76]

(upholding warrant issued for search of computer equipment and concluding that "this type of generic classification is acceptable when a more precise description is not possible, and in this case no more specific description of the computer equipment sought was possible" (citations omitted) (internal quotation marks omitted)); Davis v. Gracey, 111 F.3d 1472, 1479 (10th Cir. 1997) (upholding warrant issued for "equipment . . . pertaining to the distribution or display of pornographic material in violation of state obscenity laws" (internal quotation mark omitted)).

70. *See* State v. Nuckolls, 617 So. 2d 724, 725–26 (Fla. Dist. Ct. App. 1993) (finding warrant authorizing search and seizure of "[d]ata stored on computer, including, but not limited to, magnetic media or any other electronic form, hard disks, cassettes, diskettes, photo optical devices and file server magnetic backup tapes" to be sufficiently particular); Commonwealth v. McDermott, 864 N.E.2d 471, 489 (Mass. 2007) (upholding as sufficiently particular warrant allowing search for any computer file pertaining to defendant's "Internet activity"); State *ex rel.* Macy v. One (1) Pioneer CD-ROM Changer, 891 P.2d 600, 604–05 (Okla. Civ. App. 1994) (upholding warrant that described discs containing "obscene material" (internal quotation marks omitted)).

71. 736 A.2d 256 (Me. 1999).

72. *Lehman*, 736 A.2d at 258–59, 261 (first alteration in original) (internal quotation mark omitted); *see also* People v. Ulloa, 124 Cal. Rptr. 2d 799, 802–03 (Cal. Ct. App. 2002) (holding that search of sodomy defendant's computer adequately described objects of search by authorizing items depicting "actual or simulated sexual acts between human beings" and "computers . . . containing any of the items noted above" (internal quotation marks omitted)).

73. Davis v. Gracey, 111 F.3d 1472, 1478 (10th Cir. 1997)

74. United States v. Fumo, 565 F. Supp. 2d 638, 646 (E.D. Pa. 2008) (first alteration in original) (quoting United States v. Christine, 687 F.2d 749, 753 (3d Cir. 1982)) (internal quotation marks omitted); *see also* Maryland v. Garrison, 480 U.S. 79, 84 (1987) (noting that scope of search "'is defined by the object of the search and the places in which there is probable cause to believe that it may be found'" (quoting Unites States v. Ross, 456 U.S. 798, 824 (1982))).

75. Kerr, *supra* note 51, at 302.

76. *Id.*

Because computers hold an immense amount of information,[77] and because it is difficult to know which file to access for specific material,[78] courts have allowed the scope of the warrant to be rather wide, often permitting investigators to search the entire computer.[79] This, in turn, has led to a trend wherein courts are admitting evidence through the plain view doctrine for items that were not within the warrant's scope.[80]

3. The Plain View Dilemma

As applied to electronic data searches, the plain view doctrine gives an officer searching a hard drive or other data container the lawful right to view each file to determine whether it is within the scope of the warrant.[81] If evidence of a different crime is intermingled in the files, and its incriminating character is immediately apparent, the evidence is deemed in plain view and hence admissible.[82] One commentator has noted this process of admitting evidence outside the scope of the warrant as having turned any digital property warrant into a de facto general warrant.[83]

As discussed below, some courts have attempted to come up with solutions to the digital implications of the interplay of Fourth Amendment particularity and the plain view doctrine.

a. The Carey *Approach and Search Protocols*

In *United States v. Carey*,[84] the defendant had been under investigation for the possession and possible sale of drugs.[85] After setting up controlled buys, the police

77. *Id.* (noting that in 2004 the average computer had capacity to hold equivalent of twenty million pages of text, roughly equivalent to half the material stored in first floor of average academic library, and that storage capacity has tendency to double almost every two years).

78. *See* United States v. Riley, 906 F.2d 841, 845 (2d Cir. 1990) ("[F]ew people keep documents of their criminal transactions in a folder marked '[crime] records.'"); Wisconsin v. Schroeder, 613 N.W.2d 911, 916 (Wis. Ct. App. 2000) (noting that if searches were limited as defendant requested then "it would be all too easy for defendants to hide computer evidence: name your porn file '1986.taxreturn' and no one can open it").

79. *See, e.g.*, United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) (holding search was "about the narrowest definable search and seizure reasonably likely to obtain the images"); Maine v. Lehman, 736 A.2d 256, 260–61 (Me. 1999) (holding that description was as narrow as it could possibly be given nature of the activity under investigation).

80. Chang, *supra* note 11, at 46; *see also* Rosa v. Commonwealth, 628 S.E.2d 92, 93 (Va. Ct. App. 2006) (finding deleted image files were in plain view where investigators acted reasonably in opening files); Frasier v. State, 794 N.E.2d 449, 449 (Ind. Ct. App. 2003) (holding that images of child pornography inadvertently opened by investigators fell within plain view, even though warrant only permitted seizure of evidence relating to marijuana).

81. *See* United States v. Miranda, 325 F. App'x 858, 860 (11th Cir. 2009) (holding that officers had right to view each computer file to determine whether file contained evidence of counterfeiting crimes described in warrant), *cert. denied*, 130 S. Ct. 740 (2009).

82. *See id.* (holding that computer files containing child pornography are in plain view when intermingled with other files found on computer being searched for counterfeiting crimes).

83. Chang, *supra* note 11, at 46.

84. 172 F.3d 1268 (10th Cir. 1999).

85. *Carey*, 172 F.3d at 1270.

obtained an arrest warrant for the defendant.[86] During the course of the arrest at the defendant's residence, the defendant consented to the search and provided the officers information on how to find drug-related materials.[87] A computer in the house was taken by the police, and a separate warrant was subsequently obtained to allow the police to search for "names, telephone numbers, . . . and other documentary evidence pertaining to the sale and distribution of controlled substances."[88] In the process of executing the warrant, the investigator encountered difficulties viewing certain files on the computer he was using to conduct the search.[89] The investigator then copied the files he was searching onto a disk and opened them on a different computer; after doing so, the investigator saw a ".jpg" file which, upon opening, was found to contain child pornography.[90] The investigator downloaded roughly 244 .jpg files, but only viewed some of them to determine that they contained child pornography.[91]

The Government's argument that the search was authorized by the plain view doctrine was ultimately rejected by the Tenth Circuit.[92] The court stated that the search was constrained to the items listed in the warrant.[93] Each of the files containing pornographic material, however, were labeled .jpg and the majority of them featured sexually suggestive file names.[94] The investigator testified that he was not looking for evidence of drug trafficking while opening the .jpg files and that he only resumed looking for drug-related data after completing his five-hour search for child pornography.[95] The court stated that after the investigator opened the first file and saw a photo of child pornography, the investigator was aware that the other sexually suggestive names and file types were likely to contain similar imagery.[96] According to the investigator's own testimony, he expected to find child pornography in every subsequent .jpg he opened after viewing the initial file.[97]

The court also suggested that when dealing with intermingled computer documents, law enforcement officers must first take an intermediate step of sorting the various documents, and then limit their search to those specified in the warrant.[98] Where documents are so intermingled with irrelevant documents, the searching officer must seal or hold the seized evidence pending approval from a magistrate of the conditions and limitations for any subsequent search.[99] Further, the court suggested that

86. *Id.*

87. *Id.*

88. *Id.* (internal quotation marks omitted).

89. *Id.* at 1271.

90. *Id.*

91. *Id.*

92. *Id.* at 1273.

93. *Id.* at 1274 (citing United States v. Reyes, 798 F.2d 380, 383 (10th Cir. 1986)).

94. *Id.*

95. *Id.* at 1273.

96. *Id.*

97. *Id.* The court explained in a footnote that, because the investigator testified he inadvertently discovered the first image, the holding was confined to the subsequent files that the investigator expected would contain images of child pornography. *Id.* at 1273, n.4.

98. *Id.* at 1275.

99. *Id.* (citing United States v. Tamura, 694 F.2d 591, 595–96 (9th Cir. 1982)).

"[t]he magistrate should then require officers to specify in a warrant which type of files are sought."[100]

One of the approaches cited, but not completely adopted, by *Carey* was the approach proposed by Raphael Winick.[101] Winick was one of the earliest commentators to address the particularity problem with computer data.[102] The key solution proposed by Winick was for magistrates to require affiants to submit the investigators' intended search methods for separating out the pertinent files and ensuring that only such files are searched.[103] For example, Winick suggested that magistrates require affiants to submit the keyword search terms that would be used when executing the warrant.[104] Winick claimed that the type of information stored in a particular file was easily ascertainable, and therefore suggested that affiants be required to declare what types of files they plan to search.[105] In sum, "[t]he basic principle is that before a wide-ranging exploratory search is conducted, the magistrate should require the investigators to provide an outline of the methods that they will use to sort through the information."[106]

In *In re Search of 3817 W. West End*,[107] the government was granted a warrant to search a home for certain enumerated items that the government claimed would establish tax fraud and to seize any computer that might be found within.[108] The subsequent search of the computer, however, was conditioned upon the government providing a search protocol describing what the police sought to seize, and the techniques the government planned to use to refrain from reviewing information that was unrelated to the investigation.[109] Citing *Carey* and a Department of Justice Manual,[110] the court stated that not only was it practical to require search protocol, but it was also legally required by the Fourth Amendment's particularity requirement.[111] Furthermore, the court suggested that practical considerations are precisely what dictate the degree of particularity required in a warrant.[112] The court also distinguished computer search cases from "knock and enter" cases because—unlike computer searches, which are performed in a controlled laboratory with few dangers—no one can

100. *Id.* (citing Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 108 (1994)).

101. *Id.* at 1275–76.

102. *See generally* Winick, *supra* note 100.

103. *Id.* at 107–08. This is a similar approach to the one that the Tenth Circuit adopted in *Carey*.

104. *Id.* at 108.

105. *See id.* (noting that those with reasonable familiarity with computers know that different programs store information in different formats).

106. *Id.*

107. 321 F. Supp. 2d 953 (N.D. Ill. 2004).

108. *Search of 3817 W. West End*, 321 F. Supp. 2d at 955.

109. *Id.* at 955–56. In so ruling, the court rejected the government's argument that the court was powerless to mandate such a requirement. *Id.* at 961.

110. U.S. DEP'T. OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (2002, updated 2009), *available at* http://www.cybercrime.gov/ssmanual/ssmanual2009.pdf.

111. *Search of 3817 W. West End*, 321 F. Supp. 2d at 961.

112. *Id.* (citing United States v. Spilotro, 800 F.2d 959 (9th Cir. 1986)).

know beforehand how many knocks must be made by "knock and enter" investigators who do not know what they will confront until they are on the scene.[113]

A search protocol approach has been advocated by very few courts.[114] Even the courts that have advocated for the inclusion of search protocols have not mandated that affiants include protocols whenever a computer search is sought, but have merely suggested that magistrates may, in their discretion, compel an affiant to provide protocols.[115] The vast majority of courts to take up the issue have not required computer investigators to provide search techniques to obtain a warrant.[116]

Search protocol requirements have received criticism from both courts and commentators.[117] Orin Kerr has criticized the practice, stating that magistrates do not have the forensic knowledge of computers to implement effective rules ex ante.[118] Kerr states that even investigators do not always know what forensic tool they will need until they actually begin looking at the data on the hard drive.[119] In addition, courts have also criticized search protocol requirements for their failure to take into account how easily files can be purposely mislabeled and the ease in which incriminating files can be mixed in with innocuously named directories.[120]

113. *Id.*

114. *See, e.g.*, *id.* at 958–63 (stating that the particularity requirement as applied to computer searches allows magistrates to mandate search protocols); United States v. Barbuto, No. 2:00CR197K, 2001 U.S. Dist. LEXIS 25968, at *11–12 (D. Utah 2001) (adopting Tenth Circuit protocol for sealing off on-site documents for later determination of relevancy). *But see* United States v. Maali, 346 F. Supp. 2d 1226, 1246 (M.D. Fla. 2004) (upholding search despite lack of protocols on ground that "[w]hile it may be preferable and advisable to set forth a . . . strategy[,] . . . failure to do so does not render computer search provisions unduly broad").

115. In *United States v. Burns*, a court in the same district that heard *Search of 3817 W. West End*, refused to read the decision as requiring search protocols in electronic data search warrant cases. *Burns*, No. 07CR556, 2008 U.S. Dist. LEXIS 35312, at *9 n.4 (N.D. Ill. Apr. 29, 2008). Rather, the *Burns* court interpreted *Search of 3817 W. West End* as holding that magistrates may require search protocols in such cases, but are not constitutionally mandated to do so. *Id.*; *see also* United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1006 (9th Cir. 2009) (recommending that magistrates require affiants to offer search descriptions before issuing warrant).

116. *See generally* United States v. Stabile, 633 F.3d 219 (2011); United States v. Hill, 459 F.3d 966 (9th Cir. 2006); United States v. Brooks, 427 F.3d 1246 (10th Cir. 2005); United States v. Upham, 168 F.3d 532 (1st Cir. 1999); United States v. Fumo, No. 06-319, 2007 U.S. Dist. LEXIS 80543 (E.D. Pa. Oct. 30, 2007); United States v. Cartier, No. 2:06-cr-73, 2007 U.S. Dist. LEXIS 7119 (D. N.D. Jan. 30, 2007); United States v. Kaechele, 466 F. Supp. 2d 868 (E.D. Mich. 2006); United States v. Shinderman, No. 05-67-P-H, 2006 U.S. Dist. LEXIS 8254 (D. Me. Mar. 2, 2006); United States v. Maali, 346 F. Supp. 2d 1226 (M.D. Fla. 2004).

117. *See, e.g.*, 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). See *supra* note 116 for a list of cases where courts have declined to require search protocol.

118. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 573, 575 (2005).

119. *Id.* at 575.

120. United States v. Gray, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999); *see also* United States v. Adjani, 452 F.3d 1140, 1150 (9th Cir. 2006) (stating that investigators should not be required to trust self-labeling of suspect because file names can be easily disguised or renamed); United States v. Harding, 273 F. Supp. 2d 411, 424 (S.D.N.Y. 2003) (noting that data can exist in numerous formats as evident by fact that text files can be readily converted into image files).

b. The CDT *Approach*

While scholars and commentators have often advocated the idea of suspending the plain view doctrine for search warrants concerning computer data, they readily concede that this would be a rather extreme approach that courts would be hesitant to adopt.[121] Indeed, from the inception of computer warrant cases in the late 1980s until August of 2009, even the courts that acknowledged the dangers of applying the plain view doctrine in electronic data searches were not willing to abandon the doctrine.[122]

In *United States v. Comprehensive Drug Testing, Inc.*,[123] the Ninth Circuit, sitting en banc, came as close as possible to eliminating the plain view doctrine from such searches without actually directly abolishing it.[124] The case involved the federal investigation of steroid use by Major League Baseball players.[125] In 2002, pursuant to a collective bargaining agreement between Major League Baseball and its players' association, the League arranged for "suspicionless drug testing of all players" to determine the prevalence of banned-drug use among the players.[126] The testing was to be performed by an independent party, Comprehensive Drug Testing, Inc. ("CDT"), and players were told that all test results would remain confidential and anonymous. However, during an investigation of the Bay Area Lab Cooperative (BALCO),[127] federal agents learned of ten players who had tested positive in the CDT testing and ultimately obtained and executed a search warrant for computer records at CDT's Long Beach office.[128] The warrant was limited to the records of the ten players for whom the government had probable cause.[129] When the government executed the warrant, drug

121. Chang, *supra* note 11, at 65; Kerr, *supra* note 118, at 583–84; *see also* Derek Regensburger, *Bytes, BALCO, and Barry Bonds: An Exploration of the Law Concerning the Search and Seizure of Computer Files and an Analysis of the Ninth Circuit's Decision in* United States v. Comprehensive Drug Testing, Inc., 97 J. CRIM L. & CRIMINOLOGY 1151, 1207 (2007) (advocating elimination of plain view doctrine in all computer searches, except where "casual glance" is enough to discover incriminatory nature of object); Donald Resseguie, Note, *Computer Searches and Seizure*, 48 CLEV. ST. L. REV. 185, 198 (2000) (arguing that under current law, plain view doctrine is inapplicable to closed computer files).

122. *See, e.g.*, United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999) (refusing to even address issue of what constitutes plain view in context of computer searches).

123. 579 F.3d 989 (9th Cir. 2009).

124. Orin Kerr, *How the Ninth Circuit Tried to End Plain View for Computer Searches Without Ending Plain View for Computer Searches*, VOLOKH CONSPIRACY (Aug. 26, 2009, 8:42 PM), http://volokh.com/posts/1251325479.shtml.

125. *Comprehensive Drug Testing*, 579 F.3d at 993.

126. *Id.*

127. The Bay Area Lab Cooperative is now widely known as BALCO after the steroid scandal shook Major League Baseball, beginning with *San Francisco Chronicle* journalists Mark Fainaru-Wada and Lance Williams's coverage of the story in October 2004. MARK FAINARU-WADA & LANCE WILLIAMS, GAME OF SHADOWS: BARRY BONDS, BALCO, AND THE STEROIDS SCANDAL THAT ROCKED PROFESSIONAL SPORTS 207, 215–16 (2006).

128. *Comprehensive Drug Testing*, 579 F.3d at 993–94. The case involved two separate warrants (one stemming from the Central District of California and one from the District of Nevada), and a motion to return items seized pursuant to FED. R. CRIM. PROC. 41(g). *Id.* at 993–94. For the purposes of brevity, only the warrant issued in the Central District of California is addressed here.

129. *Id.* at 993.

testing results of hundreds of players and individuals outside the game of baseball were seized and reviewed by the investigators.[130]

In *Comprehensive Drug Testing*, the court stated early in its discussion that it was taking "the opportunity to guide our district and magistrate judges in the proper administration of search warrants . . . for electronically stored information, so as to strike a proper balance between the government's legitimate interest in law enforcement and the people's right to privacy and property in their papers and effects."[131] Throughout the opinion, the court announced numerous new procedural rules that the government must adhere to when applying for and executing a search warrant for digital evidence.

First and foremost, the court stated that "the 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."[132] Further, if the government refuses to do so, the court stated that the magistrate should either order that the data be segregated by an independent third party under the supervision of the court or completely deny the warrant altogether.[133] In so ruling, the Ninth Circuit granted the magistrate judge a seemingly unprecedented power to deny a warrant otherwise supported by probable cause and describes with sufficient particularity the place to be searched and things to be seized.

Although the court recognized the government's legitimate need to gather large amounts of electronic data and carefully examine the data for concealed or disguised evidence, it reasoned that granting broad authorization to examine this electronic data "creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant."[134] Due to the unique nature of computer searches, therefore, the court called on judicial officers to exercise greater vigilance in seeking an equitable balance between the interests of law enforcement and the right of individuals to be free from unreasonable searches and seizures.[135]

130. *Id.*

131. *Id.* at 994.

132. *Id.* at 998.

133. *Id.*

134. *Id.* at 1004 (citing United States v. Hill, 459 F.3d 966 (9th Cir. 2006)).

135. *Id.* The court provided the following summation for how magistrates are to exercise this vigilance:

> 1. Magistrates should insist that the government waive reliance upon the plain view doctrine in digital evidence cases.
>
> 2. Segregation and redaction must be either done by specialized personnel or an independent third party. . . .
>
> 3. Warrants and subpoenas must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other judicial fora.
>
> 4. The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents.
>
> 5. The government must destroy or, if the recipient may lawfully possess it, return non-responsive data, keeping the issuing magistrate informed about when it has done so and what it has kept.

Id. at 1006 (citations omitted).

III. DISCUSSION

The dichotomy between the Fourth Amendment's particularity requirement and the plain view exception has proven problematic in electronic data searches conducted pursuant to search warrants.[136] Due to the practical concerns associated with trying to find the evidentiary needle in the computer haystack, courts have been reluctant to require narrowly prescribed descriptions of the objects of searches, thereby enabling investigators to search entire computers.[137] This wide scope has led to the introduction, at trial, of plain view evidence for which there was never a showing of probable cause.[138] Both courts and commentators have shown concern that this dichotomy has created a situation that is scarily similar to the general warrants that the Fourth Amendment was intended to protect against.[139]

Commentators whom have advocated limiting the application of the plain view doctrine to electronic data searches have done so by stressing how electronic searches are factually different than physical searches, and thus require different legal standards.[140] The remainder of this Comment proposes that this is an unnecessary argument for achieving a limited application of the plain view doctrine. Instead, this Comment proposes that digital evidence searches are factually analogous to physical searches that require the government to seize an abundance of paper documents that will be searched off-site at a later date. The plain view doctrine should thus be eliminated wherever the seizure of objects takes place before the search has occurred. This solution is superior to other previously proposed solutions because it is consistent with the rationales underlying the Fourth Amendment, is reconcilable with case precedent, and does not arbitrarily draw lines between electronic data searches and comparable searches of physical documents. It further provides investigators with a reasonable alternative search process where the plain view doctrine would still be applicable: the investigator would simply need to first perform the search on-site, and then seize the pertinent evidence—whether particularly described in the warrant or discovered through plain view—just as in the case of traditional searches and seizures.

136. See *supra* Part II.B.3 for a discussion on how courts have applied the plain view doctrine to computer searches.

137. *See* Kerr, *supra* note 51, at 301–02 (noting that if search protocol is not regulated, any justification for search may permit investigators to look through "a small city's worth of private information").

138. One common scenario involves the discovery of child pornography while conducting an electronic search pursuant to a warrant for a non-sex related crime. *See generally* United States v. Upham, 168 F.3d 532 (1st Cir. 1999); United States v. Harding, 273 F. Supp. 2d 411 (S.D.N.Y. 2003); United States v. Gray, 78 F. Supp. 2d 524 (E.D. Va. 1999); Frasier v. State, 794 N.E.2d 449 (Ind. Ct. App. 2003).

139. *See* Chang, *supra* note 11, at 66 (noting that electronic data warrants are turning into de facto general warrants).

140. *Id.* at 35–38 (noting peculiar nature of digital property as compared to "'papers' and 'effects' that the Founding Fathers contemplated when adopting Fourth Amendment"); Kerr, *supra* note 118, at 536–47 (arguing that old rules created for physical world do not adequately govern in digital world); Resseguie, *supra* note 121, at 212–13 (recognizing that search and seizure of computers and computer data presents new challenges to legal system).

A. Problems with Current Solutions

1. The Flawed Analysis of *Carey* and the Shortcomings of Search Protocols

Courts that have attempted to limit the plain view doctrine's applicability in electronic data searches have had a difficult time finding support in the case law to justify such a step.[141] In *United States v. Carey*,[142] the court reasoned that the plain view doctrine did not apply because after the investigator opened the first pornographic photo, he subjectively "expected to find child pornography and not material related to drugs."[143] The court, which suppressed all of the pornographic pictures except for the first picture that was found, justified its differential treatment of the images on the grounds that the investigator had "inadvertently discovered the *first* image during his search for documents relating to drug activity."[144] Such reasoning, however, effectively amounted to a reinstatement of the inadvertency requirement that the Supreme Court expressly abandoned in *Horton v. California*.[145] *Horton* held "that even though inadvertence is a characteristic of most legitimate 'plain-view' seizures, it is not a necessary condition."[146] The Court further explained:

> [E]venhanded law enforcement is best achieved by the application of objective standards of conduct, rather than standards that depend upon the subjective state of mind of the officer. The fact that an officer is interested in an item of evidence and fully expects to find it in the course of a search should not invalidate its seizure if the search is confined in area and duration by the terms of a warrant or a valid exception to the warrant requirement.[147]

The *Carey* court incorrectly relied on the investigator's subjective state of mind when it rejected the government's plain view argument.

The *Carey* court also proposed that magistrates should require search-warrant affiants to specify what type of files they are seeking,[148] an idea first introduced by Raphael Winick.[149] Requiring affiants to specify the type of files they seek is problematic, however, because of the ease in which individuals can disguise evidence of a crime by intentionally mislabeling files and distorting their file type.[150] Winick further suggested that magistrates should require investigators to provide a detailed description on *how* they planned to search the specified files, such as by requiring affiants to provide a list of the key word searches and any other search techniques they

141. The *Comprehensive Drug Testing* court, for example, failed to provide any precedent to support its laundry list of new rules to guide magistrate judges in the circuit. See *supra* note 135 for a list of these rules.

142. 172 F.3d 1268 (10th Cir. 1999).

143. *Carey*, 172 F.3d at 1273.

144. *Id.* at 1273 n.4.

145. 496 U.S. 128 (1990); *see also* Ziff, *supra* note 117, at 853 (noting that *Carey*'s "reliance on subjective intent is contrary to *Horton v. California*, which held that the subjective intent of a searching officer does not invalidate an otherwise valid search and seizure").

146. *Horton*, 496 U.S. at 130.

147. *Id.* at 138.

148. *Carey*, 172 F.3d at 1275 (citing Winick, *supra* note 100, at 108).

149. Winick, *supra* note 100, at 108.

150. Ziff, *supra* note 117, at 863.

were planning to perform.[151] However, if the investigators do not have specific information (such as a person's name or an insurance claim number) it may be hard for investigators to know what search terms may be useful until after they begin a preliminary search of the computer.[152]

Furthermore, ex ante search protocol requirements do not find any support in the language of the Fourth Amendment or U.S. Supreme Court precedent. In *Dalia v. United States*,[153] the Court held that neither the language of the Fourth Amendment nor any of the Court's interpretations of the language suggest that investigators must specify exactly how they plan on executing the search.[154] Determining how to conduct a search, the Court reasoned, is a matter better left to the discretion of the executing investigator.[155] This rationale is even more applicable when the affiant is a police officer with limited computer knowledge and the executing investigator is a highly trained computer-lab technician, as is often the case in electronic data searches.[156]

2. *CDT*'s Lack of Precedent for Search Warrant Requirements

In *United States v. Comprehensive Drug Testing, Inc.*,[157] the court recognized that "over-seizing" was inherent in computer search warrants.[158] To strike a balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures, the court recommended that magistrates insist "that the government waive reliance upon the plain view doctrine" when applying for electronic evidence search warrants.[159] If the government fails to waive, the magistrate can either appoint a third party to first segregate the searchable from the non-searchable, or the magistrate could simply deny the warrant.[160] In creating this waiver rule, the court failed to cite a single case that has given magistrates the authority to deny a warrant based on the government's failure to promise that it will not use the plain view doctrine.[161] As Professor Kerr has pointed out, there does not appear to be any precedent to support such a denial.[162] If a warrant is based on probable cause and is

151. Winick, *supra* note 100, at 108.

152. Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193, 211 (2005) (citing Susan W. Brenner & Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 MICH. TELECOMM. TECH. L. REV. 39, 60–63, 81–82 (2002)).

153. 441 U.S. 238 (1979).

154. *Dalia*, 441 U.S. at 257.

155. *Id.* at 257–58.

156. *See* Kerr, *supra* note 118, at 537–38 ("[C]omputer forensics analysis typically is performed pursuant to a search warrant by a trained analyst at a government forensics laboratory.").

157. 579 F.3d 989 (9th Cir. 2009).

158. *Comprehensive Drug Testing*, 579 F.3d at 1006.

159. *Id.* at 998.

160. *Id.*

161. *Id.* In fact, the court did not cite a single case for any of its five new proposals. *See id.* at 1006. See *supra* note 135 for the court's proposals.

162. Kerr, *supra* note 124.

sufficiently particular under the Fourth Amendment, the magistrate would be required to issue a warrant.[163]

Although *Comprehensive Drug Testing* did not directly abolish the plain view doctrine for computer searches, some commentators have advocated this solution.[164] As RayMing Chang, a proponent of abandonment admits, such a step is "perhaps the most drastic action that can be taken to remedy the problem of digital property searches turning into general searches."[165] While recognizing that courts will have to distinguish electronic searches from physical searches to justify a deviation from the case law establishing the plain view doctrine, Chang provides no insight as to how a court would be able to circumvent plain view precedent.[166] Kerr has also recognized that abolishment of "the plain view exception may best balance the competing needs of privacy and law enforcement."[167] Although Kerr states that it is too early for Congress or the courts to impose such a rule, as the dynamics of computer searches become more relevant with the passage of time, he argues that the elimination of the plain view doctrine may seem less severe.[168] As with Chang, however, Kerr does not suggest how the courts could reconcile this rule with the current Supreme Court precedent concerning the plain view doctrine.[169]

B. Suspending Plain View Beyond Electronic Data Searches

1. Avoiding Arbitrariness

Professor Kerr argues that electronic data searches are different from the traditional searches for physical evidence.[170] In traditional physical searches, the police seek permission to look through a physical space for a particular piece of evidence.[171] The officer then seeks to remove that evidence from that physical space.[172] This is what Kerr identifies as the "search-and-retrieve mechanism."[173] Digital searches are different, Kerr explains, in that they require an additional step to the search-and-retrieve process.[174] In the course of the common computer search, the investigator seeks to search a physical space for a computer storage device and take the device

163. FED. R. CRIM. P. 41(d)(1) (stating that magistrate *must* issue warrant when there is probable cause).

164. *See, e.g.*, Chang, *supra* note 11, at 65–66 (noting that, while drastic, abolishing digital plain view is "only effective way of forestalling the negative effects of the plain view doctrine's application"); *see also* Kerr, *supra* note 118, at 583–84 (noting that "abolishing the plain view exception may best balance the competing needs of privacy and law enforcement," but stating that it is still too early to abandon rule).

165. Chang, *supra* note 11, at 65.

166. *Id.* at 65–66. Instead of offering any precedent or ways to challenge the plain view doctrine's applicability in digital searches, Chang merely states that "the pros outweigh the cons." *Id.* at 66.

167. Kerr, *supra* note 118, at 583.

168. *Id.* Professor Kerr did not, however, provide any reason as to why he thinks it is too early for abandonment of plain view.

169. *Id.* at 583–84.

170. Orin S. Kerr, *Search Warrants in an Era of Digital Evidence*, 75 MISS. L.J. 85, 90 (2005).

171. *Id.*

172. *Id.*

173. *Id.*

174. *Id.*

away from that physical space.[175] The investigator then seeks to perform a further search, off-site at a later date.[176] This process can be seen as changing the search-and-retrieve mechanism into a retrieve-and-search mechanism.[177] Simply put, most computer searches pursuant to a valid warrant, unlike most traditional physical searches, require the seizure *before* the search.[178]

It is a mistake, however, to think of this retrieve-and-search process as a paradigm that is unique to digital evidence searches.[179] Although *most* physical searches do not require a departure from the usual search-and-retrieve process, there are "rare instances where documents are so intermingled that they cannot feasibly be sorted on site."[180] An example of such a "rare instance" would be the seizure of an office filing system, as was the case in *United States v. Tamura*.[181]

Most commentators on computer searches have recognized the glaring need to balance the competing interest of preserving the privacy rights of individuals while allowing law enforcement appropriate flexibility to adequately conduct searches.[182] Courts have often recognized the practical needs of law enforcement to seize large quantities of intermingled data to access the desired evidence.[183] In order for the government to locate the desired evidence, they will have to examine a great number of files, and once they have examined any given file, the government can claim that it was in plain view.[184] It is this current application of the plain view doctrine that has created "a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant."[185]

175. *Id.*

176. *Id.*

177. *See In re* Search of 3817 W. West End, 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.").

178. *See* Kerr, *supra* note 170, at 90 ("The dynamic is . . . physical seizure, and then electronic search.").

179. *See* United States v. Hargus, 128 F.3d 1358, 1363 (10th Cir. 1997) (upholding wholesale seizure of file cabinets because of practical concerns of on-site sorting); Crooker v. Mulligan, 788 F.2d 809, 812 (1st Cir. 1986) (upholding seizure of documents, both incriminating and innocuous, which although not specified in warrant, were intermingled with relevant documents); United States v. Tamura, 694 F.2d 591, 597 (9th Cir. 1982) (permitting wholesale seizure where motivated by considerations of practicality rather than desire to engage in "fishing" scheme); United States v. Hillyard, 677 F.2d 1336, 1340 (9th Cir. 1982) ("If commingling prevents on-site inspection, and no other practical alternative exists, the entire property may be seizable, at least temporarily.").

180. *Tamura*, 694 F.2d at 595.

181. See *supra* notes 25–30 and accompanying text for a discussion of *Tamura*. *See also* United States v. Shilling, 826 F.2d 1365, 1369 (4th Cir. 1987) (permitting investigators to seize filing cabinets to search at a later time).

182. *E.g.*, Regensburger, *supra* note 121, at 1201; Kerr, *supra* note 118, at 583; United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1006 (9th Cir. 2009).

183. *See, e.g.*, United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) (permitting seizure of all computer due, in part, to difficulties of searching on-site); United States v. Hill, 322 F. Supp. 2d 1081, 1089–90 (C.D. Cal. 2004) (holding that police were not required to search defendant's computer at scene, but were permitted to seize computer for off-site search).

184. See *supra* Part II.B.3 for a discussion of plain view application to electronic data searches.

185. *Comprehensive Drug Testing*, 579 F.3d at 1004.

Preventing such general warrants is the most notable reason given for limiting or eliminating the application of the plain view doctrine in electronic data searches.[186] However, the rationale applies equally to physical searches of intermingled documents as it does to electronic data searches. In both instances, investigators have the practical need to first overseize a great number of files or records, which will be searched at a later time.[187] In the physical document searches, investigators will have to examine, at least cursorily, a great number of files to determine whether they contain the desired evidence.[188] Once the document has been examined, investigators will be able to claim that the document was in plain view.[189]

Attempting to distinguish electronic evidence cases from these physical document searches would simply be a game of arbitrary line-drawing.[190] In both instances, it is the sheer volume of information that requires that the seizure take place before the search is performed. Moreover, it is certainly plausible that a search of intermingled physical documents (e.g., from the files of an accountant's office) could contain more information than an electronic data search of a drug dealer's home computer.[191] The argument, therefore, that only computer searches are large enough to confer special treatment is unwarranted.

Furthermore, distinguishing searches of electronic data from searches of intermingled physical documents will bring about inequitable results. Consider, for example, the following hypothetical scenarios:

Imagine that federal investigators have probable cause to believe that Joey Technobookie is taking bets on sporting events through his website www.technobook.com in violation of the federal transmission of wagering information statute.[192] The investigators obtain a search warrant for a computer they found while executing a valid search at Technobookie's house. While performing the computer search at a crime lab, investigators come across a document in which Technobookie incriminates himself as having taken part in a recent bank robbery, describing to a

186. *Id.*; *see also* Chang, *supra* note 11, at 65 (noting that combating general warrant is most compelling reason for eliminating plain view doctrine from digital searches); Kerr, *supra* note 118, at 583–84 (noting that elimination of plain view doctrine from digital searches is imperfect solution, but it may be best available way to protect privacy interests).

187. *Compare* United States v. Tamura, 694 F.2d 591, 597 (9th Cir. 1982) (permitting wholesale seizure of physical documents where motivated by considerations of practicality rather than desire to engage in "fishing" scheme) (internal quotation marks omitted)), *and* United States v. Hillyard, 677 F.2d 1336, 1340 (9th Cir. 1982) ("If commingling prevents on-site inspection, and no other practical alternative exists, the entire property may be seizable, at least temporarily."), *with* United States v. Hill, 322 F. Supp. 2d 1081, 1087–89 (C.D. Cal. 2004) (finding seizure of computer media was proper, even in absence of statement in affidavit that inspection was not feasible on site), *rev'd in part*, 459 F.3d 966 (9th Cir. 2006).

188. Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976) (recognizing that in some document paper searches, "it is certain that some innocuous documents will be examined, at least cursorily," in order to decide if they are item to be seized).

189. *Comprehensive Drug Testing*, 579 F.3d at 1004–05.

190. It is precisely the arbitrariness of differentiating between the two situations that has caused courts to apply the rules of physical-search cases to electronic-search cases.

191. To go even one step further, it is certainly plausible that a medical record-storage company's warehouse would contain more information than a USB flash drive.

192. 18 U.S.C. § 1084 (2006).

friend in an online chat that "we made out with $62,000," the exact amount taken from the bank.

Federal investigators also have probable cause to believe that Tommy Simplebook has been taking sports bets at a local bar, the Stateline Sports Pub, also in violation of the wagering statute.[193] The investigators obtain a valid warrant to search Simplebook's house. While performing the search, investigators enter Simplebook's garage where they find stacks of cardboard boxes. Investigators begin to look through the first box and realize that the boxes contain, in no particular order, Simplebook's weekly golf scorecards, tax return statements, paystubs, appliance owner manuals, and some betting tabulations. The investigators gather the boxes and take them back to the police station. In a subsequent search at the police station one of the investigators comes across a Stateline Sports Pub napkin with writing on it that says, "PUT THE MONEY IN THE BAG AND DON'T SAY A WORD." The investigator immediately recognizes this note as fitting the description of the note described to him by a bank teller while investigating a recent bank robbery.

Although these two scenarios are very similar, the outcomes will be extremely different if the elimination of the plain view doctrine is only applied to computer searches. Tommy Simplebook's bank note would be admissible at trial against him, while Joey Technobookie's incriminating statement would be excluded. As one court stated fittingly, "[t]here is neither a heightened nor a reduced level of protection for information stored on computer [sic], as there is 'no justification for favoring those who are capable of storing their records on computers over those who keep hard copies of their records.'"[194] Preventing search warrants from turning into de facto general warrants is no less a concern where the retrieve-and-search case is one concerning physical items instead of electronic data. Regardless of whether the object seized to be searched is a lawyer's computer system or a doctor's physical medical records, the privacy interest is the same.

2. Reconciling Precedent

By extending the abolishment of the plain view doctrine to any documentary warrant where the search-and-retrieve procedure is reversed, the Supreme Court's application of the plain view doctrine in *Horton v. California*[195] can be distinguished. Indeed, the rationale offered by the Court is simply inapplicable to cases involving a retrieve-and-search process pursuant to a warrant.

In *Horton*, not only did the Court do away with the inadvertency requirement of the plain view doctrine, but it also laid out the rationale behind the exception.[196] The Court explained that the right of security in one's person and property is susceptible to invasion in distinct ways by seizures as compared to searches.[197] "A search

193. *Id.*

194. United States v. Vilar, No. S3 05-CR-621, 2007 U.S. Dist. LEXIS 26993, at *117 (S.D.N.Y. Apr. 4, 2007) (quoting United States v. Hunter, 13 F. Supp. 2d 574, 584 (D. Vt. 1998)).

195. 496 U.S. 128 (1990).

196. *See Horton*, 496 U.S. at 134 (stating that plain view doctrine is an exception to warrant requirement only with respect to seizures, not searches).

197. *Id.* at 133.

compromises the individual interest in privacy; a seizure deprives the individual of dominion over his or her person or property."[198] As the Court has previously stated, "[a] 'seizure' of property occurs when there is some meaningful interference with an individual's possessory interests in that property."[199] Although the plain view doctrine is often recognized as an exception to the general rule that a warrantless search is presumptively unreasonable, the *Horton* Court noted that this conception overlooks the important difference between a search and a seizure.[200] The Court stated that if an object was already in plain view, the seizure of that object would not involve any invasion of privacy.[201] It would, however, invade the owner's possessory interests in the property.[202] The plain view doctrine, therefore, is a warrant requirement exception that addresses the concerns surrounding seizures, not searches.[203] The Court later stated:

> The prohibition against general searches and general warrants serves primarily as a protection against unjustified intrusions on *privacy*. But reliance on *privacy* concerns . . . is misplaced when the inquiry concerns the scope of an exception that merely authorizes an officer with a lawful right of access to an item to *seize* it without a warrant.[204]

The Court's rationale for applying the plain view exception to a warrant requirement thus rests on the traditional search-and-retrieve process.[205] From the Court's standpoint, application of the plain view doctrine does not infringe on an individual's privacy interests.[206] Rather, application of the plain view doctrine can only infringe on an individual's possessory interests.[207] This however is not the case when the seizure occurs before the search.

Where the traditional search-and-retrieve process is reversed, and the seizure occurs before the search, the owner's possessory interests have already been infringed, albeit a reasonable infringement, so long as the warrant is supported by probable cause and is sufficiently particular.[208] Given that practical considerations dictate that the scope of the warrant in such cases be rather wide,[209] the individual's privacy interests are clearly a concern. The particularity requirement's inability to adequately protect the

198. *Id.* (citing United States v. Jacobsen, 466 U.S. 109, 113 (1984)).

199. *Jacobsen*, 466 U.S. at 113.

200. *Horton*, 496 U.S. at 133.

201. *Id.*

202. *Id.* at 134.

203. *Id.*

204. *Id.* at 141–42 (emphases added).

205. See *supra* notes 170–81 and accompanying text for a discussion of the differences between the traditional search-and-seize process and the wholesale seize-and-search process used in electronic data searches.

206. *Horton*, 496 U.S. at 133, 141–42.

207. *Id.* at 134.

208. U.S. CONST. amend. IV.

209. *See, e.g.*, United States v. Hargus, 128 F.3d 1358, 1363 (10th Cir. 1997) (upholding wholesale seizure of file cabinets because of practical concerns with on-site sorting); United States v. Tamura, 694 F.2d 591, 596 (9th Cir. 1982) (permitting wholesale seizure where motivated by considerations of practicality); United States v. Hillyard, 677 F.2d 1336, 1340 (9th Cir. 1982) ("If commingling prevents on-site inspection, and no other practical alternative exists, the entire property may be seizable, at least temporarily.").

individual's privacy rights in such cases causes the plain view doctrine to not only impede on property rights, but privacy rights as well.[210]

The Court's distinction between privacy concerns and property concerns is well placed where the traditional search-and-seize process is at play. However, when the process is reversed, the distinction between the two is blurred. In seize-and-search cases the dichotomy between the particularity requirement and the plain view doctrine become so interdependent that both have the ability to impede an individual's privacy and property rights. The Court's rationale that the Fourth Amendment's prohibition against general searches and general warrants is adequately guarded by the particularity requirement does not apply to cases which require an overseizure before a search is performed, and thus the rationale for permitting the plain view doctrine as an exception to the warrant requirement is misplaced.

However, if investigators were simply to search the data on-site, under reasonable time constraints, and seize merely the data that was the object of the search or other incriminating evidence found in plain view, the *Horton* rationale for plain view would still be completely applicable. By using a traditional search-and-retrieve model, therefore, investigators would still be able to utilize the plain view doctrine. For, under the traditional model, the plain view doctrine cannot infringe on an individual's privacy interest.[211]

IV. CONCLUSION

Electronic data has become a crucial aspect of criminal investigations. Its importance in police investigations will only increase with the advent of new technology. However, the problems that courts are now encountering in how to balance privacy interests and law enforcement's legitimate investigatory needs stem back to a pre-computer era. When cases concerning vast documentary seizures came before the courts in the dawn of the computer age, the inability of investigators to actually search through every single document in every single file–created an inherent guard against excessive intrusion upon privacy interests.[212] Now, the sophisticated search techniques implemented in electronic data searches leave no page unturned.[213]

As the Court warned three decades ago in *Andresen v. Maryland*,[214] "there are grave dangers inherent in executing a warrant authorizing a search and seizure of a

210. *Cf. Horton*, 496 U.S. at 136, 141 ("[T]he seizure of an object in plain view does not involve an intrusion on privacy. If the interest in privacy has been invaded, the violation must have occurred before the object came into plain view and there is no need for an inadvertence limitation on seizures to condemn it." (footnote omitted)).

211. *Id.* at 136, 141 ("If the interest in privacy has been invaded, the violation must have occurred before the object came into plain view").

212. It is hard to imagine that in 1976 the Court ever imagined a keyword search scanning every line of the equivalent of twenty million pages of text when it stated: "[I]t is certain that some innocuous documents will be examined, at least cursorily." Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976). With current technology, even physical documents in today's day and age are easily scanned into computers to aid the investigator in her search.

213. With current technology, even physical documents in today's world are easily scanned into computers to aid the investigator in her search.

214. 427 U.S. 463 (1976).

person's papers that are not necessarily present in executing a warrant to search for physical objects whose relevance is more easily ascertainable."[215] The Court directed that "responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy."[216] To guard against such intrusions upon privacy, the time has come for the plain view doctrine to be suspended whenever the warrant allows for an overbroad seizure of documentary material to take place before the search is performed.

215. *Andresen*, 427 U.S. at 482 n.11.

216. *Id.*