University of Cincinnati Law Review

Volume 79 | Issue 3 Article 6

10-17-2011

THE PLAIN (OR NOT SO PLAIN) VIEW DOCTRINE: APPLYING THE PLAIN VIEW DOCTRINE TO DIGITAL SEIZURES

Kate Brueggemann Ward

THE PLAIN (OR NOT SO PLAIN) VIEW DOCTRINE: APPLYING THE PLAIN VIEW DOCTRINE TO DIGITAL SEIZURES

*Kate Brueggemann Ward**

I. INTRODUCTION: THE POWER OF THE DIGITAL WORLD AND THE PLAIN VIEW DOCTRINE

The power of the digital world is truly transformative. Technological innovation reaches virtually every aspect of human life—from the way in which individuals communicate, to how they gather and store information, to how they purchase goods. The reach of the digital world extends so far that both business and social norms have been forever altered as a result.

Further evidence of the enormous power of the digital world rests in the amazing storage capacity of a single computer. Imagine a warehouse full of documents. How many documents do you think it can hold? One hundred thousand? Two hundred thousand? Now compare that large physical space to the digital capacity to store millions of documents. This 150 kilobytes document currently being read was opened on a computer with 350 gigabytes of memory; room enough for thirty-six million documents like this one.

Now imagine searching for a few dozen sensitive documents in the mass of thirty-six million documents, which were categorized, placed, and named, sometimes intentionally mislabeled, by another person. This type of challenge is frequently presented when police search and seize digital media. When conducting a search of a suspect's computer for evidence of a particular crime, investigators are confronted with the task of locating this evidence amidst millions of items. Inevitably during this type of search, investigators will come across items they were not initially looking for. These items can end up being evidence of other crimes. The question becomes, how should the courts deal with this other evidence?

This Comment analyzes the competing federal circuit court interpretations of the plain view doctrine as applied to Fourth

* Associate Member, 2009–2010 *University of Cincinnati Law Review*. The author would like to thank her husband, Matt Ward, for all his support and encouragement during the writing process and her good friend, Matt Flairty, for his creative thinking assistance during the writing process.

Amendment searches and seizures of digital media. Part II provides background of the Fourth Amendment and the plain view doctrine as well as the various legal conceptions of electronic data as interpreted by scholars and the courts. Part III examines three competing interpretations of the application of the plain view doctrine to digital searches and seizures applied by the four circuit courts that have addressed the issue. Part IV discusses the benefits and problems associated with each analytical approach. Part IV also concludes that the solution is "plain" and advocates applying the traditional objective approach to the plain view doctrine to Fourth Amendment searches and seizures.

II. BACKGROUND

The Fourth Amendment of the United States Constitution represents the fundamental value of privacy and freedom from unwarranted intrusions by the government. Yet even such a sweeping protection has its limits. One such limit is the plain view doctrine. The plain view doctrine seeks to balance a citizen's interests in privacy and freedom from intrusive searches and the government's interest in effective law enforcement when officers come across incriminating evidence of one crime while searching for evidence of another. This doctrine creates unique problems when applied to the digital world.

A. Fourth Amendment – Generally

The Fourth Amendment protects against the overarching police power,[1] specifically providing that:

> 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.[2]

Among the myriad of protections arising out of the Fourth Amendment is the exclusionary rule, which guarantees the rights of the Fourth Amendment by preventing the admission in criminal proceedings

1. Samantha Trepel, *Digital Searches, General Warrants, and The Case For the Courts*, 10 YALE J.L. & TECH. 120, 124 (2007) (explaining that the development of the Fourth Amendment was a reaction to the general warrants and writs of assistance which permitted the British to search and seize without requiring individualized suspicion or descriptions of the persons or items to be seized).

2. U.S. CONST. amend. IV.

of inappropriately obtained evidence.[3] Thus, evidence obtained without warrant or without probable cause will be inadmissible against a defendant during trial proceedings. The United States Supreme Court expanded the protections of the Fourth Amendment in *Katz v. United States*.[4] In *Katz*, the Court explained that "the Fourth Amendment protects people—and not simply 'areas,'" thus extending the Fourth Amendment's protections beyond mere physical trespass.[5] After *Katz*, courts must now consider whether a person has both a subjective and objective expectation of privacy, regardless of whether physical trespass occurred.[6] As Justice Stevens explained, "[t]he prohibition against general searches and general warrants serves primarily as a protection against unjustified intrusions on privacy."[7]

Deterrence is the Court's primary motive in excluding evidence obtained without a warrant or without probable cause.[8] The Court excludes such evidence in the hope of deterring investigators and the police from obtaining evidence in an unconstitutional manner.[9] Therefore, Fourth Amendment jurisprudence recognizes multiple exceptions to the exclusionary rule when the primary purpose of deterrence would not be served by such a restriction. Some of these exceptions include inevitable discovery,[10] good faith,[11] independent source,[12] exigent searches,[13] reasonable mistake,[14] and, the focus of this

3. Mapp v. Ohio, 367 U.S. 643 (1961); Wolf v. Colorado, 338 U.S. 25 (1949).

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

5. *Id.* at 353.

6. *Id.* at 361 (Harlan, J., concurring) ("[T]he rule that has emerged from our prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

7. Horton v. California, 496 U.S. 128, 141 (1990).

8. *Mapp*, 367 U.S. at 648, 655 (incorporating the exclusionary rule to the states).

9. *Id.* The question of whether the deterrence rationale is a viable means of ensuring the privacy of individuals are fully provided for is beyond the scope of this Comment.

10. Nix v. Williams, 467 U.S. 431 (1984) (noting that although a Fourth Amendment violation occurred, the evidence was admitted because police officers obtained legitimate leads in addition to the violation, which led them to the evidence).

11. United States v. Leon, 468 U.S. 897 (1984); Illinois v. Krull, 480 U.S. 340 (1987); Herring v. United States, 129 S. Ct. 695 (2009) (noting that the exclusionary rule is meant to deter the cop on the beat, thus when a mistake is made that is not the fault of the cop on the beat, the good faith exception to the exclusionary rule applies).

12. Murray v United States, 487 U.S. 533 (1988) (explaining that although the evidence was obtained through a Fourth Amendment violation, it would have been discovered anyway through another source, such as, if a search party was going through the woods, they would have eventually found the cabin, which had been entered without a warrant).

13. Warden v. Hayden, 387 U.S. 294 (1967) (holding that in an emergency situation, police may enter a home without a warrant or probable cause).

14. Maryland. v. Garrison, 480 U.S. 79 (1987) (noting that reasonable mistake permits

Comment, the plain view doctrine.

B. The Plain View Doctrine

In *Coolidge v. New Hampshire*,[15] the Supreme Court provided its first significant discussion of the plain view doctrine. In his plurality opinion, Justice Stewart provided an example of when the plain view doctrine would apply; specifically he indicated that it would apply when the police have a warrant to search a given area for specified objects and in the course of that search comes across some other article of incriminating character.[16] In such a situation, the Supreme Court found that probable cause was unnecessary to *seize* evidence not described in the warrant because the evidence was in "plain view."[17] The plurality held that for evidence not described in the warrant to be in "plain view," an officer must be in a lawful vantage point of such evidence,[18] must have a lawful right of access to the evidence itself,[19] and the object's incriminating character must be immediately apparent to the officer.[20] The Court subsequently reaffirmed these requirements.[21] Justice Stewart explained, once a lawful search is in progress it would be a "needless inconvenience" and "sometimes dangerous—to the evidence or to the police themselves"—for officers to ignore incriminating evidence in plain view.[22]

For officers to be in a lawful vantage point of evidence under the plain view doctrine, they must not have violated the Fourth Amendment in arriving at the place where the object can be plainly viewed.[23] In other words, the officers must have a warrant or some other recognized Fourth Amendment exception permitting their presence in the location from which the unspecified evidence is plainly viewed.[24] To justify a

admissibility of evidence if the police are wrong about their actions, however, if the circumstances are not so bizarre that some officer of minimal intelligence could have made the mistake, the evidence is admissible).

15. Coolidge v. New Hampshire, 403 U.S. 443 (1971).

16. *Id.* at 465.

17. *Id.* at 465–66 (Emphasis was added to highlight that the plain view doctrine applies to the seizure of items not searches. If an article is already in plain view, neither its observation nor its seizure would involve any invasion of privacy, and therefore constitutes no violation of the Fourth Amendment).

18. *Id.* at 465.

19. *Id.*

20. *Id.*

21. Arizona v. Hicks, 480 U.S. 321 (1987); Horton v. California, 496 U.S. 128 (1990).

22. *Coolidge*, 403 U.S. at 468.

23. *Horton*, 496 U.S. at 135–36.

24. *Id.* at 139.

seizure of evidence not mentioned in a warrant, the plain view doctrine cannot take effect until a search is already in progress.[25]

Lawful access to the evidence requires officers, when conducting a search, to adhere to the scope of the warrant or to rely on a Fourth Amendment exception, which either permits a search or permits extending a search; furthermore, the officer's must stop the search once the items described in the warrant are discovered.[26] For example, officers may not trespass on a suspect's property to obtain evidence in plain view without obtaining a warrant or confronting a situation in which a Fourth Amendment exception applies.[27]

To avoid an expansion of the plain view doctrine as a justification for general exploratory searches "from one object to another until something incriminating at last emerges," the incriminating character of the evidence seized must be immediately apparent to the investigating officer.[28] In *Arizona v. Hicks*, the Court established that an investigating officer must have probable cause upon initial sight to believe that the evidence is linked to a crime in order to justify its seizure under the plain view doctrine.[29] *Hicks* involved an officer, who pursuant to an exigency search[30] of an apartment, moved expensive stereo equipment to obtain its serial numbers, which were later were used to prove that the equipment was stolen.[31] The Court found this evidence inadmissible and the plain view doctrine inapplicable because the stereo equipment lacked incriminating character upon sight.[32] Although the officer maintained he had a reasonable suspicion that the equipment was stolen, because it looked out of place in the small apartment, the Court held the plain view doctrine requires that the higher standard of probable cause to be met.[33]

Initially, the Court maintained inadvertence as a requirement under the plain view doctrine.[34] By this standard, the plurality in *Coolidge* maintained officers executing a search warrant could not have knowledge that they may come across evidence unspecified in the

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

26. 79 C.J.S. SEARCHES § 273 (2010).

27. *Horton*, 496 U.S. at 136 (citing *Coolidge*, 403 U.S. at 465–66).

28. *Coolidge*, 403 U.S. at 466.

29. Arizona v. Hicks, 480 U.S. 321, 326 (1987).

30. In an emergency situation, an officer may enter a residence to check out the situation. *See, e.g.*, Warden v. Hayden, 387 U.S. 294 (1967).

31. *Hicks*, 480 U.S. at 325.

32. *Id.* at 322.

33. *Id.* at 326.

34. Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971).

warrant.[35] However, in *Horton*, the Court explicitly overruled itself and held the Fourth Amendment does not prohibit warrantless seizures of evidence of a crime in plain view, even if the discovery of the evidence was not inadvertent on the part of the police officer.[36]

In sum, to justify a seizure under the plain view doctrine each of the three previously described elements must be met. To use the example described in Part I to demonstrate the application of the plain view doctrine, imagine a judge issues a warrant to search an entire warehouse for a document relating to the crime of extortion. As police search for this document, they discover boxes filled with cocaine. Under the plain view doctrine, the cocaine is admissible as evidence of drug trafficking. The police met the lawful vantage point requirement because the warrant permitted them to search the warehouse. The search of the boxes was within the scope of the warrant because boxes reasonably contain documents, so the officers had lawful access to the cocaine itself. Finally, the incriminating nature of the cocaine is immediately apparent because it is always illegal to possess cocaine.

C. Legal Conceptions of Electronic Data and Digital Media

While the plain view doctrine is fairly well-settled, its use becomes muddled when it is applied to the unique challenges of the digital world. The Court's language explains the plain view doctrine in terms of physical space, whereas evidence on a computer is found in virtual space. A court's application of the plain view doctrine to electronic data and digital media evidence depends on how a court actually views a digital search and seizure. There are two principle conceptions of electronic data stored on computers and digital devices.[37] One view asserts that the traditional Fourth Amendment principles apply because a computer is a container, and the data in electronic storage are merely

35. *Id.*

36. Horton v. California, 496 U.S. 128, 137–39 (1990). The Court found two flaws in the inadvertence requirement: (1) Objective standards are better for evaluating the actions of law enforcement as opposed to a subjective state of mind because if an officer has a valid warrant to search for one item and merely a suspicion concerning the second, there is no reason why that suspicion should immunize the second item from seizure if it is found during a lawful search for the first. (2) No additional Fourth Amendment interest is served by requiring that the discovery of the evidence be ignored because the interests of the Fourth Amendment are already served by the requirements that no warrant issue unless it particularly describes the place and persons to be searched and seized. If the scope of the search exceeds the terms of the warrant, the subsequent seizure is constitutionally invalid. *Id.*

37. Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193, 196 (2005).

forms of documents.[38] The other view asserts that data searches are unique thus requiring unique procedures.[39]

1. Data as Documents

Some courts analogize computers and digital storage devices as closed containers or file cabinets.[40] The physical computer is a container, and all electronic data stored therein are fairly searchable if agents have a valid warrant to search the device; furthermore, when those contents are exposed they are in plain view and subject to seizure.[41] This view asserts that there is no distinction between records kept electronically and those kept in paper form.[42] Under this approach, courts look to traditional Fourth Amendment means to limit the scope of document searches.[43] Therefore, the plain view doctrine applies.

2. Data as Unique

For Fourth Amendment analysis, many scholars consider data searches and seizures unique and find the "closed container" approach to be an oversimplification of the complexities involved in this area of law. For one thing, the sheer volume of storage space in a computer exponentially outmatches anything in a typical storage container.[44] Computers, unlike file cabinets, hold information touching on many aspects of life, all conveniently stored in one small location.[45] Moreover, individuals put a wide variety of information on their computers ranging from pictures, to correspondence, to financial records.[46] Typical containers or document files are much more limited in what types of information they contain. Based on this, applying the plain view doctrine to searches and seizures of data on a computer or digital device allows police officers to access a much larger amount of

38. *Id.*

39. *Id.*

40. Trepel, *supra* note 1, at 126.

41. *Id.*

42. *Id.* at 126–27.

43. *Id.* at 126–27.

44. RayMing Chang, *Why the Plain View Doctrine Should Not Apply to Digital Evidence*, 12 SUFFOLK J. TRIAL & APP. ADVOC. 31, 35 (2007) ("The School of Information Management and Systems at the University of California, Berkeley estimates that about five exabytes of new information, which is equivalent to 37,000 times the amount of information in the Library of Congress book collections, was created in 2002 alone.").

45. David J.S. Ziff, Note, *Fourth Amendment Limitations on the Execution of Computer Searches Conducted Pursuant to a Warrant*, 105 COLUM. L. REV. 841, 867 (2005).

46. Chang, *supra* note 44, at 35.

information than with traditional searches and seizures.

In addition, some scholars argue that the traditional application of the plain view doctrine is predicated on the "empirical concept of visual observation" and note that sight in the physical world is unambiguous, but in the computer world, searches and seizures are method-specific.[47] For example, to view the contents of the file, the file must be opened, so there is an intermediary step before the contents of the file come into view. This view cannot be said to be "plain" because it was not immediately apparent to the viewer. Therefore, digital searches are more like unlocking and opening a box, which requires an officer to have the implements to unlock and then open the box, thus falling outside the scope of the plain view doctrine.[48] Also, unlike physical property, police cannot see digital property directly.[49] When police look at a hard drive, they cannot interpret the code without the assistance of a machine that reads the digital property storage device and a program that translates the digital property into a perceivable form that may not represent the true nature of the digital property.[50]

Under this interpretation, for the plain view doctrine to apply, the government must meet the three-part test to comply with the Fourth Amendment. The federal circuit courts disagree regarding which conceptualization of digital storage is the more appropriate model to determine the plain view doctrine's application to electronic data and digital media evidence. This shapes the outcome of their holdings involving seizure of electronic evidence justified by the government under the plain view doctrine.

III. THE CIRCUIT SPLIT: APPLYING SEPARATE ANALYTICAL APPROACHES TO THE PLAIN VIEW DOCTRINE

Courts struggle with the application of the plain view doctrine to seizure of data and electronic files discovered during searches of computers and other digital devices. Digital media presents challenges distinguishable from traditional physical searches because evidence discovered electronically is discovered in a non-physical world. Courts have yet to successfully apply the complications of the digital world to a once fixed concept of space. As a result, the four circuit courts that have addressed this issue have split into three distinct analytical approaches.

47. Susan W. Brenner and Barbara A. Frederiksen, *Computer Searches and Seizures: Some Unresolved Issues*, 8 MICH. TELECOMM. & TECH. L. REV. 39, 94 (2002).

48. *Id.*

49. Chang, *supra* note 44, at 36.

50. *Id.*

A. Traditional Fourth Amendment Jurisprudence: The Objective Application of the Plain View Doctrine

In *United States v. Williams*,[51] the Fourth Circuit used an objective approach to apply the plain view doctrine to the seizure of child pornography discovered during the execution of a warrant for a separate crime.[52] The court analogized the search of the computer to a search of a file cabinet with a large number of documents and indicated that there was no reason to depart from the rules that apply to a file cabinet when conducting a computer or digital device search.[53] Under this approach, the traditional search and seizure rules apply to computer and digital media searches and seizures.

The police in *Williams* conducted an investigation regarding several e-mails sent to the Fairfax Baptist Temple threatening rape and bodily injury to several named boys who attended the temple.[54] Once the investigation uncovered the identity of the individual who the e-mail account was registered to, a warrant was issued permitting the police to search the contents of the defendant's computer systems, digital storage media, videotapes, video tape recorders, and instrumentalities in connection with the offenses of harassment by computer and threats of death of bodily injury.[55] Pursuant to this search warrant, officers opened deleted files on the various media and found "many deleted images of young male erotica."[56] Officers also opened a DVD labeled, "Virus Shield, Quaranteed [sic] Files, Destroy."[57] The DVD contained thousands of images in "thumbnail view" of minor boys; thirty-nine of the images constituted child pornography.[58]

The defendant argued that the search for and seizure of child pornography violated his Fourth Amendment right against unreasonable searches and seizures because the warrant did not authorize the search and seizure of child pornography and because the search did not fall within any recognized exception to the Fourth Amendment's warrant requirement.[59] Specifically, the defendant argued that the plain view

51. United States v. Williams, 592 F.3d 511 (4th Cir. 2010), *cert. denied*, 131 S. Ct. 595 (2010).

52. *See generally id.*

53. *Id.* at 523.

54. *Id.* at 514–15.

55. *Id.* at 515–16.

56. *Id.* at 516.

57. *Id.*

58. *Id.*

59. *Id.* at 517, 518. The defendant relied on an article by Professor Orin Kerr, which advocates for a new approach to the plain view doctrine in digital searches and seizures. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 513 (2005).

exception to the warrant requirement could not be applied in the context of computer searches unless the files sought to be seized pursuant to the warrant were discovered *inadvertently*.[60] The defendant questioned the validity of the search as a deliberate extension of the search warrant beyond its expressed bounds.[61] Notably, the investigating officer testified that his experience as a detective informed his judgment on the propensity for perpetrators like the defendant to possess child pornography.[62] The defendant argued that reliance on this experience was not inadvertent, but instead deliberate.[63] The warrant, however, did not mention the crime of child pornography.[64] The court noted the nuance of the defendant's argument is that traditional Fourth Amendment rules should not apply "[s]ince computers can hold so much information, touching on virtually every aspect of a person's life, the potential for invasion of privacy in a search of electronic evidence is significantly greater than in the context of a non-computer search."[65]

The Fourth Circuit rejected the notion that inadvertence on the part of the officers plays any role in determining whether the seizure of particular evidence falls within the scope of the plain view exception to the warrant requirement regarding electronic seizures or other types of seizure.[66] The court explained that Supreme Court jurisprudence maintains a well-established principle that "the scope of a search conducted pursuant to a warrant is defined *objectively* by the terms of the warrant and the evidence sought, not by the *subjective* motivations of an officer."[67] Inadvertence improperly focuses on the subjective motivations of the officer instead of actually applying the plain view doctrine as laid out by the Supreme Court.[68]

To apply this doctrine to computer and electronic data searches, the Fourth Circuit began by accepting the premise that, in this case, the warrant implicitly authorized officers to open each file on the computer to view its contents, at least cursorily, to determine if the file fell within

60. *Id.* at 518 (emphasis added). The defendant relied on *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999), which is discussed at length in Part III(b).

61. United States v. Williams, 592 F.3d 511, 522 (4th Cir. 2010), *cert. denied*, 131 S. Ct. 595 (2010).

62. *Id.* at 515.

63. *Id.* at 518.

64. *See id.*

65. *Id.* at 517.

66. *Id.* at 522–23.

67. *Id.* at 522 (citing Maryland v. Garrison, 480 U.S. 79, 84 (1987); Whren v. United States, 517 U.S. 806, 813 (1996)).

68. *Id.* at 522–23 (citing Horton v. California, 496 U.S. 128, 138 (1990)).

the scope of the warrant's authority.[69] For a computer or other digital device to be effectively searched, the search cannot be limited to only reviewing the files' designation or labeling because files can be easily manipulated to hide their substance.[70] In other words, a criminal will not label his computers files "evidence-of-crime.doc." Accepting that a computer or digital device search pursuant to a warrant permits cursory review of each file on said device, the Fourth Circuit explained that the criteria for the plain view doctrine was satisfied:

> *First*, an officer who has legal possession of the computer and electronic media and a legal right to conduct a search of it is "law fully [sic] present at the place from which evidence can be viewed," . . . . *Second*, the officer, who is authorized to search the computer and electronic media for evidence of a crime and who is therefore legally authorized to open and view all its files, at least cursorily, to determine whether any one falls within the terms of the warrant, has "a lawful right of access" to all files, albeit only momentarily. And *third*, when the officer then comes upon child pornography, it becomes "immediately apparent" that its possession by the computer's owner is illegal and incriminating.[71]

The Fourth Circuit held that any child pornography on the computer or electronic media may be seized under the plain view exception.[72] In addition, the court also made broader statements in dicta regarding electronic data searches and seizures, expounding on the reasoning behind its holding and treatment of electronic searches and seizures. The Fourth Circuit maintained that searches and seizures of electronic files, despite the large amount of information contained on such media, do not require special treatment under the Fourth Amendment.[73]

B. The "Inadvertence" Standard: The Subjective Application of the Plain View Doctrine

Two circuits seemingly resurrected the *Coolidge* standard by adopting a subjective application of the plain view exception and mandating inadvertent discovery of the evidence said to be in plain view. These circuits expressed concern with police officers subverting probable cause and warrant requirements.[74] Both circuits operate under the

69. *Id.* at 523.

70. *Id.* at 522.

71. *Id.* (internal citations omitted).

72. *Id.*

73. *Id.* at 511, 522.

74. United States v. Mann, 592 F.3d 779, 786 (7th Cir. 2010), *cert. denied*, 130 S. Ct. 3525 (2010).

premise that digital searches and seizures are different from traditional Fourth Amendment jurisprudence and mandate additional requirements to satisfy the plain view doctrine.

1. The Seventh Circuit

Decided just one day after *United States v. Williams*, the Seventh Circuit in *United States v. Mann* elected to analyze the digital media as unique and held the plain view doctrine can only apply if the evidence is discovered inadvertently, which requires examining the subjective intentions of the officer.[75] Similar to *Williams*, *Mann* involved a case where child pornography was discovered during the execution of a warrant for a separate crime. Officers obtained a warrant to search the defendant's computers and hard drives for images of voyeurism.[76] The detective on the case used software known as a "forensic tool kit" (FTK) to catalogue the images on the computer into a viewable format, as well as a "known file filter" (KFF) which flags those files identifiable from a library of known files previously submitted by law enforcement—most of which are images of child pornography.[77] Through the search of the computers, the detective discovered evidence of voyeurism and child pornography.[78] The defendant argued that the detective's search was an impermissibly general search of his computers for crimes unrelated to the crime of voyeurism.[79]

Similar to the Fourth Circuit, the Seventh Circuit held the plain view exception applied to the evidence of child pornography discovered during the execution of the voyeurism search warrant; however, unlike the Fourth Circuit, the Seventh Circuit relied on the subjective intentions of the officer to provide legitimacy to the plain view discoveries of child pornography.[80] The Seventh Circuit began its analysis from the same premise as the Fourth Circuit: in order to conduct a thorough search pursuant to the warrant, the officer conducting the search had to view all

75. *Id.* at 784.

76. *Id.* at 780–81.

77. *Id.* at 781.

78. *Id.*

79. *Id.*

80. *See id.* at 784. The court explained that the detective's focus on finding images related to voyeurism as opposed to images of child pornography validated the seizure of the child pornography images under the plain view exception. As a point of comparison, the court contrasted this with a detective who had abandoned his initial search for drug-related evidence once he discovered child pornography and began a search for child pornography exclusively. *See* Carey v. United States, 172 F.3d 1268, 1273 (10th Cir. 1999).

the digital files.[81] But the Seventh Circuit added inadvertence as a criterion for applying the plain view doctrine. The court explained the officer's actions were justified under the plain view exception because at no time did he stray from his initial search for evidence of voyeurism while searching the computer.[82] This determination was based upon the subjective intentions of the officer. Although the detective found child pornography, he did not then abandon his search for evidence of voyeurism and then look for child pornography; therefore, despite coming into plain view, his intent was not to find child pornography.[83]

The Seventh Circuit more explicitly highlighted the inadvertence requirement in its analysis of the four flagged "KFF Alert Files," which were deemed inadmissible.[84] The court explained once the software had flagged those files, the detective reviewing the files *knew* or *should have known* that files in a database of known child pornography images would be outside the scope of a warrant issued to search for evidence of voyeurism.[85]

Therefore, in the Seventh Circuit, for the plain view doctrine to apply, the evidence in question must have been discovered inadvertently. Inadvertence is determined by looking at the subjective intentions of the officer conducting the search. While admitting the evidence of child pornography under the plain view exception, the court offered a caveat that it would have been preferable for the officer to stop his search after stumbling upon the child pornography and request a separate warrant.[86]

2. The Tenth Circuit

Presented with another factual scenario involving the seizure of images of child pornography while executing a search warrant for a separate crime, the Tenth Circuit, in *United States v. Carey*,[87] held that the images were not in plain view and exceeded the scope of the warrant.[88] In *Carey*, police obtained a warrant to search the defendant's

81. United States v. Mann, 592 F.3d 779, 784 (7th Cir. 2010), *cert. denied*, 130 S. Ct. 3525 (2010).

82. *Id.*

83. *Id.*

84. *Id.*

85. *Id.* (emphasis added to highlight the court's focus on the subjective intentions of the detective).

86. *Id.* at 786.

87. United States v. Carey, 172 F.3d 1268 (10th Cir. 1999).

88. The court suggested in this case that it was not addressing the question of what constitutes "plain view" in the context of computer files, however, the court's language and holding clearly implicate the plain view doctrine in its analysis. Further, other courts' subsequent reliance on *Carey* when discussing the plain view doctrine indicates that its reasoning and holding involve the plain view

computer files for names, telephone numbers, ledgers, receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances.[89] During the search, the detective on the case discovered "JPEG" files, which after downloading and opening, he discovered contained images of child pornography.[90]

The court explained that the plain view argument was not available because it was "the contents of the files and not the files themselves which were seized."[91] According to the court, although it was the file's contents that were seized, it was only the file's label, and not is contents, that were actually in plain view.[92] The court conceded that the detective could not at first distinguish between files holding evidence of drug dealing and evidence of child pornography,[93] and therefore, he did not expect to find child pornography.[94] However, each time he opened a subsequent JPEG file, he expected to find child pornography and not material related to drugs.[95] The court found this lack of inadvertence fatal to the application of the plain view doctrine to the images discovered after the initial discovery because the detective clearly knew he was acting without judicial authority.[96] As in the Seventh Circuit, the Tenth Circuit examined the subjective intentions of the officer conducting the search.

In a subsequent case, the Tenth Circuit explained that obtaining a second search warrant could rectify the problem in *Carey*.[97] This means once an officer opens a file and evidence of a crime not mentioned in the initial warrant comes into plain view, that officer must stop the search and seek a new warrant.[98]

Carey is cited frequently in both *Williams* and *Mann*. In *Williams,* the Fourth Circuit expressly disagreed with the inadvertence holding in *Carey*, stating:

> While Williams relies accurately on *Carey*, which effectively imposes an "inadvertence" requirement, such a conclusion is inconsistent with

doctrine. *See, e.g.*, United States v. Williams, 592 F.3d 511, 518 (4th Cir. 2010), *cert. denied*, 131 S. Ct. 595 (2010).; *Mann*, 592 F.3d at 783.

89. *Carey*, 172 F.3d at 1272–73.

90. *Id.* at 1271.

91. *Id.* at 1273.

92. *Id.* at 1275.

93. *Id*. at 1273 ("Indeed, he had to open the first JPG file and examine its contents to determine what the file contained.").

94. *Id.*

95. *Id.*

96. *Id.*

97. *See* United States v. Burgess, 576 F.3d 1078 (10th Cir. 2009).

98. *Id.* at 1083.

> *Horton*. Inadvertence focuses incorrectly on the subjective motivations of the officer in conducting the search and not on the objective determination of whether the search is authorized by the warrant or a valid exception to the warrant requirement.[99]

In addition, the Fourth Circuit endorsed the file cabinet analogy the Tenth Circuit found inadequate. In *Carey*, the Tenth Circuit explained that because electronic storage is likely to contain a greater quantity and variety of information, relying on analogies to closed containers or file cabinets may lead courts to oversimplify a complex area of the Fourth Amendment.[100] In contrast, *Mann* relies on *Carey* as authority to justify its decision.[101]

C. Independent Redaction and Review: The Plain View Doctrine Does Not Apply

Instead of attempting to apply the plain view exception to computer and digital searches and seizures, the Ninth Circuit specifically rejected using the plain view exception for these types of searches and seizures and instead developed an entirely different standard of evaluation. In *United States v. Comprehensive Drug Testing Inc.*, the Ninth Circuit rejected the government's attempt to justify its seizure of the digitally stored drug-testing records for hundreds of Major League Baseball players and indicated that the government must foreswear reliance on the plain view doctrine applied to digital seizures altogether.[102] This case was revised and superseded in a rehearing en banc by the Ninth Circuit.[103] However, the concurring opinion, joined by five judges, adopted the same analysis when attempting to resolve the problems of digital seizures,[104] and the court's per curium opinion, while failing to identify a solution, maintained the same analysis regarding the problems of digital seizure.[105] Therefore, the analytical approach to the plain view

99. United States v. Williams, 592 F.3d 511, 523 (4th Cir. 2010), *cert. denied*, 131 S. Ct. 595 (2010). *See also* Horton v. California, 496 U.S. 128, 138 (1990).

100. *Carey*, 172 F.3d at 1275 (citing Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 104 (1994)).

101. United States v. Mann, 592 F.3d 779, 783–85 (7th Cir. 2010) (contrasting the defendant's actions with the actions of the defendant in *Carey* and finding the inadvertence standard met), *cert. denied*, 130 S. Ct. 3525 (2010).

102. United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989 (9th Cir. 2009), *revised and superseded by* United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162 (9th Cir. 2010).

103. *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1162.

104. *Id.* at 1178. The concurrence adopts this language verbatim when explaining the procedure that should be followed regarding digital evidence. The concurrence explains that because this issue is likely to arise again, guidance regarding how to deal with electronic sources is useful.

105. *See id*. at 1171–75. The revising court lays out the problem of digital searches verbatim as

doctrine used by the Ninth Circuit remains viable and is important when considering how the plain view doctrine should apply to the seizure of digital evidence.

The warrant authorized the seizure of only ten players' drug-testing records, but officers used this warrant to seize and examine the records for hundreds of players.[106] The government sought to justify this seizure under the plain view doctrine.[107] The court determined that the problem with searches and seizures of computer and digital devices is there is no way to know exactly what a file contains unless the file is opened and its contents revealed.[108] Specifically, necessary efforts to locate particular files requires examining a great many other files to exclude the possibility that the sought-after data is concealed in those other files.[109] Once a file is examined, however, the government may claim that the contents are in plain view, and if incriminating, may keep it, which allows for over-seizing.[110] In order to solve this problem, the Ninth Circuit eliminated the plain view doctrine in cases involving digital evidence and adopted a special standard.[111] Under the Ninth Circuit's special standard, when the government wishes to obtain a warrant to examine a computer hard drive or electronic storage medium in searching for certain incriminating files, or when a search for evidence could result in the seizure of a computer, magistrate judges must observe the following:

> **1.** [They] should insist that the government waive reliance upon the plain view doctrine . . . .
>
> **2.** Segregation and redaction must be either done by specialized personnel or an independent third party. If the segregation is to be done by government computer personnel, it must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant.
>
> **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

this court, however, does not lay out the specific procedures to follow when dealing with digital evidence.

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

107. *Id.* at 997.

108. *Id.* at 1004.

109. *Id.*

110. *Id.* at 1004–05. *See also*, *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1172.

111. *Comprehensive Drug Testing, Inc.*, 579 F.3d at 998.

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.[112]

"Non-reliance" on the plain view doctrine means that should the government come upon evidence of one crime while executing a warrant for a separate crime, they cannot seize evidence because the plain view exception is unavailable. The court explained that if the government refuses to waive reliance on the plain view doctrine, the magistrate judge should order that the seizable and non-seizable data as described by the warrant be separated by an independent third party under the supervision of the court or should deny the warrant altogether.[113]

In sum, the circuit courts cannot agree on how to legally conceptualize digital data or on the legal application of the Fourth Amendment to that data. The Fourth Circuit applied the plain view doctrine as is to digital seizures. The Seventh and Tenth Circuits added a subjective inadvertence requirement to the plain view doctrines three-prong test. The Ninth Circuit does not rely on the plain view doctrine whatsoever in digital seizures.

IV. DISCUSSION: A "PLAIN" EVALUATION OF EACH APPROACH

The circuit split described above demonstrates the uncertainty encountered when considering traditional Fourth Amendment principles in the electronic search and seizure context. The courts are clearly grappling with how the Fourth Amendment applies in the technological world, and the plain view doctrine creates a particular problem. The solution to the problem of the plain view doctrine requires courts to determine whether computer and digital device searches are distinguishable from traditional searches, and how to apply the Fourth Amendment rules. The three separate approaches developed by the federal circuit courts each provide solutions to the problems associated with the plain view doctrine applied to the digital world and raise important concerns that must be considered before either approach is endorsed. This Comment concludes that the objective approach, employed by the Fourth Circuit, best serves the goals of the Fourth Amendment by adequately addressing privacy interests and balancing those interests with law enforcement and crime control interests.

112. *Id.* at 1006 (internal citations omitted). *See also Comprehensive Drug Testing, Inc.*, 621 F.3d at 1178 (J. Kozinki, concurring).

113. *Comprehensive Drug Testing, Inc.*, 579 F.3d at 998.

A. Traditional Fourth Amendment Jurisprudence Endorsed

The solution to the computer search and seizure problems seems somewhat elusive; however, the traditional application of the plain view doctrine furthers both crime control goals and privacy interests. This objective approach, as applied by the Fourth Circuit in *Williams*, offers the best solution to the quandaries of digital and electronic searches. *Williams* exemplifies that the plain view doctrine, which is well-established within the Supreme Court's Fourth Amendment precedent, can be seamlessly applied to the search and seizure of computers as well as other digital and electronic devises.

The objective approach is well grounded in Fourth Amendment jurisprudence. The Supreme Court recognizes that the Fourth Amendment protects "intangible as well as tangible evidence."[114] Extending this sentiment to the seizure of digital data, the intangible nature of computer data does not affect its analysis under the Fourth Amendment.[115] Once a court permits the search of a computer or other digital device through a warrant, the contents of that computer are searchable. Although the courts addressing this issue disagree regarding the application of the plain view doctrine to computer searches, each court accepts the necessity and legality in opening all files on the specified computer to determine its contents for purpose of a search warrant.[116] When searching for documents, the Supreme Court recognizes that the object of a search determines its permissible scope and as a result, some "innocuous documents" must be viewed in order to determine whether those documents can be seized pursuant to the warrant.[117] Similarly, files on a computer or digital device require a cursory view to determine their contents. To be effective, a search of a computer cannot be limited to reviewing only the file's designation or label because the designation or label of digital files can be easily manipulated to hide the file's substance.[118] Once this premise is accepted, a court can readily apply the three criterion of the plain view doctrine to data seizures with relative ease as the Fourth Circuit did in *Williams*.

As laid out in *Williams*, in order to seize data evidence under the plain

114. Warden v. Hayden, 387 U.S. 294, 305 (1967).

115. Raphael Winick, *Searches and Seizures of Computer and Computer Data*, 8 HARV. J.L. & TECH. 75, 81 (1994).

116. United States v. Williams, 592 F.3d 511, 522 (4th Cir. 2010), *cert. denied*, 131 S. Ct. 595 (2010); United States v. Mann, 592 F.3d 779, 784 (7th Cir. 2010), *cert. denied*, 130 S. Ct. 3525 (2010); *Comprehensive Drug Testing Inc.*, 579 F.3d at 999.

117. Ziff, *supra* note 45, at 862 (citing Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976)).

118. *Williams*, 592 F.3d at 522.

view doctrine, an officer must: (1) legally possess the computer or digital media device through the execution of a warrant; (2) this legal possession puts the officer in a position to lawfully view all the files on the computer; and (3) if an officer discovers evidence of another crime, he may seize it if its incriminating nature is readily apparent.[119] This mirrors the three criterion endorsed by the Supreme Court when applying the traditional plain view doctrine: (1) lawful vantage point; (2) lawful access; and (3) the incriminating character of the evidence must be immediately apparent.[120] Under this approach, courts are not required to break precedent covering non-digital property, and existing Fourth Amendment jurisprudence need not be altered.[121] The Department of Justice Guidelines currently suggest this approach.[122] The relative legal and factual ease in applying this approach makes its use very attractive to the courts.

These traditional elements of the plain view doctrine adequately promote law enforcement in addition to protecting privacy interests. Under the traditional application of the plain view doctrine, a search of a specified area must be legitimate and already in progress to justify the seizure of an item in plain view.[123] As explained in *Williams*, to obtain the computer in the first place, an investigating officer must obtain a warrant.[124] Thus, the justifications for the warrant will be subject to the scrutiny of a judicial officer in order to determine if probable cause exists. Should a warrant be issued to search a computer, officers searching would be in a "lawful vantage point" to view its contents. This is no different from a traditional application of the plain view doctrine.[125] Once officers meet this first criterion and obtain legal possession, they may lawfully view all the files on the computer as previously discussed, thus meeting the lawful access requirement. These first two criteria, if met, provide the power to conduct a thorough search; however, the scope of this power is distinctly limited by the third criteria.

The "immediately apparent" criterion provides the most protection for privacy interests; furthermore, courts and scholars often fail to recognize its powerful protection when discussing data and file seizure.[126] To

119. *Id.*

120. Horton v. California, 496 U.S. 128 (1990); Arizona v. Hicks, 480 U.S. 321 (1987).

121. Chang, *supra* note 44, at 60.

122. *Id.*

123. *Horton*, 496 U.S. at 135.

124. *Id.* at 142 n.11 (holding that, for the plain view doctrine to apply, an officer must be acting within the scope of a warrant or be acting within the scope of another Fourth Amendment exception).

125. *See supra* Part II.

126. Scholarly works as well as the court in *Comprehensive Drug Testing* fail adequately consider

satisfy this criterion, the incriminating nature of the file viewed must be immediately apparent to be seizeable, and therefore, an officer can only open a file to the extent necessary to determine that it is not mislabeled.[127] As the *Williams* court explained, officers are only permitted a "cursory" view of each file.[128] This approach to data seizures is consistent with what the Supreme Court permits in traditional seizures. In *Arizona v. Hicks*, the Supreme Court decided a case involving a police officer who observed expensive stereo equipment during an exigency search.[129] The officer moved the equipment to take down the serial number, and upon running the number, discovered it was stolen.[130] The Court held this evidence inadmissible,[131] indicating that the plain view doctrine was unavailable because the incriminating nature of the stereo system was not readily apparent, and therefore the serial number on it could not be seized.[132]

Similarly, in discussing a traditional plain view seizure of documents, the Sixth Circuit explained that when officers were only authorized to search for cocaine, documents that must be read to determine their incriminating character may not be seized because their incriminating character was not immediately apparent.[133] This particular requirement greatly mitigates any concern of a warrant becoming a general search as a result of the plain view doctrine's application to digital and electronic files.[134] For example, a picture of a child in a sexually explicit pose can be recognized immediately as incriminating and is therefore admissible under the plain view doctrine. Financial statements or telephone numbers, however, are not immediately incriminating unless reviewed further and, thus, cannot be seized and admitted under the plain view doctrine.[135]

One critique regarding this objective, traditional approach relates to the sheer amount of information stored on computers. This argument advocates a unique approach to data searches and seizures because a

the privacy protection of the criterion.

127. Ziff, *supra* note 45, at 869.

128. United States v. Williams, 592 F.3d 511, 522 (4th Cir. 2010), *cert. denied*, 131 S. Ct. 595 (2010).

129. Arizona v. Hicks, 480 U.S. 321, 323–24 (1987) (holding that the exigency exception allows officers to enter without a warrant in times of emergency).

130. *Id.*

131. *Id.* at 325.

132. *Id.* at 326–27.

133. United States v. Garcia, 496 F.3d 495, 510.

134. General searches are exactly what the Founders sought to protect against when ratifying the Fourth Amendment. Trepel, *supra* note 1, at 123.

135. Unless, of course, the search warrant specified that these particular items may be seized, or the seizures are within the scope of the warrant and admissible in context of that warrant.

significant amount and wide variety of information was not contemplated by the framers of the Fourth Amendment and is completely unique to Fourth Amendment jurisprudence. Nonetheless, this argument fails because it is merely a statement of fact not a legal argument. The amount of evidence to be potentially found in a device that contains evidence has never been taken into consideration by the Supreme Court. In addition, to assert that computers and digital devices contain "a lot" of information is an arbitrary distinction. What does "a lot" or a "large amount" precisely mean for the purposes of Fourth Amendment legal analysis? Is there some threshold that pushes a storage device to the point of containing "a lot"? Could this "a lot" requirement extend to physical file cabinets that hold "a lot" of files? An "a lot" requirement could logically be extended to the hypothetical warehouse full of documents. Furthermore, although it is possible for digital devices to contain significant amounts of information that does not mean they always do. For example, while a digital camera can store hundreds of pictures, it often contains a relatively small number of pictures.

In an area of the law where there are arguably numerous exceptions to the rule, it is unwise to create further exceptions when current legal doctrines are easily applied and adequately protect the interests to be served.

B. Inadvertence Rejected

The inadvertence approach begins with the premise that technology has created a means of storing information that is so vastly different from anything else to which the traditional Fourth Amendment rules have applied that such computer and digital searches and seizures require special search execution rules. It attempts to remedy the problems of computer searches by adding the additional requirement of inadvertence. This requirement permits judges to assess the testimony of an investigating officer to determine whether he believed he was acting within the scope of the warrant during the investigation.[136]

The first problem with the subjective application of the plain view doctrine is a legal one—it fails to respect the Supreme Court's plain view doctrine precedent. In *Horton v. California*, the Supreme Court overruled the inadvertence requirement mentioned in *Coolidge v. New Hampshire* stating, "evenhanded law enforcement is best achieved by the application of objective standards of conduct, rather than standards

136. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 577 (2003).

that depend upon the subjective state of mind of the officer."[137] Therefore, adopting this method would require overturning *Horton* and restoring the inadvertence requirement that it explicitly rejected.[138] *Horton* clarifies that the inadvertence requirement fails to accomplish the goal of preventing police from converting specific warrants into general warrants.[139] An officer's subjective intent may be difficult to discern.[140] If a court relies on an officer's subjective intent in evaluating a search or seizure, that officer has an incentive to testify that his subjective intent was proper, thereby subverting the goal.[141]

In addition, a subjective analysis rewards law enforcement for using untrained officers, who might not know that certain types of evidence will usually only be found in certain types of computer files, and will therefore be more likely come across other evidence inadvertently.[142] Another approach law enforcement may use is to set specific polices and standards that mandate very thorough investigations of computer and digital devices.[143] This is because "[w]hen every step taken by an analyst is a matter of routine policy, it becomes difficult to exclude evidence on the ground that the analyst was attempting to circumvent the warrant."[144]

The most significant problem with the subjective approach of the plain view doctrine is in its application. It truly offers no greater protection for privacy against "general" searches and seizures than the objective approach, but places police officers in a worse position. As applied by the Seventh Circuit in *Mann*, all the subjective approach required was for the officer not to intend to find evidence outside the scope of the warrant.[145] Determining an individual's intent is an onerous task that encourages officers to misrepresent their intentions. Ultimately, the same type and category of evidence will be seized and admitted as was seized and admitted in *Williams*.[146] In the Tenth Circuit when applying the subjective approach, the plain view doctrine applied

137. Horton v. California, 496 U.S. 128, 138–39 (1990). The court also noted the inadvertence requirement in *Coolidge* was only for a plurality of Justices.

138. *Kerr*, *supra* note 136, at 577.

139. Jim Dowell, Note, *Criminal Procedure: Tenth Circuit Erroneously Allows Officers' Intentions to Define Reasonable Searches:* United States v. Carey, 54 OKLA. L. REV. 665, 669 (2001).

140. Kerr, *supra* note 136, at 578.

141. Dowell, *supra* note 139, at 676.

142. *Id.*

143. Kerr, *supra* note 136, at 578–79.

144. *Id.* at 579.

145. *See* United States v. Mann, 592 F.3d 779, 786 (7th Cir. 2010), *cert. denied*, 130 S. Ct. 3525 (2010).

146. *See* United States v. Williams, 592 F.3d 511 (4th Cir. 2010), *cert. denied*, 131 S. Ct. 595 (2010).

to the first file opened containing evidence outside the scope of the warrant because it was discovered inadvertently.[147] The court then maintained that if the officer continued the search, he could no longer maintain that subsequent discoveries were inadvertent; however, all the officer must do is temporarily stop his search and obtain a second warrant which is virtually guaranteed to be issued because the officer has viewed evidence of another crime. The only purpose the subjective approach serves is to inconvenience police officers without any tangible privacy benefit to suspects.

The subjective approach breaks with firm judicial precedent and does not resolve any of the problems associated with this area of criminal procedure.

C. Independent Redaction and Review Rejected

Like the subjective approach, a court's election to exclude the plain view doctrine's application to the seizure of computer and digital data begins with the premise that these types of searches and seizures are unique and therefore require a unique application of traditional Fourth Amendment rules. Like the objective approach, the rule is simple and easily applied. It permits investigators to conduct whatever search is necessary with the caveat that only evidence within the scope of the warrant could be used in court.[148] This alleviates the problem of general searches because only evidence within the scope of the warrant could be used in court.[149]

Whatever problems this rule might remedy, it also raises two other important issues: (1) the practical issue that police must ignore what they find; and (2) the legal issue of providing justification for this type of approach. Elimination of the plain view doctrine for digital data seizures means police would lose a valuable tool in gathering evidence of criminal conduct discovered during a digital property search. As a consequence, criminals would go unpunished for crimes that may not have otherwise been discovered, such as in cases of child pornography.[150] The purpose of the Fourth Amendment is not to allow individuals to hide their crimes, but rather to protect society from unreasonable government searches. Proponents of this viewpoint contend that the draconian nature of this rule is somewhat lessened by the availability of other traditional Fourth Amendment exceptions,

147. Carey v. United States, 172 F.3d 1268, 1273 (10th Cir. 1999).

148. Kerr, *supra* note 136, at 582.

149. *Id.*

150. *See, e.g.*, *Williams*, 592 F.3d 511.

including the independent source exception and the inevitable discovery doctrine.[151] Under these doctrines, evidence can still be admitted if the government can show that it had some independent source for the same information or that it would have discovered the same evidence through other means.[152] From a practical standpoint, however, once officers view evidence of a crime, they will likely find some other way to obtain it, using these other Fourth Amendment warrant exceptions artificially. For example, if child pornography is viewed during a search for evidence of a drug dealer's list, officers must "ignore" the evidence. The officer, however, can swear in an affidavit after the fact that he or she would have come upon the evidence some other way. As a result, officers are encouraged to misrepresent themselves, and Fourth Amendment exceptions are degraded by their artificial application.

In addition, courts applying this approach must articulate legal justification. Digital property must be legally distinguished from other types of property in order to justify deviating from the Supreme Court's plain view doctrine precedent.[153] As one scholar notes, the Supreme Court at one time did attempt to distinguish between types of containers in ranking expectations of privacy.[154] However, a plurality of the court recognized that this structures analytical "bankruptcy" because it lacked basis in the language of the Fourth Amendment.[155] Thus, based on the Supreme Court's analysis, there is no distinction between the search and seizure of the contents of a file cabinet and a search and seizure of data from a computer because Fourth Amendment rules do not distinguish between different types of storage units.

In *Comprehensive Drug Testing*, the Ninth Circuit misinterpreted the traditional plain view doctrine's application because if the court applied traditional plain view analysis, it would have reached the same result as it would under independent redaction and review. The officer in this case had to read the files in order to determine the incriminating nature of the players' drug-testing records. The plain view doctrine forbids seizure of any item not immediately incriminating. As explained by the Sixth Circuit, if an officer must read a document to determine its incriminating nature, it may not be lawfully seized under the plain view doctrine.[156] The plain view doctrine would only permit officers in *Comprehensive Drug Testing* to have cursorily viewed the file, allowing

151. Kerr, *supra* note 136, at 584.

152. *Id.*

153. *Id.* at 528.

154. Clancy, *supra* note 37, at 216.

155. *Id.* (citing Robinson v. California, 453 U.S. 420, 426 (1987) (plurality opinion)).

156. United States v. Garcia, 496 U.S. 495, 510 (6th Cir. 2007).

them to determine that it was not a file involving the players listed in the warrant. Any search beyond that fails the immediately incriminating criterion.

The concern regarding general searches in these types of cases does not stem from the application of the plain view doctrine, but rather, from the magistrate judge's failure to appropriately limit the scope of the search warrant. For example, in *Comprehensive Drug Testing*, by permitting a complete search of all electronic files, the magistrate judge failed to appropriately limit the scope of the search warrant and exposed to discovery the drug-testing records of players not under investigation. The search should have been limited in a manner that access was only granted to the records of those players under investigation. Because the files being searched were kept in the ordinary course of business, they were highly unlikely to be mislabeled; therefore, a search warrant for all computer files was overly broad—a problem which could have been solved by properly tailoring the warrant. When issuing warrants, judges must ensure that the warrant's scope is properly limited.

V. CONCLUSION

Despite confusion in the courts and the fact that computers and digital devices are used in all aspects of life, the Supreme Court denied certiorari for both *Williams* and *Mann*. While an application of the plain view doctrine to computers and other digital devices has been significantly discussed in scholarship for some time, recent circuit court decisions have brought these "virtual" arguments into reality, demonstrating a tangible need for the Supreme Court to clarify this confusion. The most reasonable approach for the Supreme Court to adopt is the objective application. Although technology changes, the traditional application of the plain view doctrine continues to properly balance privacy interests with the government's interest in effective law enforcement regardless if law enforcement officials are confronted with a warehouse full of thousands of documents or a computer full of millions.