PORNOGRAPHY AND PRIVACY IN PLAIN VIEW: APPLYING THE PLAIN VIEW DOCTRINE TO COMPUTER SEARCHES

Corey J. Mantei*

With the vast majority of American households owning a computer, technology is a permanent fixture in everyday life. From boardrooms to dorm rooms, computers are capable of storing and manipulating data in previously unimaginable ways. This technology is also changing the methods by which crimes are planned and executed. As a result, hard drives and other memory devices often provide evidence to government agents during their investigations. Computer searches present challenging constitutional issues because the Framers drafted the Fourth Amendment to define the boundaries of traditional physical searches. As reflected by a federal circuit split and several wildly unpredictable court decisions, a complex issue arises when, during a warranted computer search, the government relies on the plain view doctrine to seize digital evidence. This Note examines the plain view doctrine's proper scope and application in computer searches. Although the Fourth Amendment was originally created to define the parameters of lawful, physical searches, its principles and exceptions must also broadly extend to computers. A warrant's language—not categorical restrictions—should ultimately define the permitted scope of plain view seizure.

---

* J.D. Candidate, University of Arizona James E. Rogers College of Law, 2012. The Author would like to thank Professors Barbara Atwood, Toni Massaro, Melissa Meister, Marc Miller, and Sally Rider for their unwavering support during the past two years. Many thanks as well to the *Arizona Law Review* Editorial Board, especially Alexis Danneman and Brad Honigman, for their humor and thoughtfulness. Finally, this Note is dedicated to the Mantei family. The joy you bring into my life is a blessing in every imaginable way. Thank you for your prayers, guidance, and unconditional love.

TABLE OF CONTENTS

INTRODUCTION

Welcome to the information superhighway. With the creation and growing popularity of mobile devices such as MP3 players, handheld videogames, laptop computers, and cell phones, it is hard to imagine an existence without portable forms of data storage. Armed with only a laptop or smart phone, a knowledgeable user can conquer the digital world by surfing the Internet, watching the latest NFL highlights, and ordering a large Starbucks Frappuccino with the single touch of a button.[1] Clearly distinguishable from the hard drives of the mid-1950s, which were commonly the size of two refrigerators stacked together,[2] modern storage devices incorporating flash technology are often no larger than a single half-dollar coin.[3] In addition to reducing the physical size of these devices, manufacturers have also dramatically increased their storage capabilities.[4] In 1956, for example, IBM's RAMAC 305 hard drive had a meager five-megabyte capacity,[5] the equivalent of 2500 typewritten pages.[6] By comparison, nearly 10% of purchased 3.5-inch hard drives—the industry standard for desktop PCs—can

1. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 569 (2005) ("In the 1980s, computers were used primarily as glorified typewriters. Today they are postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more.").

2. Rex Farrance, *Timeline: 50 Years of Hard Drives*, PCWORLD (Sept. 13, 2006), http://www.pcworld.com/article/127105/timeline_50_years_of_hard_drives.html.

3. *See* Jeff Tyson, *Removable Flash Memory Cards*, HOWSTUFFWORKS, http://electronics.howstuffworks.com/flash-memory2.htm (last visited Oct. 16, 2010).

4. *See generally* Farrance, *supra* note 2 (exploring the creation and expansion of hard drive technology in the last 50 years).

5. *Id.*

6. *See* L.S. Wynn, *How Much Text is in a Kilobyte or Megabyte?*, WISEGEEK, http://www.wisegeek.com/how-much-text-is-in-a-kilobyte-or-megabyte.htm (last modified July 29, 2011).

hold at least a terabyte of data.[7] For illustrative purposes, a one-terabyte hard drive can store 1000 copies of the *Encyclopedia Britannica*,[8] and even more astonishingly, a ten-terabyte drive could hold the entire printed collection of the Library of Congress.[9]

These technological advances, including the rise and expansion of the Internet, have also had unintended consequences. Criminals are becoming increasingly proficient at using computer technology to carry out illegal activities.[10] Complex encryption technology and high-speed Internet connections allow users to exchange files involving drug sales, hacking, and credit card fraud.[11] Law enforcement officials at local, state, and federal levels routinely confront forms of criminal activity that were unimaginable just twenty years ago.[12]

Computers are also changing the methods of criminal conduct.[13] Users can easily store evidence of both petty offenses and complex enterprises in file folders with family pictures, research papers, digital music, and other benign materials.[14] One of the most troubling consequences of this advancing technology

---

7. Press Release, Western Digital, WD Launches Industry's First 2 TB Hard Drives (Jan. 27, 2009), *available at* http://www.wdc.com/en/company/pressroom/releases.aspx?release=01d0ef49-e149-410a-a173-f872d0e6c335.

8. *Megabytes, Gigabytes, Terabytes… What Are They?*, WHAT'S A BYTE?, http://www.whatsabyte.com/ (last visited Oct. 16, 2010); s*ee also* Jeff Welty, *Computer Searches and Plain View*, UNC SCH. OF GOV'T (Sept. 21, 2009, 7:21 AM), http://sogweb.sog.unc.edu/blogs/ncclaw/?p=715 ("At approximately 30,000 pages per gigabyte, a low-end laptop computer with a 250 gigabyte hard drive can store the equivalent of more than 7 million pages of paper. That's thousands of bankers' boxes worth, or as many pages as you'd find at a branch library with 30,000 books.").

9. *Megabytes, Gigabytes, Terabytes… What Are They?*, *supra* note 8. Although manufacturers have not yet created a ten-terabyte hard drive, business servers can exceed this capacity by utilizing several hard drives. *See, e.g.*, *PowerEdge R510 Rack Server*, DELL.COM, http://www.dell.com/us/business/p/poweredge-r510/pd?refid=poweredge-r510&baynote_bnrank=0&baynote_irrank=0&~ck=baynoteSearch (follow "Tech Specs" hyperlink) (last visited Aug. 2, 2011). With further optimization of this data-storage technology, such high-volume capacities are not unthinkable for consumer use sometime in the future. For example, Hitachi scientists will reportedly unveil a four-terabyte hard drive sometime later this year. Dan Grabham, *Hitachi Makes 4TB Hard Disk Breakthrough*, TECHRADAR UK (Oct. 15, 2007), http://www.techradar.com/news/computing-components/storage/hitachi-makes-4tb-hard-disk-breakthrough-148744. Hitachi has exceeded Western Digital's three-terabyte drive by "by shrinking the size of the hard disk's read head [to a size] 2,000 times thinner than a human hair." *Id.*

10. INTERNET CRIME COMPLAINT CENTER, 2009 INTERNET CRIME REPORT 4 (2009), http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf (noting that from January 1, 2009 through December 31, 2009, there were 336,655 total complaints filed for Internet-related crimes including auction and credit card fraud, child pornography, and computer intrusion).

11. *Id.* at 18.

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

13. *Id.*

14. *See id.*

involves the pervasiveness of possessory offenses such as child pornography.[15] Digital cameras and webcams allow online voyeurs to buy, sell, and trade explicit images of children on websites and other peer-to-peer networks. This media often depicts violent sexual exploitation including rape, bondage, and torture.[16] Moreover, the creation and distribution of child pornography is neither rare nor accidental within the modern technological era: 20% of all Internet pornography involves children.[17] With nearly 100,000 websites containing child pornography, this industry generates $3 billion annually.[18] As these figures illustrate, unforeseen dangers have accompanied the rapid development and expansion of computers.

This Note addresses just one example of the complex interplay between modern technology and criminal activity. Specifically, it focuses on warranted computer searches where law enforcement officers seize digital evidence under the plain view doctrine. The Note concludes that existing search-and-seizure law for physical searches, including the plain view doctrine, should broadly apply to digital evidence. Part I provides an introduction to physical searches by exploring the Fourth Amendment's warrant requirement and its prohibition against unreasonable searches and seizures. This Section also evaluates the plain view doctrine in the context of physical searches by discussing its elements and underlying objectives. Part II highlights the controversy by specifically analyzing the doctrine's application in computer searches. It not only discusses the current federal circuit split, but also explores how both federal *and* state lower courts are addressing this complex issue. Finally, Part III evaluates the merits of these decisions and concludes that courts should continue to develop the plain view doctrine incrementally through case law. A warrant's language should ultimately define the legal boundaries of plain view seizure, not bright-line prohibitions.

I. THE FOURTH AMENDMENT AND THE PLAIN VIEW EXCEPTION

Like other great stories of social rebellion and political awareness, the Fourth Amendment was a direct response to oppressive and otherwise overzealous government intrusion.[19] In England during the 1760s, general warrants gave the King's representatives almost unlimited authority to search private homes or businesses for any evidence of criminal activity.[20] Meanwhile, the new American

---

15. *See* Press Release, National Center for Missing & Exploited Children, Child Porn Among Fastest Growing Internet Businesses (Aug. 18, 2005), *available at* http://www.missingkids.com/missingkids/servlet/NewsEventServlet?PageId=2064 (reporting that, due to credit card purchases and the existence of online anonymity, child pornography is one of the fastest growing businesses on the Internet).

16. *Id.*

17. *Id.*

18. *National Pornography Statistics*, BYU WOMEN'S SERVICES, https://t1.byu.edu/content/national-pornography-statistics (last visited Sept. 20, 2010).

19. *See* Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 561–62 (1999).

20. Kerr, *supra* note 1, at 536. In the renowned case *Entick v. Carrington*, for example, plaintiff John Entick published a collection of pamphlets highly critical of the English government. (1765) 95 Eng. Rep. 807 (C.P.) 808; 2 Wils. K.B. 275, 275–76. In response, Halifax, a government minister, issued a warrant not only authorizing the search of Entick's home and papers, but also the permanent seizure of any evidence relevant to

colonies were also burdened by similarly overbroad searches.[21] Writs of assistance, which authorized English customs agents to search for taxable goods, neither specified the place or things to be searched, nor contained any significant time limitations for their execution.[22] Moreover, they compelled any government officials and subjects of the Crown to assist in the agents' searches.[23]

After breaking away from English rule, the Framers wanted to prohibit the use of general warrants and writs of assistance, and thereby restrict the scope of government search authority.[24] The Fourth Amendment provides:

> 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.[25]

By delineating between two forms of personal liberty—a privacy interest implicated by searches and a property interest affected by government seizures[26]—the Fourth Amendment recognizes that unreasonable searches and seizures intrude upon separate interests.[27] Because the Fourth Amendment does not specifically define the characteristics of a search *or* a seizure,[28] the U.S. Supreme Court has provided some clarity in this undefined area of constitutional law.[29] This definition is essential because the Fourth Amendment's protections do not apply in the absence of a government search or seizure.[30] When questions arise as to the lawfulness of government action—specifically, where agents gather information for criminal investigations—any judicial inquiry must first establish whether a search or seizure has actually occurred.

Entick's alleged libel. *Id.* at 808, 2 Wils. K.B. at 275–76. In a celebrated opinion, Lord Camden ultimately held that Halifax had no sustainable basis under either statute or case law to issue the warrant: "The great end, for which men entered into society, was to secure their property. That right is preserved sacred and incommunicable in all instances, where it has not been taken away or abridged by some public law for the good of the whole." 19 Howell's State Trials 1029, 1066 (1765).

21. Tracey Maclin, *The Complexity of the Fourth Amendment: A Historical Review*, 77 B.U. L. REV. 925, 939 (1997).

22. *Id.* at 945.

23. *Id.* at 945–46.

24. Kerr, *supra* note 1, at 536. For an excellent discussion of the Amendment's creation, including the process by which Congress drafted and adopted its specific language, see generally Maclin, *supra* note 21, at 950–60.

25. U.S. CONST. amend. IV.

26. *See* Horton v. California, 496 U.S. 128, 133 (1990) ("A search compromises the individual interest in privacy; a seizure deprives the individual of dominion over his or her person or property.").

27. *Id.*

28. Ziff, *supra* note 12, at 843.

29. Kerr, *supra* note 1, at 536 ("[T]he modern Supreme Court has used the text of the Fourth Amendment to craft a comprehensive set of rules regulating law enforcement.").

30. *See* Katz v. United States, 389 U.S. 347, 353 (1967).

In *Katz v. United States*, the Supreme Court ultimately provided this analytical framework in the form of a two-part test.[31] A search occurs when "a person ha[s] exhibited an actual (subjective) expectation of privacy and . . . the expectation [is] one that society is prepared to recognize as [objectively] 'reasonable.'"[32] When government officials gather information in places where a reasonable expectation of privacy exists, they must act under a valid warrant

---

31. *See id.* at 361 (Harlan, J., concurring). For the purposes of this Note, the primary question is whether law enforcement agents have unlawfully exceeded their search authority by seizing digital evidence in plain view. Although a fascinating topic for discussion, the constitutional parameters of lawful seizures are outside this Note's scope because, in each case and illustration, the government has obtained a warrant that authorizes some type of seizure. For a thoughtful discussion of this subject, see Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 YALE L.J. 700 (2010).

However, one of the most interesting cases to implicate the seizure of digital information arose in the recent Ninth Circuit decision, *United States v. Cotterman*, 637 F.3d 1068 (9th Cir. 2011). In *Cotterman*, border agents seized the defendant's laptop when he attempted to enter the United States at a Mexico–Arizona port of entry. *Id.* at 1070–71. This inspection occurred because a computer database flagged several of his convictions, each of which involved misconduct with children. *Id.* at 1071. The system informed the agents to be "on the 'lookout' for child pornography." *Id.* Because there were no forensic technicians on-site and the border agents could not open Cotterman's password-protected files, Immigration and Customs Enforcement ("ICE") agents transported the laptop to the Tucson field office for a more thorough forensic investigation. *Id.* at 1072. After successfully bypassing 23 password-protected files, the ICE investigator discovered 378 images of child pornography, several of which showed Cotterman sexually molesting a "seven- to ten-year-old girl over a two- to three-year period." *Id.* at 1073.

The Ninth Circuit upheld this investigation as a valid extension of the border search doctrine. *Id.* at 1083–84. Under this doctrine, when an individual is crossing the border, the government can search his property without any level of suspicion. *Id.* at 1074–75. Although the discovery of child pornography occurred two days after the initial stop and nearly 170 miles from the border itself, *id.* at 1070, the court noted "[s]o long as property has not been officially cleared for entry into the United States and remains in the control of the Government, any further search is simply a continuation of the original border search," *id.* at 1079. Moreover, in addressing the legality of the government's two-day seizure, the court held the detention "was reasonably related in scope to the circumstances that justified the initial detention at the border." *Id.* at 1082 (citation omitted). The government not only brought the laptop to the forensic expert quickly, but also completed the actual computer search in a timely manner. *Id.* at 1082–83. Because the government's conduct was reasonable, this seizure did not violate the Fourth Amendment. *See id.* at 1083–84. In dissent, Judge Fletcher noted: "I add my voice to the chorus lamenting the apparent demise of the Fourth Amendment." *Id.* at 1087 (Fletcher, J., dissenting) (citing United States v. Pineda-Moreno, 617 F.3d 1120, 1121 (9th Cir. 2010) (Kozinski, J., dissenting); United States v. Seljan, 547 F.3d 993, 1014–19 (9th Cir. 2008) (en banc) (Kozinski, J., dissenting)).

32. *Katz*, 389 U.S. at 361 (Harlan, J., concurring). Although this language appeared in Justice Harlan's concurring opinion, it has become the primary authority for defining a Fourth Amendment search. 1 JOSHUA DRESSLER & ALAN C. MICHAELS, UNDERSTANDING CRIMINAL PROCEDURE: INVESTIGATION 74 (4th ed. 2006).

supported by probable cause.[33] However, various exceptions to the warrant requirement exist, including the plain view doctrine.[34]

Although courts generally consider warrantless searches presumptively unreasonable,[35] the plain view doctrine does not implicate the Fourth Amendment's warrant requirement because no reasonable expectation of privacy exists over items in open view.[36] Indeed, this doctrine provides the government with a legitimate basis to seize evidence in plain view without a warrant.[37] Although the plain view doctrine is a powerful tool for law enforcement officials, the government must still demonstrate: (1) the officer observed the item from a lawful vantage point; (2) he had a right of physical access to it; and (3) its nature as an object subject to seizure was immediately apparent when the officer observed it, i.e., he had probable cause to seize it.[38]

The plain view doctrine's application frequently arises during physical searches involving homes or other forms of real property.[39] The government typically relies on the doctrine when officers enter a home pursuant to a lawful warrant and discover evidence of possessory offenses often, but not always, linked to drugs.[40] As previously mentioned, officers may lawfully seize property located in open view if there is probable cause to associate this evidence with criminal activity.[41] However, if these investigative efforts extend beyond the scope of a warrant—for example, when officers search rooms or objects not implicated by its specific terms—the government cannot utilize the plain view doctrine because this conduct constitutes a second, unauthorized search.[42]

---

33. *See Katz*, 389 U.S. at 353 (majority opinion).

34. 68 AM. JUR. 2D *Searches and Seizures* § 114 ("Exceptions to the warrant requirement include searches and seizures conducted incident to a lawful arrest, those yielding contraband in plain view, those in the hot pursuit of a fleeing criminal, those limited to a stop and frisk based on reasonable suspicion of criminal activity, those based on probable cause in the presence of exigent circumstances, and those based on consent.").

35. *Katz*, 389 U.S. at 357.

36. Horton v. California, 496 U.S. 128, 133 (1990).

37. *See id.* at 133–34.

38. *Id.* at 136–37; *see also* Coolidge v. New Hampshire, 403 U.S. 443, 465 (1971).

39. *See* Kerr, *supra* note 1, at 536–37.

40. *See, e.g.*, United States v. Wise, 588 F.3d 531, 537–38 (8th Cir. 2009) (the seizure of drugs); United States v. Stanley, 351 F. App'x 69, 72–73 (6th Cir. 2009) (same); United States v. Wright, 324 F. App'x 800, 804 (11th Cir. 2009) (same). *But see, e.g.*, Iowa v. Oliver, 341 N.W.2d 744, 745–47 (Iowa 1983) (upholding the plain view seizure of "bachelor magazines" during a murder investigation); Luster v. Nevada, 991 P.2d 466, 468–69 (Nev. 1999) (upholding the seizure of guns, ammunition, and other evidence linked to kidnapping).

41. *See* Arizona v. Hicks, 480 U.S. 321, 328–29 (1987).

42. *Id.* (holding that a police officer violated the Fourth Amendment during a warrantless apartment search by moving stereo equipment to examine its serial numbers).

II. THE PLAIN VIEW DOCTRINE AND COMPUTERS

Enter computer technology. Three-quarters of American households currently own a computer.[43] This figure will surely rise with the increasing affordability of laptops, desktop PCs, and tablet computers.[44] The Framers never could have envisioned the creation of computers nor the complex interplay between government searches and digital evidence. Although plain view seizure can occur during consent searches,[45] this Note examines the doctrine's application when investigators are acting under a lawful warrant.

Consider the following hypothetical: The FBI receives credible informant testimony that Daniel Damian, an online merchant who specializes in rare sports collectibles, has been defrauding customers with knock-off merchandise. After obtaining a warrant that authorized the search and seizure of any computers at his residence, agents promptly enter Damian's home and remove his personal computer. During a relatively unsophisticated computer search, the investigating agent discovers a file named "xxxkiddypix.jpg" without using any forensic search tools. He opens it. The file contains child pornography. Because this evidence is unrelated to the warrant's specific terms involving fraud, the government must rely on the plain view doctrine to lawfully seize the file. This raises an important question: should this type of seizure be permitted?

In part, the difficulty of this issue arises because computers are capable of storing large amounts of data. Evidence of criminal activity can be kept with harmless materials like family photos, school papers, and digital music.[46] Some commentators have suggested that as applied to computers, the plain view doctrine can transform previously narrow and lawful searches into unlawful, general ones.[47]

Although Congress has occasionally regulated the government's use of emerging technologies such as wiretaps,[48] it has not provided any guidance for the plain view seizure of digital evidence. Currently, the judiciary is the sole arbiter of

---

43. *Americans in Love with "Terabyte Lifestyle"; Study Finds Nearly All Own Products with Digital Technology*, PHYSORG.COM (Aug. 11, 2005), http://www.physorg.com/news5759.html.

44. *See* Joshua Cooper Ramos, *How Cheap Can Computers Get?*, TIME, Jan. 22, 1996, at 60, *available at* http://www.time.com/time/magazine/article/0,9171,983993-1,00.html.

45. *See infra* note 167 (discussing the lawful scope of plain view seizure during consent searches).

46. This issue should not be confused with investigations involving the on-screen display of evidence. Courts have routinely upheld plain view seizures when officers observe incriminating pictures, movies, or text displayed on a computer monitor during a lawful search of a home or business. *See, e.g.*, State v. Mays, 829 N.E.2d 773, 779 (Ohio Ct. App. 2005) (holding that an on-screen message reading, "he will die today," could be properly admitted into evidence against the defendant).

47. *See, e.g.*, RayMing Chang, *Why the Plain View Doctrine Should Not Apply to Digital Evidence*, 12 SUFFOLK J. TRIAL & APP. ADVOC. 31, 50 (2007) ("[L]imit[ations] do not effectively stop digital property warrants from becoming a type of de facto general warrant.").

48. *See* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, §§ 801–804, 82 Stat. 197 (1968) (codified at 18 U.S.C. §§ 2510–2522 (2006)).

this issue. With contradictory analysis at both the state and federal levels, each holding seems to create additional confusion as to the proper scope of plain view seizure in this digital context.[49] These decisions can generally be grouped into one of three basic categories: (1) the inadvertence approach; (2) the prophylactic-test approach; and (3) the computers-as-containers approach. This Section will discuss these approaches separately by analyzing the representative case law within each category.

A. The Inadvertence Approach

In *United States v. Carey*, the Tenth Circuit was the first federal circuit court to address the plain view doctrine's application to computer searches.[50] Carey had been under investigation for his alleged sale and distribution of cocaine.[51] Following his arrest, he provided the police with written permission to seize any property under his control.[52] Even with this voluntary grant of consent, the government also obtained a warrant to search his computers for any evidence concerning "the sale and distribution of controlled substances."[53] After viewing the directories of Carey's two computers, a detective and computer technician downloaded various files onto floppy disks.[54] Although they observed many JPG image files with "sexually suggestive titles," the investigators' initial keyword searches were limited to terms having some relationship to the drug offenses.[55]

When these keyword searches failed to produce any files responsive to the warrant, the detective explored the directories using a more precise search protocol; specifically, he looked at the name and extension of each file to determine if they were associated with illegal drug activites.[56] After coming across several unidentifiable image files, he opened one of them.[57] The file contained child pornography.[58]

---

49. *Compare* United States v. Williams, 592 F.3d 511, 523 (4th Cir. 2010) (holding that the plain view doctrine can be applied to computer searches), *cert. denied*, 131 S. Ct. 595 (2010), *with* United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1006 (9th Cir. 2009) (en banc) (holding that the plain view doctrine cannot be applied to computer searches), *modified on reh'g*, 621 F.3d 1162 (9th Cir. 2010) (en banc).

50. 172 F.3d 1268 (10th Cir. 1999).

51. *Id.* at 1270.

52. The Tenth Circuit rejected the argument that this written consent also applied to Carey's computer files. *Id.* at 1274. According to the court, his consent authorizing the search of the "premises and property located at 3225 Canterbury # 10" was limited to the apartment itself. *Id.* Thus, the government could not rely on a broad consent search to actually seize the computer files because this evidence was beyond the warrant's specific language. *Id.*

53. *Id.* at 1270.

54. *Id.*

55. *Id.* at 1270–71 ("His method was to enter key words such as, 'money, accounts, people, so forth' into the computer's explorer to find 'text-based' files containing those words.").

56. *See id.* at 1271.

57. *Id.*

58. *Id.*

Following this discovery, the detective downloaded approximately 244 image files to floppy disks and occasionally viewed some of the files' contents to determine if they also contained pornographic images.[59] After being charged under 18 U.S.C. § 2252A(a)(5)(B)—a federal statute which prohibits the transportation of goods containing child pornography through interstate commerce[60]—Carey moved to suppress this evidence because, he argued, the detective's procedure permitted the general and unlawful search of his computers.[61] The United States responded by comparing computer searches to traditional physical searches involving filing cabinets or other closed containers.[62] Like the discovery of pornographic photographs in a filing cabinet, the United States argued this seizure was lawful because the computer files fell within the warrant's scope.[63] Specifically, Carey could have stored the JPG files with drug-related evidence, and therefore, the warrant explicitly authorized the search of any computer files, including the pornographic images.[64]

The Tenth Circuit rejected these arguments by relying on an inadvertence standard. As the court noted, once the detective opened the initial JPG file, he *expected* to find additional child pornography.[65] According to the detective's own testimony, after he discovered the first explicit image, he abandoned his drug-trafficking investigation and instead searched for additional child pornography.[66] He only returned to the drug investigation after "conducting a five hour search" for these targeted files.[67] Each of the seized images contained a JPG extension, and most of them also included sexually suggestive titles.[68] In this respect, the court believed the filing-cabinet analogy was inappropriate because "[the detective] knew, or at least had probable cause to know, each drawer was properly labeled and its contents were clearly described in the label."[69] Stated differently, the detective knew he would uncover evidence beyond the warrant's scope; therefore, the court suppressed every file seized after the first, inadvertent discovery.[70]

Even though most courts do not follow the *Carey* approach, some recent decisions still seem to emphasize, or at least take into account, the requirement of inadvertent discovery.[71] In *United States v. Mann*, for example, the Seventh Circuit

---

59. *Id.* ("Although none of the disks was viewed in its entirety, Detective Lewis looked at 'about five to seven' files on each disk.").

60. *Id.* at 1270 (citing 18 U.S.C. § 2252A(a)(5)(B) (1996)).

61. *Id.* at 1271–72.

62. *Id.* at 1272 ("[A] computer search such as the one undertaken in this case is tantamount to looking for documents in a file cabinet, pursuant to a valid search warrant, and instead finding child pornography.").

63. *Id.*

64. *Id.*

65. *Id.* at 1273.

66. *Id.*

67. *Id.*

68. *Id.* at 1274.

69. *Id.* at 1275.

70. *Id.* at 1273, 1276–77.

71. *Compare* United States v. Grimmett, 439 F.3d 1263, 1268 (10th Cir. 2006) (limiting the application of a subjective-intent test by instructing lower courts to look to the warrant's scope rather than at the officer's motivations to determine the lawfulness of plain

upheld the government's seizure of child pornography discovered during a search for evidence of voyeurism.[72] The defendant, a lifeguard instructor, secretly installed a video camera in a pool locker room to capture women changing out of their clothes.[73] After one of his female students discovered the camera and contacted the police, the State of Indiana obtained a warrant to search Mann's computers and external hard drives for any evidence relevant to these recordings.[74]

During their investigation, law enforcement officials discovered over 677 flagged thumbnails of child pornography and two videos recorded from a high school locker room.[75] Although the Seventh Circuit admitted almost all of these materials into evidence, the court suppressed four files that had been flagged by a "known file filter" ("KFF") alert.[76] The KFF database was a catalogue of files that allowed officers to search a computer for "targeted" hash values;[77] most of these values were linked to illicit files containing child pornography.[78] The court excluded the KFF-discovered files because once the database flagged the images, the detective "knew (or should have known) that files in a database of known child pornography images would be outside the scope of the warrant."[79]

This inadvertence approach is ultimately inconsistent with the Supreme Court's instruction in *Horton v. California*[80]—one of the Court's seminal decisions for defining the scope of plain view seizure. Under *Horton*, the relevant inquiry for admissibility is not focused on subjective standards; instead, the proper analysis evaluates whether the officer possessed a lawful right of access to the item as defined by the warrant's language.[81] Inadvertent discovery offers no additional privacy protections because the requirement of particularity "prevent[s] the police

---

view seizure), *and* United States v. Kim, 677 F. Supp. 2d 930, 948–49 (S.D. Tex. 2009) (concluding that most courts, including the Tenth Circuit, no longer rely on an officer's subjective intent), *with* United States v. Mann, 592 F.3d 779, 784–85 (7th Cir. 2010) (applying a subjective-intent test).

72. 592 F.3d at 780.

73. *Id.*

74. *Id.* at 780–81.

75. *Id.* at 781. This investigation occurred in two separate phases. During the initial search of his computers, Detective Huff discovered evidence that Mann visited a website called, "Perverts Are Us," "where he had read and possibly downloaded stories about child molestation." *Id.* The detective also found child pornography, along with a story apparently written by Mann about a "swim coach masturbating while watching young girls swim." *Id.* The second phase focused on Mann's external hard drive. *Id.* It was during this search that Detective Huff discovered both the thumbnail images of child pornography and the locker room recordings. *Id.*

76. *Id.* at 786.

77. A hash value is an identifier on computer files resulting from "subjecting the set of electronic data to a complex algorithm." Leonard Deutchman, *Do Computer Searches Distort the 'Plain View' Doctrine?*, LAW TECHNOLOGY NEWS (May 14, 2010), http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202458173965. "[T]he long, alphanumeric string" is unique to the specific file being analyzed. *Id.* Therefore, two identical files will have the same hash value. *Id.*

78. *Mann*, 592 F.3d at 781.

79. *Id.* at 784.

80. 496 U.S. 128 (1990).

81. *Id.* at 140.

from conducting general searches, or from converting specific warrants into general warrants."[82] The warrant's terms will sufficiently limit the scope and duration of a search.[83] Therefore, particularity renders any additional requirement for inadvertence unnecessary because any evidence seized outside the warrant's specific terms will be deemed inadmissible.[84]

In *Horton*, the Court also expressed a reluctance to investigate the officer's subjective state of mind to determine whether he anticipated finding new evidence. Justice Stevens noted that "evenhanded 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."[85] Although the Supreme Court has not revisited this issue in the context of computer searches, it has held that an officer's subjective beliefs are irrelevant for inquiries involving probable cause. In *Whren v. United States*, for example, the Court upheld the constitutionality of a pretextual stop because, according to Justice Scalia's analysis, determinations of reasonableness are rooted in objective standards.[86] Although it can certainly be argued that questions of reasonableness in this specific "stop" context implicate a slightly different liberty interest than search-and-seizure law—in other words, the person is being seized rather than his property—the *Whren* decision, when read with *Horton*, demonstrates the Court's attempt to limit subjective standards in Fourth Amendment jurisprudence. Even in computer searches, this case law provides a powerful basis to eliminate any analysis directed toward an investigator's motivations or subjective beliefs.

B. The Prophylactic-Test Approach

In *United States v. Comprehensive Drug Testing, Inc.*,[87] the Ninth Circuit also confronted the issue of whether the plain view doctrine applied to computers. In an en banc decision, the court adopted a series of prophylactic rules that prevented the government from relying on the plain view doctrine in computer searches.[88] No other federal circuit has embraced this standard, and the Ninth Circuit has since written an amended opinion reclassifying these rules as "guidance" rather than mandatory circuit law.[89] The most common criticism of this short-lived, en banc decision was that the Ninth Circuit offered no legitimate basis

---

82. *Id.* at 139.

83. *Id.* at 141–42.

84. *Id.* at 140 ("[I]f the police stray outside the scope of an authorized . . . search they are already in violation of the Fourth Amendment, and evidence so seized will be excluded." (quoting Coolidge v. New Hampshire, 403 U.S. 443, 517 (1971))).

85. *Id.* at 138.

86. 517 U.S. 806, 813 (1996); *see also* Devenpeck v. Alford, 543 U.S. 146, 153 (2004) ("Our cases make clear that an arresting officer's state of mind (except for the facts that he knows) is irrelevant to the existence of probable cause.").

87. 579 F.3d 989 (9th Cir. 2009) (en banc), *modified on reh'g*, 621 F.3d 1162 (9th Cir. 2010) (en banc).

88. *Id.* at 1006.

89. *See* United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1178 (9th Cir. 2010) (reh'g en banc) (Kozinski, J., concurring).

to completely eliminate plain view seizure in digital-evidence cases.[90] Although the en banc decision is no longer binding authority in the Ninth Circuit, criminal defendants will likely use Chief Judge Kozinski's reasoning, now embodied in *Comprehensive Drug Testing*'s concurring opinion, in circuits facing this issue as a matter of first impression.[91]

The Ninth Circuit's controversial holding arose from a complex fact pattern involving professional baseball players, steroids, and the now infamous Bay Area Lab Cooperative ("BALCO"). In an effort to discover the rate of performance-enhancing drug use among its players, Major League Baseball ("MLB") and the MLB Players Association hired Comprehensive Drug Testing, Inc. ("CDT") to administer a suspicionless testing program that included each MLB player.[92] In exchange for the players' participation in the program, League officials assured them that the results would remain anonymous and confidential.[93] The program's purpose was to determine whether more than 5% of the players would test positive because, if this percentage was exceeded, MLB would require additional testing in future seasons.[94] CDT kept a list of the tested players and the program's results.[95]

After the CDT testing program concluded, the federal government began an investigation to determine if BALCO had distributed steroids to MLB players.[96] The government learned that ten players tested positive in the CDT program (including well-known players such as Manny Ramirez, Barry Bonds, Sammy Sosa, and Alex Rodriguez),[97] and as part of its BALCO investigation, secured a grand jury subpoena in the Northern District of California to recover all "drug testing records and specimens" in CDT's possession relating to Major League Baseball.[98] These broad terms not only included the records of the ten players who

---

90. United States v. Mann, 592 F.3d 779, 785 (7th Cir. 2010) ("[T]here is nothing in the Supreme Court's case law (or the Ninth Circuit's for that matter) counseling the complete abandonment of the plain view doctrine in digital evidence cases.").

91. For example, prior to the Ninth Circuit's amended opinion, criminal defendants had used *Comprehensive Drug Testing* to not only suggest that computers are entitled to heightened Fourth Amendment protections, *see, e.g.*, Defendant's Motion to Suppress Evidence at 9, United States v. Fahlberg, No. 09-00683-MMM (C.D. Cal. May 31, 2010), but also that plain view seizure transforms narrow computer searches into general ones, *see, e.g.*, Brief for Defendant-Appellant at 38, United States v. Stabile, 633 F.3d 219 (3d Cir. 2011) (Nos. 09-3500, 09-3501).

92. *Comprehensive Drug Testing*, 579 F.3d at 993. It should be noted that although CDT was responsible for administering the program and collecting the players' urine samples, an independent laboratory called Quest Diagnostics, Inc. actually tested the specimens for banned substances. *Id.*

93. *Id.*

94. *Id.*

95. *Id.* ("CDT maintained the list of players and their respective test results; Quest kept the actual specimens on which the tests were conducted.").

96. *Id.*

97. Lily R. Robinton, Note, *Courting Chaos: Conflicting Guidance from Courts Highlights the Need for Clearer Rules to Govern the Search and Seizure of Digital Evidence*, 12 YALE J.L. & TECH. 311, 313 (2010).

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

tested positive for steroids, but also included any evidence relevant to the testing program itself.[99] After they failed to convince the government to narrow the subpoena, both CDT and the MLB Players Association filed a motion to quash the warrant.[100]

On the same day as this filing, the federal government obtained a search warrant in the Central District of California to search CDT's Long Beach facilities for evidence that *was* limited to the positive-testing players.[101] During the execution of this warrant, federal officials seized certain computer files known as the "Tracey Directory" to analyze at an off-site location.[102] As the investigators soon discovered, the incriminating scope of these files went far beyond the original ten players; one of the files was a Microsoft Excel spreadsheet containing "information and test results involving hundreds of other baseball players and athletes engaged in other professional sports."[103] The government ultimately used this evidence "to generate additional warrants and subpoenas to advance the investigation."[104]

The warrants contained a very specific protocol that outlined the permitted scope of each search.[105] Under the Ninth Circuit's existing authority for searches involving intermingled, physical documents,[106] investigators were first required to determine whether any data implicating the ten players could be segregated from non-responsive items during an on-site search.[107] This threshold step was to be performed by forensic experts who were not involved in the CDT investigation as case agents.[108] Because the investigators could not segregate the non-responsive data on-site, the warrant required forensic experts to screen and segregate the digital materials during an off-site search before the case agents could actually inspect the files.[109]

---

99. *Id.*

100. *Id.*

101. *Id.* The government's efforts were not limited to California. After obtaining the Long Beach warrant, investigators promptly secured a warrant in the District of Nevada to seize the urine samples located at Quest's lab in Las Vegas. *Id.*

102. *Id.* at 996.

103. *Id.* (quoting United States v. Comprehensive Drug Testing, Inc., No. CV-04-02887-FMC (C.D. Cal. Oct. 1, 2004)).

104. *Id.* at 999.

105. *Id.* at 995–96.

106. This screen-and-segregate requirement emerged in *United States v. Tamura*, 694 F.2d 591, 595–96 (9th Cir. 1982). In *Tamura*, the government seized thousands of documents—including 11 cardboard boxes of computer printouts, 34 file drawers of vouchers, and 17 drawers of cancelled checks—for an investigation involving various counts of fraud, conspiracy, and racketeering. *Id.* at 594–95. The Ninth Circuit found this search to be unreasonable because, although the agents were permitted to inspect the records for evidence responsive to the warrant, "the wholesale *seizure* for later detailed examination of records not described in a warrant is significantly more intrusive." *Id.* at 595.

107. *Comprehensive Drug Testing*, 579 F.3d at 996.

108. *Id.*

109. *Id.* at 995.

Although the investigating agents completely ignored this screen-and-segregate protocol,[110] the United States argued that the plain view doctrine applied to the "Tracey Directory."[111] Specifically, it believed the agents were in a lawful position under the warrant's terms to seize any incriminating evidence, which included any records extending beyond the original ten players.[112] By moving under Federal Rule of Criminal Procedure 41(g), CDT and the MLB Players Association demanded the return of any information implicating the unnamed players in the "Tracey Directory."[113] In granting the 41(g) motion, the Ninth Circuit created a series of complex, prophylactic rules eliminating the plain view doctrine's application to computer searches.[114] First, the government had to forswear any reliance on the plain view doctrine.[115] Second, the government's search protocol needed to be designed in such a way to limit the discovery of evidence not supported by probable cause.[116] Third, any forensic search was to be carried out by an independent third party or a government agent who agreed not to share any evidence with investigators.[117] Finally, the government had to return any non-responsive evidence that a recipient lawfully possessed or destroy evidence classified as contraband.[118] Under these rules, the government could never lawfully seize digital evidence in plain view.[119]

Again, although these rules are no longer binding authority in the Ninth Circuit, Chief Judge Kozinski's concurring opinion incorporates these search requirements to ensure the government's compliance with the Fourth

---

110. *Id.* at 996.

111. *Id.* at 997.

112. *Id.*

113. *Id.* at 993. Rule 41(g) is used as a vehicle by which parties to litigation can seek the return of improperly seized property. FED. R. CRIM. P. 41(g). Its application in the en banc decision is novel, however, because the unnamed players, i.e., those who were not specified in the warrant, were not the parties who actually filed the motion. It is therefore questionable whether the Ninth Circuit actually needed to address the issue of plain view seizure because the named parties may not have had the authority to actually request the return of materials. *See Comprehensive Drug Testing*, 579 F.3d at 1022–23 (Ikuta, J., dissenting); *see also* Preiser v. Newkirk, 422 U.S. 395, 401 (1975) ("[A] federal court has neither the power to render advisory opinions nor to decide questions that cannot affect the rights of litigants in the case before them." (citation omitted) (internal quotation marks omitted)). The court ultimately resolved this issue by concluding that any continued seizure violated the privacy interests of any members of the Players Association and also interfered with the Association's business operations. *Comprehensive Drug Testing*, 579 F.3d at 1002 (majority opinion). *But cf.* Warshak v. United States, 532 F.3d 521, 528 (6th Cir. 2008) (holding that a pre-enforcement challenge to future e-mail searches presented a "purely speculative legal question").

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

115. *Id.*

116. *Id.*

117. *Id.*

118. *Id.*

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

Amendment.[120] By preventing government officials from ever being in a position to seize digital evidence in plain view, the prophylactic approach seems, at least in theory, to be an efficient check on overbroad searches. However, these rules create more problems than they actually solve and should not be adopted in any form.

The elimination of plain view seizure in such a context unnecessarily forecloses the doctrine's proper, incremental development through case law and also undermines well-established Supreme Court precedent.[121] The exact specifics of a search are "generally left to the discretion of the executing officers."[122] The Supreme Court has never interpreted the Fourth Amendment to require officers to specify the precise manner and methods by which they execute a search.[123] Indeed, the prophylactic-test approach gives the courts, specifically magistrate judges, unprecedented authority to supervise the execution of warrants. By requiring the use of filter teams in *all* digital-evidence investigations, this reasoning abandons the Supreme Court's repeated refusal to "declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment."[124]

The requirement of independent filter teams also creates logistical nightmares for both law enforcement agents and prosecutors. Because computer searches "can be as much an art as a science,"[125] they often require detailed case knowledge to determine what information is actually relevant to an investigation.[126] Under Chief Judge Kozinski's model, case agents would need to spend significant amounts of time briefing the filter teams on the facts *and* law relevant to an investigation. In complex cases involving terrorism, conspiracy, or drug trafficking, this briefing could span weeks or even months.[127] Even with these procedures, the filter teams would likely overlook crucial data because the investigating agents will simply be more familiar with the case and, thus, more qualified to execute a forensic search.[128] With such logistical problems in play, the government will certainly never agree to this voluntary search protocol despite a "safe harbor" to conduct the investigation.[129]

---

120. United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1178 (9th Cir. 2010) (reh'g en banc) (Kozinski, J., concurring).

121. *See Comprehensive Drug Testing*, 579 F.3d at 1013 (Callahan, J., concurring in part and dissenting in part).

122. Dalia v. United States, 441 U.S. 238, 257 (1979).

123. United States v. Grubbs, 547 U.S. 90, 98 (2006) (quoting *Dalia*, 441 U.S. at 257).

124. Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 663 (1995) (quoting Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 629 n.9 (1989)).

125. United States v. Brooks, 427 F.3d 1246, 1252 (10th Cir. 2005).

126. Brief for the United States in Support of Rehearing En Banc by the Full Court at 15–16, *Comprehensive Drug Testing*, 579 F.3d 989 (Nos. 05-10067, 05-15006, 05-55354).

127. *See id.* at 16.

128. *Id.* ("Even after receiving such a crash course, filter team members will be unlikely to know a case as well as the case agents, with the result that at least some responsive and potentially case-critical information will go unrecognized.").

129. *See* United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1178 (9th Cir. 2010) (reh'g en banc) (Kozinski, J., concurring).

Chief Judge Kozinski's analysis also unnecessarily forecloses the development of case law on this issue.[130] Computer technology is continuously evolving, and contrary to Kozinski's concurrence, courts should be allowed to define the scope of plain view seizure in this context. This fact-driven approach is consistent with the development of Fourth Amendment jurisprudence in other key areas such as defining the requisite standard for valid stops (reasonable suspicion)[131] and search-and-seizure law (probable cause).[132] Moreover, other jurisdictions have established a workable framework for defining the permitted scope of plain view seizure in digital-evidence cases.[133] Therefore, courts should be reluctant to place blanket prohibitions on this doctrine.

C. The Computers-as-Containers Approach

The computers-as-containers approach is the final category of judicial decisions involving the plain view seizure of digital evidence. Although many courts at both the federal and state levels have adopted this framework,[134] the most prominent example of this approach arose from the Fourth Circuit's holding in *United States v. Williams*.[135] In *Williams*, a Baptist church located in Fairfax, Virginia began receiving threatening e-mails from a person identifying himself as "Franklin Pugh."[136] During one particularly perverse message, the sender named several of the children who attended the church's school and expressed his desire to molest the boys and sacrifice them to God.[137] He commented, "I know where they go to lunch after church. I know where they live. I know when they come and leave school. There's [sic] boys I'd love to sleep with right now. There is an endless supply."[138]

In subsequent messages, the sender focused his profane commentary on specific boys by referring to them by name and describing his sexual urges in explicit detail.[139] Before he could carry out any of his threats, the Fairfax County Police Department determined some of these e-mails were sent from an account

---

130. *See id.* at 1180.

131. Terry v. Ohio, 392 U.S. 1, 10 (1968). Although the Court did not actually use the term "reasonable suspicion" in *Terry*, subsequent cases make clear that, unlike probable cause, this standard only requires "some minimal level of objective justification." INS v. Delgado, 466 U.S. 210, 216–17 (1984).

132. Brinegar v. United States, 338 U.S. 160, 174–76 (1949).

133. *See generally infra* Part II.C.

134. *See, e.g.*, United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999); United States v. Farlow, No. CR-09-38-B-W, 2009 WL 4728690, at *7 (D. Me. Dec. 3, 2009) (relying on *Upham*); United States v. Al-Marri, 230 F. Supp. 2d 535, 541 (S.D.N.Y. 2002); United States v. Gray, 78 F. Supp. 2d 524, 528–29 (E.D. Va. 1999); United States v. Barth, 26 F. Supp. 2d 929, 936 (W.D. Tex. 1998); People v. Gall, 30 P.3d 145, 153 (Colo. 2001); Frasier v. State, 794 N.E.2d 449, 463–64 (Ind. Ct. App. 2003); Commonwealth v. McDermott, 864 N.E.2d 471, 488 (Mass. 2007); State v. Schroeder, 613 N.W.2d 911, 916 (Wis. Ct. App. 2000).

135. 592 F.3d 511, 521, 523 (4th Cir. 2010), *cert. denied*, 131 S. Ct. 595 (2010).

136. *Id.* at 514.

137. *Id.*

138. *Id.*

139. *Id.* at 514–15.

registered to Karol Williams, wife of the defendant, Curtis Williams.[140] After this crucial discovery, the police obtained a warrant to search their home for any evidence relevant to the harassment.[141]

The warrant permitted the broad search and seizure of digital evidence including "computer systems and digital storage media, videotapes, videotape recorders, documents, [and] photographs."[142] In addition to discovering an unlicensed machine gun and a silencer, investigators from both the Fairfax Police Department and FBI also seized various computers, DVDs, CDs, and external storage devices.[143] FBI agents immediately began a thorough search of these items. After discovering "many deleted images of young male erotica"[144] during the preliminary phases of the investigation, one of the agents searched the contents of a DVD labeled, "Virus Shield, Quarantined Files, Destroy."[145]

Following the rather typical pattern of plain view seizure involving computers, the agent observed thousands of thumbnail images of minor boys; 39 of these files contained child pornography.[146] Williams was indicted on one count of child pornography possession and various weapons violations.[147] Under a Fourth Amendment challenge, he contested the child pornography's admissibility by arguing that the government seizure exceeded the scope of the warrant.[148] Moreover, he claimed this seizure did not fall within the plain view doctrine or any other recognized exception to the Fourth Amendment's warrant requirement.[149]

The Fourth Circuit rejected Williams's argument on two grounds. First, because the warrant's terms authorized a search for "instrumentalities of computer harassment" and photographs communicating vulgar or obscene language, the warrant implicitly permitted the seizure of child pornography.[150] The court concluded that this evidence was relevant in establishing the "authorship and purposes" of the profane e-mails.[151] Alternatively, the Fourth Circuit held that even if the warrant's terms did not authorize a search for child pornography, the seizure was justified under the plain view doctrine.[152]

In construing the warrant's terms broadly, the court concluded that the investigators were permitted to search computers and other forms of digital media—mainly, the CDs and DVDs—for *any* evidence of harassment or threatening behavior.[153] Therefore, they could view the contents of each file to

---

140. *Id.* at 515.
141. *Id.*
142. *Id.*
143. *Id.* at 516.
144. *Id.* As the Fourth Circuit noted in its decision, child erotica refers to "non-pornographic images of children, apparently used for sexual gratification." *Id.* at 515 n.1.
145. *Id.* at 516.
146. *Id.*
147. *Id.*
148. *Id.* at 517.
149. *Id.* at 518.
150. *Id.* at 520.
151. *Id.*
152. *Id.* at 521.
153. *Id.*

determine which ones were actually responsive to the warrant.[154] According to the Fourth Circuit, a search exclusively confined to file names or extensions would be ineffective because a user can easily alter these identifiers to conceal the file's actual contents.[155] For example, picture files containing child pornography or other illicit materials can be mislabeled with relatively innocuous titles such as "Rodgers's Lambeau Leap.img" or "Corey in the Snow.jpg."[156] Likewise, a file's extension can easily be changed as an attempt to conceal illicit photographs and video data.[157]

For these reasons, the Fourth Circuit refused to depart from the existing rules for physical searches.[158] Although the court noted that computers are capable of storing large amounts of data, it still believed digital searches could be appropriately analogized to filing cabinets or other closed containers.[159] In fact, similar to searches involving large quantities of physical documents, investigators would likely examine certain innocuous computer files to determine whether they were actually responsive to the warrant.[160] The court did, however, warn law enforcement agents to conduct these searches with "care and respect for privacy" as to avoid seizure beyond the warrant's specific terms.[161]

This respect for privacy is ultimately maintained through the traditional application of the plain view doctrine.[162] Judges, prosecutors, and law enforcement officials can, and should, be expected to comply with the already-existing framework for search-and-seizure law. Because the language of a warrant will establish the proper constitutional boundaries of a search, bright-line exclusions

---

154. *Id.*

155. *Id.* at 522.

156. *Id.*; *see also* Ziff, *supra* note 12, at 863 ("A given file name or extension says nothing about the contents of a file; it only reveals how the file's owner decided to label it.").

157. *See* Ziff, *supra* note 12, at 863. In Windows 7, this process can be accomplished in two relatively simple steps. *See* Hasan Nizamani, *How to Change File Extension in Windows 7*, PROGRAMMERFISH (Oct. 25, 2009), http://www.programmerfish.com/how-to-change-file-extension-in-windows-7/. A user must allow the operating system to display file extensions in the "Folder Options" menu. *Id.* The file extension can then be changed by simply right-clicking the specific file and renaming it in the desired format. *Id.*

158. *Williams*, 592 F.3d at 523. By relying on the traditional rules for plain view seizure, the court also admonished any approach requiring inadvertent discovery. *Id.* at 522–23. As explored in previous sections of this Note, *see supra* Part II.A, the Fourth Circuit relied on existing Supreme Court authority to reject the Tenth Circuit's inadvertence approach, *Williams*, 592 F.3d at 523. Because the search warrant authorized the agents to "open and cursorily view each file," the discovery of child pornography did not intrude upon the defendant's privacy interests beyond those implicated by the warrant itself. *Williams*, 592 F.3d at 523; *accord* United States v. Stabile, 633 F.3d 219, 240 (3d Cir. 2011) (rejecting an inadvertency requirement for plain view seizure because, even in computer searches, "an investigator's subjective intent is not relevant to whether a search falls within the scope of a search warrant").

159. *Williams*, 592 F.3d at 523.

160. *Id.* at 519–20.

161. *Id.* at 523–24.

162. *See generally infra* Part III.

improperly bypass the judiciary's extraordinary responsibility to assess the reasonableness and legality of government action.

III. APPLYING EIGHTEENTH-CENTURY DOCTRINE TO TWENTY-FIRST-CENTURY TECHNOLOGY

By following the analysis in *Williams*, courts can apply the plain view doctrine to computers without usurping the proper constitutional boundaries of government search authority. The computers-as-containers approach strikes a delicate balance between the need for exhaustive police investigations *and* the privacy concerns implicated by plain view seizure. Although computers can store significantly more information than filing cabinets and other closed containers,[163] this approach is also consistent with existing Supreme Court precedent.[164] While some legal scholars have expressed concern that the plain view doctrine transforms computer search warrants into unlawful, general warrants,[165] the majority of jurisdictions, despite such criticism, have embraced the doctrine's expansive application to computers.[166]

This Section will address the reasons why courts should broadly apply the traditional physical search rules to computers. It will discuss the Fourth Amendment's requirement for particularity in warrants and how this mandate empowers magistrate judges to restrict overbroad computer searches by denying warrant applications. This Section will also explore the plain view doctrine's proper application to both on- and off-site searches where investigators use forensic tools to discover evidence; specifically, it will evaluate the complex interplay between criminal investigations and the methods by which suspects conceal their illicit activities. This doctrine will not permit the wholesale seizure of digital evidence in many investigations because the legality of plain view seizure will ultimately depend on the search warrant's language and scope. Finally, when plain view seizure is appropriate, the government should always seek a second warrant before seizing evidence beyond the original warrant to ensure compliance with the Fourth Amendment.

---

163. *See supra* Introduction.

164. *See supra* text accompanying notes 121–24.

165. *See, e.g.*, Chang, *supra* note 47, at 50; Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 299 (2005) ("These rules help ensure that warrant searches do not devolve into general warrants that authorize general rummaging through a suspect's property."); Robinton, *supra* note 97, at 333; Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 110 (1994). *But see, e.g.*, Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L.J. 193, 205 (2005) (rejecting a "special approach" to computer searches by analogizing computers to closed containers); Ziff, *supra* note 12, at 861–71 (arguing that when applied to computer searches, existing physical search rules "adequately protect privacy interests").

166. *See supra* note 134 (citing various jurisdictions that have used the computers-as-containers approach to justify the plain view seizure of digital evidence).

A. Particularity in Warrants: The Preventative Check on Overbroad Searches

Absent some type of justification for a warrantless search,[167] the Fourth Amendment requires warrants to "describe the things to be seized with sufficient particularity to prevent a general exploratory rummaging through one's belongings."[168] Because investigators will not be in a lawful position to seize digital evidence in open view without a warrant—and thus will be unable to invoke the plain view doctrine[169]—the requirement of particularity is the first preventative check on plain view seizure. In certain criminal investigations, agents may be searching the storage device (e.g., hard drive, CD-ROM, flash memory) for a select number of files in identifiable locations due to informant testimony or other admissions. A magistrate judge might determine that a warrant authorizing the search of every computer file would be unconstitutionally overbroad because a relatively simple on-site search would be sufficient to uncover this evidence.[170] In such instances, the warrant's terms will implicate the electronic data to be seized rather than the physical storage device itself.[171]

In other circumstances, a more precise description in the warrant application is simply infeasible.[172] In *United States v. Lacy*, for example, the Ninth

---

167. Although outside the scope of this Note, one of the most interesting developments of search-and-seizure law involves the interplay between consent searches and plain view seizure. The legality of plain view seizure during a consent search will depend upon the voluntariness of the defendant's consent *and* the scope of this grant. *See* Florida v. Jimeno, 500 U.S. 248, 252 (1991) ("A suspect may of course delimit as he chooses the scope of the search to which he consents."). In *United States v. Stierhoff*, for example, the court held that officers could not lawfully seize incriminating tax-related evidence because the defendant only consented to the search of file folder marked "Creative Writing." 477 F. Supp. 2d 423, 443 (D.R.I. 2007), *aff'd*, 549 F.3d 19 (1st Cir. 2008); *accord* United States v. Richardson, 583 F. Supp. 2d 694, 722–23 (W.D. Pa. 2008) (holding that the defendant's consent to a search involving his Internet activity did not extend to file folders containing child pornography). This analysis is incredibly important because consent searches "are a dominant—[and] perhaps *the* dominant—type of warrantless search." DRESSLER & MICHAELS, *supra* note 32, at 261. As noted by Dressler and Michaels, "there are few areas of Fourth Amendment jurisprudence of greater practical significance than consent searches." *Id.*

168. United States v. Mann, 592 F.3d 779, 782 (7th Cir. 2010); *see also* Marron v. United States, 275 U.S. 192, 196 (1927) ("The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.").

169. *See supra* text accompanying note 38 (discussing the requirements for lawful seizure under the plain view doctrine).

170. *See* United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) (discussing the requirement that a warrant should specify "the narrowest definable search and seizure reasonably likely to obtain the [evidence]").

171. *See* Orin S. Kerr, *Search Warrants in an Era of Digital Evidence*, 75 MISS. L.J. 85, 99 (2005) ("This approach does not describe accurately what the police will do on-site, but it does describe the evidence sought at the second stage of the warrant process—the off-site electronic search.").

172. United States v. Lacy, 119 F.3d 742, 746 (9th Cir. 1997). *But cf.* Ark. Chronicle v. Easley, 321 F. Supp. 2d 776, 792–93 (E.D. Va. 2004) (holding that a warrant

Circuit held that a warrant was not unconstitutionally overbroad when the government failed to specify the exact computer systems subject to the search.[173] Although the government knew that the defendant downloaded child pornography, the investigators were unaware of whether he stored these materials on a computer hard drive or on some form of removable media.[174] This holding is ultimately in accord with Justice Stevens's observation in *Kyllo v. United States* that special rules or distinctions based on a certain type of technology are "unwise[] and inconsistent with the Fourth Amendment."[175] Warrant language permitting the wholesale search of a computer's hard drive will not be unconstitutionally overbroad if the investigation requires such generality.[176] In fact, as Justice Scalia discussed in *United States v. Grubbs*, the Fourth Amendment does not require a general particularity requirement.[177] Instead, a warrant must only particularly describe "the place to be searched" and "the persons or things to be seized."[178] In situations where a user stores illicit materials such as child pornography on a hard drive, the computer itself can be considered contraband.[179]

B. A Game of Hide-and-Seek: Searching a Computer's File System

Once a magistrate judge determines that a warrant application is particularized and supported by probable cause, the government will usually execute a warrant in a two-step process.[180] First, in what is called the "physical search stage," agents will enter the location to be searched and seize the electronic storage devices implicated by the warrant.[181] This on-site seizure may include computers, diskettes, CD-ROMs, and other devices that might contain relevant

---

permitting the "wholesale . . . seizure of voluminous private, personal and confidential materials" was overbroad).

173. 119 F.3d at 746.

174. *Id.* at 746–47.

175. 533 U.S. 27, 41 (2001) (Stevens, J., dissenting).

176. As discussed previously, *supra* Part II.B, *Comprehensive Drug Testing* is one example of a court imposing ex ante restrictions on computer search warrants. In circumstances like *Comprehensive Drug Testing*, some courts have replaced traditional ex post review—i.e., review occurring after the warrant's execution—with ex ante procedures allowing magistrate judges to review, and possibly deny, the government's search protocol. *See* Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241, 1244–45 (2010). As Professor Kerr notes, because computer search-and-seizure rules "remain in their infancy," certain magistrates have conditioned warrant approval on the government's precise methods for executing a search. *Id.* at 1248. However, ex ante review not only restricts constitutionally permitted search methods, *id.* at 1278, but also clashes with the traditional rule that the exact specifics of a search are "generally left to the discretion of the executing officers," Dalia v. United States, 441 U.S. 238, 257 (1979).

177. 547 U.S. 90, 97 (2006).

178. *Id.* (quoting U.S. CONST. amend. IV).

179. U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 70–71 (3d ed. 2009), *available at* http://www.cybercrime.gov/ssmanual/ssmanual2009.pdf ("If the computer hardware is itself contraband, an instrumentality of crime, or fruits of crime, the warrant should describe the hardware and indicate that the hardware will be seized.").

180. Kerr, *supra* note 176, at 1248.

181. *Id.*

evidence. In most investigations, agents will seize these electronic devices without searching the confiscated hardware.[182] Instead, the warrant process will proceed to a second step, the "electronic search stage," where law enforcement personnel, usually consisting of specialized computer technicians, conduct a forensic investigation of the hardware.[183] The electronic search stage is necessary in most investigations for several reasons. In addition to obvious inefficiency concerns,[184] a manual search of an operating system may lead to evidentiary issues because of compromised or damaged hardware, data loss, or poor forensic analysis.[185] Therefore, investigators will usually create a bitstream copy of a computer's hard drive that duplicates "every bit and byte on the target drive."[186] Assuming the file is read-only, investigators can freely search the bitstream image without altering the copy.[187] Courts have routinely upheld these off-site procedures assuming, of course, the investigators have complied with the warrant's scope and the Fourth Amendment.[188]

Regardless of whether investigators perform an on- or off-site investigation, a court must evaluate the legality of any computer search under a standard of reasonableness.[189] Although certain court decisions involving the plain view doctrine seem to turn on the amount of files searched as compared to the total number of files actually stored on the hard drive,[190] the more important question is whether the seized materials fall within the warrant's scope. Take the following

---

182. *Id.*

183. *Id.*

184. United States v. Hill, 459 F.3d 966, 974–75 (9th Cir. 2006) ("[T]he officers would have to examine every one of what may be thousands of files on a disk—a process that could take many hours and perhaps days.").

185. G. Robert McLain, Jr., Note, United States v. Hill*: A New Rule, But No Clarity for the Rules Governing Computer Searches and Seizures*, 14 GEO. MASON L. REV. 1071, 1093 (2007); *see also Hill*, 459 F.3d at 974 (discussing the serious risk that investigators might "damage the storage medium or compromise the integrity of the evidence by attempting to access the data at the scene").

186. Kerr, *supra* note 1, at 540–41. Investigators can also install software on a computer to "freeze" its contents and restrict any changes to the file system. *See* State v. Schroeder, 613 N.W.2d 911, 913 (Wis. Ct. App. 2000).

187. Kerr, *supra* note 1, at 540–41.

188. *See, e.g.*, United States v. Hay, 231 F.3d 630, 637 (9th Cir. 2000) ("[T]he affidavit explained why it was necessary to seize the entire computer system in order to examine the electronic data for contraband. It also justified taking the entire system off site because of the time, expertise, and controlled environment required for a proper analysis."); United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) (describing the impracticality of performing an on-site inspection in certain circumstances); United States v. Hunter, 13 F. Supp. 2d 574, 583 (D. Vt. 1998) ("[U]ntil technology and law enforcement expertise render on-site computer records searching both possible and practical, wholesale seizures, if adequately safeguarded, must occur.").

189. *See Hill*, 459 F.3d at 974 ("As always under the Fourth Amendment, the standard is reasonableness.").

190. *See, e.g.*, United States v. D'Amico, 734 F. Supp. 2d 321, 367 (S.D.N.Y. 2010) ("[T]his is not a case where the government reviewed an exceedingly large amount of electronic files when it was only authorized to seize a very narrow category of documents.").

hypothetical, for example: Federal agents receive informant testimony that several managers at New Life LLC, including its founder, Derek Duncan, have engaged in widespread fraud and embezzlement. Because the investigators believe that Duncan may be concealing incriminating financial records at New Life's headquarters and his personal residence, they file a warrant application to search these locations for all documents, computer systems, and storage devices that might contain incriminating materials. After a magistrate judge approves this application, the agents immediately arrive at both locations to seize computers, external hard drives, filing cabinets, and any other storage systems, electronic or otherwise, which might contain evidence of fraud or embezzlement.

Unbeknownst to the investigators, Duncan's filing cabinets *and* personal computer contain a handful of photographs constituting child pornography. The critical issue is easily framed: if the agents uncover these materials during their search for financial records, will they be able to lawfully seize the photographs in plain view? The easier issue obviously involves the investigators' seizure of physical photographs stored in Duncan's filing cabinets. Assuming the agents actually discover the child pornography, any analysis will proceed under the existing framework for closed containers.[191] Because the warrant's scope likely includes any documents in Duncan's physical folders, the plain view doctrine will permit the photographs' seizure.[192]

A much more difficult question arises if the investigators do not find the "filing cabinet" photographs and instead only discover the digital evidence stored on Duncan's personal computer. Under this scenario, the government will need to rely on the plain view doctrine to lawfully seize the digital evidence because the warrant's terms implicated fraud and embezzlement, not child pornography. Moreover, because the government lacks an independent basis for probable cause—for example, by discovering the "filing cabinet" photos and seeking an additional warrant—any such finding would have to be sustained exclusively by the digital photographs. Therefore, the photographs' admissibility depends entirely on whether the government was in a lawful position to seize the child pornography. This analysis should ultimately focus on *how* the agents discovered the evidence.

Because the government probably created a bitstream copy or otherwise "froze" Duncan's hard drive,[193] a suppression court would likely consider whether the investigating agents used any search tools or forensic software to discover the child pornography.[194] If they did not use these forensic aides, their efforts would be

---

191. *See supra* text accompanying note 38 (discussing the requirements for plain view seizure).

192. *See* United States v. Kaechele, 466 F. Supp. 2d 868, 886 (E.D. Mich. 2006) ("[A]n officer searching an ordinary file cabinet for evidence of drug transactions might inadvertently come across photographs depicting child pornography." (citing United States v. Carey, 172 F.3d 1268, 1272 (10th Cir. 1999))).

193. *See supra* notes 186–87 and accompanying text.

194. Forensic examination software such as EnCase, Forensic Toolkit ("FTK"), and Helix streamline the search process for investigators. McLain, *supra* note 185, at 1094–95 & n.172. Not only can these tools search deleted files and folders, but they also allow investigators to scan and open non-active, operating system files. *Id.* at 1094.

primarily confined to a "point-and-click" type of search.[195] Files can easily be renamed or relabeled with innocuous identifiers,[196] so the investigators would likely need to open each accessible file to determine whether they were responsive to the warrant.[197] If this type of review were not permitted, a bizarre set of circumstances would arise when criminals mislabel illicit evidence as other, unrelated forms of criminal activity. For example, Duncan could label his fraudulent tax returns as "ForbiddenFruit" or "Illegal_Loli#" to possibly avoid the investigator's cursory inspection of the file. As in *United States v. Kim*, where the government was denied a warrant application to open files with these very same, falsely suggestive file names,[198] investigators would face a challenging dilemma over whether to open the files and risk losing the child pornography to suppression, or, if they refrained, lose valuable evidence relevant to their tax investigation. The computers-as-containers approach properly eliminates this Catch-22 scenario by permitting a cursory scan of files that could be implicated by the warrant's terms.[199] Therefore, as applied to the current hypothetical, the reasoning in *Williams* would permit plain view seizure if the investigators discovered the child pornography during a cursory review of the computer's file system—that is, of course, assuming the files fell within the warrant's scope.[200]

However, a "point-and-click" search method will not be useful in all criminal investigations. In a complicated search for a narrow category of documents—which inevitably includes the tax returns in the Duncan hypothetical—investigators would likely go beyond this simple procedure and utilize some type of forensic tool. Although the exact search protocol in this hypothetical would be subject to numerous factors including the nature of the informant's testimony, the computer's operating system, and the existence of file encryption,[201] analysts would likely initiate their search at a specific folder location

---

195. *See* Frasier v. State, 794 N.E.2d 449, 454–55 (Ind. Ct. App. 2003) (discussing the detective's search of a computer, which included "opening documents listed in the 'Documents' sub-menu of the . . . 'Start' menu").

196. *See supra* notes 155–57 and accompanying text (discussing the relative ease of changing file names and extensions).

197. *See Frasier*, 794 N.E.2d at 466 ("In order to find out what is contained in the file, it must necessarily be 'opened' in some way to ascertain its contents.").

198. 677 F. Supp. 2d 930, 934 (S.D. Tex. 2009).

199. United States v. Williams, 592 F.3d 511, 522–23 (4th Cir. 2010), *cert. denied*, 131 S. Ct. 595 (2010).

200. *See supra* Part III.A (discussing the role of particularity in narrowing the scope of warrants). Although David Ziff argues that the "immediately apparent" requirement of the plain view doctrine limits its application in a digital context, Ziff, *supra* note 12, at 869–70, courts have been slow to embrace this approach. Instead, many courts have upheld plain view seizure even when officers have subjected documents to intensive and prolonged review. *See, e.g.*, United States v. Khabeer, 410 F.3d 477, 482 (8th Cir. 2005) (admitting receipts in a fraud case beyond the warrant's scope); United States v. Calloway, 116 F.3d 1129, 1133 (6th Cir. 1997) (upholding the seizure of a note listing weapons, bank receipts, and power of attorney information). Moreover, these cases stand for the proposition that plain view seizure is not exclusively limited to photographs or other images. The plain view doctrine also applies to written materials such as receipts, records, and memoranda.

201. *See* Kerr, *supra* note 1, at 546–47.

or with program files relevant to the warrant.[202] For example, the search might begin at files created by tax software. Next, they could attempt to find the financial records by searching known files for "a particular word or phrase" responsive to the crimes or conduct implicated by the warrant.[203] This search query would include "flagged" or "active" files and those stored "more broadly throughout the entire hard drive."[204]

When an investigation involves complex search protocol and large quantities of data, the analysts may never even encounter the child pornography. The computers-as-containers approach offers *no guarantee* of discovery. It only offers investigators the *opportunity* to seize digital evidence. For example, many of these forensic tools can locate specific images by using hash values.[205] Agencies such as the National Drug Intelligence Center ("NDIC") have compiled the hash values for thousands of files containing child pornography, bootlegged computer applications, and other illegal materials.[206] Although these specialized values are a critical tool for discovering illicit photographs or videos, they are useless in other types of investigations. Where, as here, the investigation has no connection to child pornography or other crimes involving indecency, investigators will not be able to employ the NDIC values to bypass the warrant's terms.[207] These procedures would give law enforcement agents almost unlimited search authority under the plain view doctrine and ultimately undercut the Fourth Amendment's prohibition against unreasonable searches and seizures.[208]

Although the use of specialized hash values in this instance will not be a legitimate basis for plain view seizure, this hypothetical outlines the gamesmanship present in search-and-seizure law. If investigators use a more basic search protocol not utilizing hash values,[209] they may uncover evidence outside the warrant's terms but be unable to find evidence located in hidden or encrypted files. On the other hand, a more complex protocol will improve the depth of any computer search but may increase the likelihood of suppression. Under either scenario, however, investigators should always be prepared to seek a second warrant if they discover materials unrelated to the original warrant. This protocol limits the available scope of suppression by preventing investigators from abandoning the original search.[210]

---

202. *Id.* at 545.

203. *Id.*

204. *Id.* at 545–46.

205. *Id.* at 546. See *supra* note 77 for an explanation of how hash values are created and why they are helpful in forensic investigations.

206. Kerr, *supra* note 1, at 546.

207. *Cf.* United States v. Mann, 592 F.3d 779, 784–86 (7th Cir. 2010) (admitting evidence of child pornography specifically uncovered by an analyst's use of Forensic Toolkit when the investigation involved a search for photographs involving indecency).

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

209. *See supra* text accompanying note 195.

210. *Mann*, 592 F.3d at 786 (suppressing four images of child pornography discovered during a secondary hash-value search because the investigator knew the files contained child pornography, and he should have obtained a second warrant before actually opening them); United States v. Burgess, 576 F.3d 1078, 1094–95 (10th Cir. 2009) (noting

This hypothetical also illustrates the profound complexities of Fourth Amendment searches. Although the scope of plain view seizure is arguably broader in computer searches than under the more traditional rules for closed containers, any analysis that completely abandons the plain view doctrine is misguided. This type of approach—as embodied in Chief Judge Kozinski's concurrence in *Comprehensive Drug Testing*[211]—transforms computer hard drives into a safe harbor for any evidence of criminal activity. Users could convert illicit documents and photographs into a digital medium, and, if the warrant was unrelated to these materials, they would likely avoid any criminal liability because the government would never be in a lawful position to seize this evidence.[212] Even the most skeptical legal scholars should have reservations about completely eliminating the plain view doctrine's application to computers. This policy forces investigators to ignore clear violations of law simply because a user converted illegal materials into a digital format.

Computer technology is constantly evolving.[213] Both criminals and law enforcement agencies are using computers and data-storage systems in novel ways. By eliminating the plain view doctrine's application in computer searches, courts would be unnecessarily handicapping government search efforts. As computer technology continues to improve, less invasive search tools may become common in all jurisdictions.[214] But perhaps this technology will become so advanced that forensic software will be able to locate every piece of digital evidence in seconds, rendering even the most simple of search queries unreasonable under the Fourth Amendment.[215] It is almost impossible to predict the future of search-and-seizure technology. However, similar to the Fourth Amendment in other key contexts,[216] the precise boundaries of the plain view doctrine should continue to develop incrementally through case law.

---

that when the investigator "observed a possible criminal violation outside [the warrant's scope]," he "immediately closed the gallery view . . . and did not renew the search until he obtained a new warrant"); *accord* United States v. Giberson, 527 F.3d 882, 890 (9th Cir. 2008) (finding that suppression was not required when an officer continued to search for items within the warrant's scope).

211. 621 F.3d 1162, 1178 (9th Cir. 2010) (reh'g en banc) (Kozinski, J., concurring). For a more thorough discussion of *Comprehensive Drug Testing* and the implications of this analysis, see *supra* Part II.B.

212. In the hypothetical, for example, Duncan would avoid criminal liability by scanning any physical forms of child pornography into a digital format. Because the warrant had no connection to the photographs, the investigators would need to rely on the plain view doctrine to lawfully seize such evidence. By eliminating the doctrine in such a context, the agents would not have any lawful basis to seize the pornographic materials.

213. *See supra* Introduction.

214. For example, Professor Kerr describes the development of a "Perfect Tool." *See* Kerr, *supra* note 1, at 570. The Perfect Tool would find all relevant evidence and, at the same time, avoid any evidence beyond the warrant's scope. *Id.* Although he concludes that such a tool is "likely impossible in practice," *id.*, this commentary demonstrates the immense effect technology will continue to have on search-and-seizure law.

215. *See id.* (discussing the development of a "General Tool" to find every piece of incriminating evidence during a computer search).

216. *See supra* text accompanying notes 131–32.

CONCLUSION

Computer technology serves as a medium for the very best and worst of mankind. It helps scientists find cures for debilitating diseases and aids children in their schoolwork and language development. Soldiers deployed overseas can speak to their loved ones with the click of a button, and long lost friends can reunite through social networking websites like Facebook. At the same time, however, computers provide relative anonymity to users who transmit and download illicit materials such as child pornography. Likewise, previously unimaginable forms of criminal conduct such as identity theft and credit card fraud are becoming prevalent due to the ever-expanding use and functionality of computers.

Given the complex interplay between crime and computers, law enforcement agents will continue to seize forms of digital evidence during their investigations. Even during relatively narrow computer searches, they may discover illicit materials unrelated to the specific terms of their warrant. As this Note has established, courts have reached different conclusions about the plain view doctrine's proper application in this context. Following the Fourth Circuit's lead in *United States v. Williams*, courts should broadly apply existing search-and-seizure law to computers.

As instructed by the Supreme Court, the reasonableness of a Fourth Amendment search is determined by objective standards and not by an officer's thoughts or motivations. Moreover, ex ante warrant restrictions clash with the Court's instruction that the exact specifics of a search are generally determined by the investigating agents. Screen-and-segregate requirements ultimately create logistical difficulties by imposing protections already obtained by a particularized warrant supported by probable cause. The scope of plain view seizure, like the search itself, is dictated by the factual circumstances of an investigation. Thus, the plain view doctrine will not permit the wholesale seizure of digital evidence in every search. The holding in *Williams* embraces the development of plain view seizure through case law, not bright-line prohibitions. These rules strike a delicate balance between privacy rights, the need for effective law enforcement investigations, and the proper constitutional boundaries of a government search.