THE NEED FOR SUI GENERIS STANDARDS OF PLAIN VIEW IN COMPUTER SEARCHES; *BALCO* IN CONTEXT

Prevailing jurisprudence regarding the application of the plain view doctrine to electronic searches and seizures has allowed expansive, far reaching intrusions into personal data.[1] However, in *U.S. v. Comprehensive Drug Testing*,[2] the Ninth Circuit embraced the prevailing overly cumbersome and restrictive rules for the search and seizure of electronic evidence. In rejecting the Ninth Circuit's standard, this Note will offer an intuitive approach to the application of both the particularity requirement and plain view doctrine as applied to computer searches. First, I will explain the legal background of the plain view doctrine as applied to computer searches and seizures. Then, I will dissect and describe the import of the *BALCO*[3] deci-

1. Though beyond the scope of this note, illegal searches and seizures are just the beginning of the troubles that electronically stored information has given the courts. *See, e.g.,* Erik Harris, *Discovery of Portable Electronic Devices*, 61 ALA. L. REV. 193, 194 (2009) ("Courts, litigators, businesses, and individual parties will face fresh, unique, and especially difficult technological and legal challenges when attempting to fit the new and diverse data storage paradigms of PEDs into the 'old' framework presented by traditional approaches to electronic discovery.").

2. U.S. v. Comprehensive Drug Testing, Nos. 05-10067, 05-15006, 05-55354, 2010 WL 3529247 (9th Cir. Sept. 13, 2010) (hereinafter *BALCO V*).

3. Otherwise known as "Bay Area Laboratory Co-Operative." "In 2001, Barry Bonds hit 73 home runs for the San Francisco Giants. Also in 2001, as well as in prior and succeeding years, BALCO Laboratories, Inc. in San Francisco recorded, under the name 'Barry Bonds,' positive results of urine and blood tests for performance enhancing drugs." U.S. v. Bonds, 608 F.3d 495, 497 (9th Cir. 2009). In 2003, BALCO came under investigation for illegal steroid use when Trevor Graham turned in a syringe with a substance known as "THG" to the U.S. Anti-Doping Agency. Dick Patrick, *Graham prompted BALCO probe,* USA TODAY, Aug. 23, 2004, at 06d; *see also* David Powell, *Co-operative Under Scruti-*

sion. Next, I will interpret the potential effects of that decision on the modern problems with the plain view doctrine as applied to computer searches and seizures. Finally, I will propose a twofold paradigmatic standard that allows the police to seize incriminating items within computer data in plain view yet protects the Fourth Amendment rights of Americans in their electronic data.[4]

I. LEGAL BACKGROUND

A. Particularity, Plain View, and U.S. v. Carey*: A Special Approach*

In examining the plain view doctrine's application to computers as a whole, one must not only examine the background of that doctrine but also that of the corollary doctrine of particularity. It is a familiar maxim that warrants must "particularly describe the things to be seized [in order to make] general searches under them impossible and prevent[] the seizure of one thing under a warrant describing another."[5] Under the plain view doctrine, police can lawfully seize evidence when they are lawfully present, the evidence's incriminating character is immediately apparent, and the police have a lawful right to access the evidence.[6] The doctrine—as a useful tool for law enforcement—has allowed seizure of any contraband items within view during an arrest[7] and within view when police were otherwise lawfully

---

ny, THE TIMES, Oct. 23, 2003, at Sports 49 ("Victor Conte, president of the Bay Area Laboratory Co-Operative (BALCO), . . . is about to face a federal grand jury in San Francisco and is identified by the US Anti-Doping Agency as a supplier of THG"). A federal grand jury subpoenaed seven Major League Baseball players—among them Jeffrey Giambi and Barry Bonds—who subsequently testified before it. Elliott Almond, *MLB unsure if its 500 samples include those named in Balco probe*, San Jose Mercury News, *available at* http://web.ebscohost.com.libdata.lib.ua.edu/ ehost/ detail? vid=1 & hid=12 & sid=66b85cfd-9a0d-48f5-b936-33973ad389b0%40sessionmgr12&bdata= JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db = nfh&AN= 2W74251106299; Gary Mihoces, *Giambi calls subpoena 'no big deal,'* USA TODAY, Oct. 21, 2003 at 03c. Prompted by their testimony, the government sought their testing records in 2003 and subpoenaed Comprehensive Drug Testing, Inc., and Quest, Inc., the two organizations that had stored the data. *See* Mark Fainaru-Wada & Lance Williams, BALCO GRAND JURY SEEKS '03 SAMPLES / TESTS COULD REVEAL IF PLAYERS USED THG, S.F. Chronicle, Apr. 3, 2004, at A1. Thus began the evidentiary struggle that precipitated the *Comprehensive Drug Testing* decision. As a result, the case has regularly been referred to by the 'BALCO' acronym. *See* David Wharton, *Baseball: Most Samples Were Discarded; Vials from anonymous drug tests were thrown out before a federal subpoena was issued, official says.*, L.A. TIMES, Apr. 6, 2004, at D5 ("The federal subpoena is part of the larger BALCO case and was served on two outside contractors: Comprehensive Drug Testing of Long Beach, which administered the tests, and Quest Diagnostics of Teterboro, N.J., which analyzed the samples."); *see generally* MARK FAINARU-WADA & LANCE WILLIAMS, GAME OF SHADOWS: BARRY BONDS, BALCO, AND THE STEROIDS SCANDAL THAT ROCKED PROFESSIONAL SPORTS (2006).

4. The policy for this proposal is based on Congress' paradigmatic statement of purpose in enacting the Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2701 (2002), expressing the need for "a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies." S. Rep. 99-541, located at 1986 U.S.C.C.A.N. 3555, 3559.

5. Marron v. U.S., 275 U.S. 192, 196 (1927). *See also* U.S. v. Spilotro, 800 F.2d 959, 963 (9th Cir. 1986) (" The description must be specific enough to enable the person conducting the search reasonably to identify the thing authorized to be seized.") .

6. Horton v. California, 496 U.S. 128, 136-137 (1990).

7. *See e.g.,* U.S. v. Maple, 334 F. 3d 15, 17 (D.C. Cir. 2003), *reversed* 348 F.3d 260 (D.C. Cir.

executing a search.[8] With the advent of computers and electronic evidence, courts and commentators in the last twenty years have struggled to determine a permissible scope of the doctrine: is a computer itself covered in a warrant sufficiently akin to a "container"[9] and thus fully searchable pursuant to plain view;[10] are individual files akin to "containers" for purposes of this analysis,[11] or do the files located on storage devices constitute "intermingled documents,"[12] subject to intensive separation before search?

The Tenth Circuit examined the permissible scope of electronic seizures pursuant to plain view in *U.S. v. Carey*,[13] outlining what has become the dominant approach.[14] The defendant had given consent to be searched for drugs, and the investigators explored the directories of a seized computer, uncovering a file of child pornography. The investigators began to search exclusively for pornography, uncovering more than two hundred photos in .JPG format for which the defendant was convicted of possession of child pornography. On appeal, the Tenth Circuit held that the first file discovered was subject to plain view[15] and took hold of the intermingled documents approach of *U.S. v. Tamura*[16] as advocated by Raphael Winick:[17]

2003); U.S. v. Maple, 348 F.3d 260, 265 (D.C. Cir. 2003) (holding that drugs discoveredwhen officer, after arrest opened center console in order to place cell phone inside to secure it found them were in plain view).

8. *See e.g.,* U.S. v. Tate, 133 F. App'x 447, 448 (9th Cir. 2005) (holding that police seizure of guns during a search authorized by warrant was justified by plain view when drugs could have been found at their location and when the suspect had been convicted of firearm offenses, indicating the incriminating nature of the evidence).

9. Containers have been the subject of extensive scrutiny by the courts due to the privacy interests surrounding their nature. *See* United States v. Chadwick 433 U.S. 1, 13-14 (1977) (holding that search of a container in custody not pursuant to a search is an unreasonable search and seizure); *see also* U.S. v. Beusch, 596 F.2d 871, 876-77 (9th Cir. 1979) (establishing that search of an entire ledger is permissible under the Fourth Amendment).

10. U.S. v. Wong, 334 F.3d 831, 838 (9th Cir. 2003) (holding that evidence found in graphics files while searching for evidence under a search warrant that could reasonably be found on a computer under the terms of the search warrant was lawfully seized under the plain view doctrine).

11. Although no court has directly made the comparison, analogies do exist. *See, e.g.,* Frasier v. State, 794 N.E.2d 449, 466 (Ind. App. 2003) (comparing a computer file to a photograph in a sealed, labeled envelope).

12. U.S. v. Tamura, 694 F.2d 591, 595-96 (9th Cir. 1982) ("In the comparatively rare instances where documents are so intermingled that they cannot feasibly be sorted on site, . . . the Government and law enforcement officials generally can avoid violating fourth amendment rights by sealing and holding the documents pending approval by a magistrate of a further search").

13. U.S. v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999).

14. David J. S. Ziff, *Fourth Amendment Limitations on the Execution of Computer Searches Conducted Pursuant to a Warrant*, 105 COLUM. L. REV. 841, 846 (2005) (recognizing *Carey* as the dominant approach). *See also* U.S. v. Stierhoff, 477 F.Supp.2d 423, 443 (D.R.I. 2007) (following *Carey*), *aff'd by* U.S. v. Stierhoff, 549 F.3d 19 (1st Cir 2008), *on motion in* U.S. v. Stierhoff, 500 F.Supp.2d 55, (D.R.I. 2007), *aff'd by* U.S. v. Stierhoff, 549 F.3d 19 (1st Cir. 2008); *In re* Search of 3817 W. West End, First Floor Chicago, Illinois 60621, 321 F.Supp.2d 953, 957-60 (N.D. Ill. 2004) (utilizing principles outlined in *Carey*); U.S. v. Osorio, 66 M.J. 632, 636 (A.F. Ct. Crim. App. 2008) (finding *Carey* persuasive).

15. *Carey*, 172 F.3d at 1273 n. 4.

16. *Tamura*, 694 F.2d at 595-96.

17. *Carey*, 172 F.3d at 1275. *See* Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 105-11 (1994) (advocating *Tamura*'s approach within a computer context).

Where officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search through the documents. The magistrate should then require officers to specify in a warrant which type of files are sought.[18]

Once data was in police custody, searches could be conducted by "observing files types and titles listed on the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory."[19] The court found the investigator's conduct violated the defendant's rights; it inferred from the officer's testimony that, after opening the first file, he suspected other similarly labeled digital photo files to be of the same type.[20] To the court, this led him to search for such files past the warrant, suggesting both a lack of inadvertence and the beginnings of an unconstitutional general search.[21]

B. The Expansion of Tamura

The Ninth Circuit in *U.S. v. Hill*[22] applied *Tamura*'s approach concerning segregation and search protocols in a startlingly broad manner. The court found that a wholesale seizure of a computer for search of child pornography not accompanied by an affidavit explaining the need for off-site search did not comport with *Tamura*; nevertheless, it found that suppression of the evidence was not necessary.[23] Additionally, the court found that allowing the search of the entire computer with no protocol did not render the search warrant overbroad, both because "there is no way to know what is in a file without examining its contents, just as there is no sure way of separating talcum from cocaine except by testing it" and because of the risk of tampering, hiding, or destruction of computer files, the court found that such a result would be unreasonable.[24, 25] While most other courts to con-

18. Winick, *supra* note 18, at 105.

19. *Carey*, 172 F.3d at 1276 (10th Cir. 1999). It is not known what the court meant by "type" of file. Perhaps they referred to the file's general classification (e.g., photo, document), the file's extension (.doc, .jpg) or the category of contraband the file exhibited (child pornography).

20. *Id.* at 1273, 1276.

21. *Id.*

22. U.S. v. Hill, 459 F.3d 966 (9th Cir. 2006).

23. *Hill*, 459 F.3d at 976-977 ("'[T]he exclusionary rule does not require the suppression of evidence within the scope of a warrant simply because other items outside the scope of the warrant were unlawfully taken as well.'") (quoting *Tamura*, 694 F.2d at 597).

24. *Id.* at 978. *But see Horton*, 496 U.S. at141 ("Police with a warrant for a rifle may search only places where rifles might be and must terminate the search once the rifle is found.") (quoting Coolidge v. New Hampshire, 403 U.S. 443, 517 (1971) (White, J., concurring in part and dissenting in part). *Horton's* holding as to inadvertence is particularly relevant as evidence that this analysis is unprovoked; the *Horton* court suggested that one reason that inadvertence was not necessary for plain view was that the particularity requirement already acted to prevent general searches, namely because the requirement limits a warrant in scope of the search area. *Id.* at 139-40.

25. The court's pronouncement in this regard is without basis in precedent and seems to grind

sider the issue have taken similar action,[26] one court has indicated that search protocols are mandatory for warrants to search computers due to the particularity requirement.[27]

II. THE *U.S. V. COMPREHENSIVE DRUG TESTING* DECISIONS[28]

A. Background

In 2002, the federal government began its investigation into alleged drug use within Major League Baseball (MLB).[29] Under pressure from a motion to quash filed by the Major League Baseball Players' Association (MLBPA), the government applied for and obtained two warrants—one in the Central District of California, and the other in Nevada—to search laboratories in those respective jurisdictions.[30] The warrants authorized a broad search of all computer equipment and storage devices and allowed for seizure of the data or computer to be effected on advice of a computer analyst in the event that on site search proved too daunting.[31] On the advice of the computer analyst the government copied a directory containing baseball players' test results to search off-site.[32] An officer was then allowed to search the directory freely without segregation of the files inside.[33] Using information from this directory, the officers sought and obtained warrants for the records of all players in the directory who had tested positive for steroids.[34] On motion for return of property, the District of Nevada found that the government had callously disregarded the constitutional rights of the players and had unreasonably failed to follow *Tamura* and held against

directly against the substance of the particularity doctrine. *See* supra, note 6.

26. *See also* U.S. v. Adjani, 452 F.3d 1140, 1149-50 (9th Cir. 2006) ("To require such a pinpointed computer search, restricting the search to an email program or to specific search terms, would likely have failed to cast a sufficiently wide net to capture the evidence sought."); U.S. v. Hall, 142 F.3d 988, 996-97 (7th Cir. 1998) (sanctioning search for broad term "child pornography"); U.S. v. Henson, 848 F.2d 1374, 1383 (6th Cir. 1988) (holding broad, generic description in the warrant not overbroad); United States v. Cartier, 543 F.3d 442, 448 (8th Cir.2008) (declining to find that search methodology is necessary) *cert. denied*, Cartier v. U.S., 129 S.Ct. 1390 (2009).

27. *In re Search of 3817 W.West End,* 321 F.Supp.2d at 958-59 (N.D.Ill. 2004) (upholding prior ruling requiring search protocol prior to search considering that the government was allowed to seize the computer prior to search, the privacy interests implicated by searching computers, and the tools with which the government had access to search them).

28. For purposes of this article, these decisions will be noted as follows: U.S. v. Comprehensive Drug Testing, 473 F.3d 915 (9th Cir. 2006) (*BALCO I*) *on rehearing* U.S. v. Comprehensive Drug Testing, 513 F. 3d 1085 (9th Cir. 2008) (*BALCO II*) *reh'g en banc granted by* U.S. v. Comprehensive Drug Testing, 545 F. 3d 1106 (9th Cir. 2008) (*BALCO III*) *and on rehearing en banc* U.S. v. Comprehensive Drug Testing, 579 F. 3d 989 (9th Cir. 2009) (*BALCO IV*) *and on rehearing en banc* U.S. v. Comprehensive Drug Testing, Nos. 05-10067, 05-15006, 05-55354, 2010 WL 3529247 (9th Cir. Sept. 13, 2010) (*BALCO V*).

29. *BALCO I*, 473 F.3d at 919.

30. *BALCO V,* 2010 WL 3529247 at *1(9th Cir. Sept. 13, 2010).

31. *BALCO I,* 473 F.3d at 921.

32. *Id.* at 922-23.

33. *Id.* at 923.

34. *BALCO II*, 513 F. 3d at 1094.

the government.[35] Two other judges, one on motion for return of property and another on motion to quash subpoenas, agreed with that district, and the government appealed all three decisions.[36]

B. BALCO: The Ninth Circuit Appeals

Initially, the Ninth Circuit noted that the ex ante suggestions of *Tamura* had been complied with because the accompanying affidavits set out specific procedures to be followed and described the difficulty of sorting on site.[37] Nevertheless, the court pointed out that the government had yet to undertake a *Tamura*–compliant segregation of the documents.[38] Ultimately, the Ninth Circuit held that, upon "proper objection," a magistrate should review the files collected and segregate them, and the court remanded the underlying actions to their respective courts to facilitate that action.[39] Judge Thomas scathingly dissented, characterizing the court's activity as overruling *Tamura* because it abrogated the rule that a magistrate's approval be obtained before search and seizure.[40] He also noted that the data in question could not be said to be in plain view because of the obscure nature of its storage[41] and because the presence of positive markers on steroid tests was "sheer speculation" that any given player had actually done drugs.[42]

On its first rehearing of the case, the court once again found that *Tamura* had been complied with due to the difficulties of on-site segregation.[43] It also similarly found that the seizure of the entire directory, despite the obvious compliance of Comprehensive Drug Testing and the ease of access to more specific locations, was lawful and not overbroad.[44] Although the dissent opined that the government should have been confined to using key words in an on-site search (found to be an effective method of searching for the specific files by a representative of Comprehensive Drug Testing),[45] the majority disposed of that argument by noting that the government would

35. *Id.* at 1094-95.
36. *Id.* at 1095-96.
37. *Id.* at 1110.
38. *BALCO I*, 473 F.3d at 938
39. *Id*. at 940, 943.
40. *Id.* at 965, 974-76 (Thomas, J., dissenting). In Thomas's mind, the court's insistence on a "proper objection" to enforce the rule rendered it effectively useless because a magistrate might never see a proper objection or the evidence.
41. *Id*. at 967.
42. *Id.* at 968 ("The government also failed to sustain its burden to establish the plain view exception because, as the district courts found, the incriminating character of the information was not 'immediately apparent.'"). Judge Thomas also predicted that, under the majority's rule, magistrates unable to segregate files would allow law enforcement to hold on to them. *Id.* at 973, Minnesota v. Dickerson, 508 U.S. 366, 375 (1993).
43. *BALCO II*, 513 F. 3d at 1110.
44. *Id.* at 1110-11. ("Although the Players Association contends that the government behaved unreasonably by copying the entire . . . directory, an analysis of the difficulty of segregating intermingled electronic data reveals the opposite.")
45. *Id.* at 1120 (Thomas, J., dissenting).

have risked overlooked documents in so doing.[46] Holding that the evidence came within the warrant, the court did not reach a discussion of the plain view doctrine's applicability.[47]

On petition, the Ninth Circuit voted for an en banc rehearing.[48] The court this time deferred, agreeing with the district judges that although the government sought authority to segregate the files of the directory off-site, once the items were seized the requirement that the items be sorted and segregated was ignored.[49] The court found that two of the decisions had a preclusive effect on their review of the government's failure to segregate intermingled documents under the Nevada order.[50] Nevertheless, the court found it necessary to comment and elaborate on suggestions for the application of the plain view doctrine to the search and seizure of electronic data.[51]

In its per curiam opinion, the court expressed a general concern that the evolution of warrants in computer searches risks the same type of "general warrants" the fourth amendment was designed to guard against.[52] First, the government failed to adhere to the standards outlined within the warrant itself—utilizing a technicality within the language authorizing officials to retain anything "otherwise legally seized," the government unsuccessfully attempted to argue that the warrants authorized their behavior.[53] Further, the court remarked that the execution of the warrant failed to follow the language of the warrant or *Tamura*'s procedure—no segregation of documents took place. Instead, the case agent took immediate control of the directory and utilized them to examine all files within. After recognizing these errors and elaborating on the dual needs of law enforcement and the public at large regarding electronic seizure, the court ended by stating that it had "updated *Tamura* to apply to the daunting realities of electronic searches."[54]

In his concurrence, Judge Kozinski offered suggestions to guard against such governmental abuses. First, the government should be required to forswear reliance on the plain view doctrine, the court should deny the warrant, or, upon seizure, the court should have the evidence sorted by a neutral third party.[55] Next, Kozinski opined that the process of segregating data must be

46. *Id.* at 1112.
47. *Id.*
48. *BALCO III*, 545 F. 3d at 1106. The Ninth Circuit subsequently reviewed and re-ordered that opinion per curiam. The only practical differences between the two are 1) the placement of Chief Judge Kozinski's concurrence, and 2) the substance of Judge Bea's dissent; in the original per curiam opinion, Kozinski's suggestions were the majority opinion, and Judge Bea included suggestions for plausible rules of search and seizure. *BALCO I*, 513 F. 3d at 1000-01, 1017-18. The opinion evaluated here is their final submission.
49. BALCO V, 2010 WL 3529247 at *6-7, 2010 WL 3529247 (9th Cir. Sept. 13, 2010).
50. *Id.* at *6.
51. *Id.* at *6-7.
52. *Id.* at *11-12.
53. *Id.* at *6.
54. *Id.* at *11-14.
55. *Id.* at *14. The Court also suggested that the government disclose the actual risk of concealment and destruction of evidence to the court, but that topic has little to do with plain view and is thus beyond

designed to "achieve that purpose and that purpose only."[56] Specifically addressing the possibility of "general warrants" for electronic evidence, he suggested that the warrant should specify a protocol to prevent the government from retaining or examining any data other than that for which probable cause is shown.[57] Under this proposed segregation process, once the segregation is complete, officers would only be allowed to view the items covered by the warrant.[58]

Judge Bea filed a separate concurring-in-part and dissenting-in-part opinion in which he opined that the concurrence's guidance was unnecessary and unadvisable.[59] Judges Callahan and Ikuta dissented from the concurrence's treatment of the plain view doctrine, initially pointing out that the suggestions of that opinion do not have the force of law.[60] In particular, they disagreed with the breadth of the new proposed guidelines and their unduly restrictive nature.[61] Judge Callahan also pointed out that the proposed rules might conflict with existing law; Ninth Circuit precedent declined to give heightened protection to computer files, and the Federal Rules of Criminal Procedure specified that items seized should be more generally described and that officers could retain copies.[62] Finally, both judges commented that the opinion unnecessarily overrode Supreme Court precedent by suggesting the prudence of the elimination of the plain view doctrine in the context of the electronically stored information and pointed out that requiring segregation of these files is unsupported by legal authority and imprudent due to considerations of cost and efficiency.[63]

III. MODERN PROBLEMS WITH THE PLAIN VIEW AND PARTICULARITY DOCTRINES IN COMPUTER SEARCHES

While the *Carey* court's mere suggestions as to warrant protocol opened the door to such an expansive interpretation of particularity that accomplishes the very same goal that the *Carey* court's "special approach" sought to curb—an unconstitutional general search—the *BALCO* line of cases advocates a restrictive approach that was both unwarranted and unprecedented. First, under the standard the concurrence suggests, the government will

---

the scope of this Note. *Id.*

56. *Id.* at *15. The court suggested that tools for hashing could be used to detect specific files, such as drug testing data on only ten baseball players, but that the warrant would have to authorize such use. *Id.*

57. *Id.* If segregation was to be done by qualified personnel, the court proposed that the warrant should be explicit that those personnel and only those would segregate the data in strict confidentiality. *Id.*

58. *Id.*

59. *Id.* at *19 (Bea, J., dissenting). As stated *supra* note 48, Judge Bea himself offered substantive advice in the original en banc opinion. *BALCO IV*, 579 F. 3d at 1017-18,

60. *Id.*

61. *BALCO V*, at *19-20.

62. *Id.; see generally* Fed. R. Crim. Proc. 41.

63. *Id.* at *20, 27.

be foreclosed from using the plain view doctrine at all. It would be needlessly inconvenient for the police to be barred from seizing plainly incriminating evidence.[64] Under such a warrant, no matter how informed that the file he is perceiving is child pornography, a segregator would be proscribed from seizing contraband.[65]

The requirement of a segregation of documents is just as anomalous a result and has caused the courts numerous problems since *Tamura*. The main problem is that, even under the import of a rule suggesting the use of document segregation, courts have seldom actually required it.[66] Figure 1 adequately describes this result; governed by these decisions, the police could search the entire hard drive (represented by the boxed area). This includes the dots of 'evidence' not even tangentially related to the case. Perhaps courts have embraced this ambiguity because of the difficulty of specifically defining what the police are searching for.[67] The *Tamura* analogy suggests that a computer's files and intermingled documents are comparable;[68] while this point is facially appealing, an anomalous segregation of documents, working in tandem with the plain view doctrine, has done nothing to restrict the scope of the government's search under warrant.[69]

64. *See* Coolidge v. New Hampshire, 403 U.S. 443, 467-68 (1971) (stating that an inconvenience to police officers is a rationale for the doctrine).

65. There is no legitimate privacy right to possess contraband. Illinois v. Caballes, 543 U.S. 405, 408 (2005). This evidence, then, is just the sort that the plain view doctrine was meant to discover. *See* Payton v. New York, 445 U.S. 573, 587 (1980) ("It is also well settled that objects such as weapons or contraband found in a public place may be seized by the police without a warrant. . . . The seizure of property in plain view involves no invasion of privacy and is presumptively reasonable, assuming that there is probable cause to associate the property with criminal activity.").In the situation that the concurrence suggests, the contraband would not be subject to the terms of the warrant and thus not seizable, not even if probable cause existed. *See BALCO IV*, 579 F.3d at 1019 (Bea, J., dissenting) (stating that contraband is not returnable, creating ambiguity as to whether it should be returned or whether anyone viewing such contraband would be criminally liable); Minnesota v. Dickerson, 508 U.S. 366, 375 (1993) ("The warrantless seizure of contraband . . . is deemed justified by the realization that resort to a neutral magistrate under such circumstances would often be impracticable and would do little to promote the objectives of the Fourth Amendment.").

66. *See* U.S. v. Brooks, 427 F.3d 1246, 1251-52 (10th Cir. 2005) (warrant is not overbroad if sorting procedure not followed); U.S. v. Upham, 168 F.3d 532, 535 (1st Cir. 1999) (allowing off-premises search); U.S. v. Hay, 231 F.3d 630, 637 (9th Cir. 2000) (allowing seizure for off-site search because of time and expense); U.S. v. Welch, 291 Fed.Appx. 193, 205 (10th Cir. 2008) ("In this instance, a predetermined search protocol is not necessary."); *but see Carey*, 172 F.3d 1268, 1275-76 (10th Cir. 1999) (suggesting that computers should be brought off-site for segregation before search).

67. U.S. v. Hill, 322 F. Supp.2d 1081, 1090-91(C.D. Cal. 2004) ("There is no way to know what is in a file without examining its contents, just as there is no sure way of separating talcum from cocaine except by testing it."), *aff'd by* U.S. v. Hill, 459 F.3d 966 (9th Cir. 2006).

68. Winick, *supra* note 18, at 105.

69. *See* Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 305 (2005) (suggesting that applying plain view exception to computers under any procedure creates general warrants).

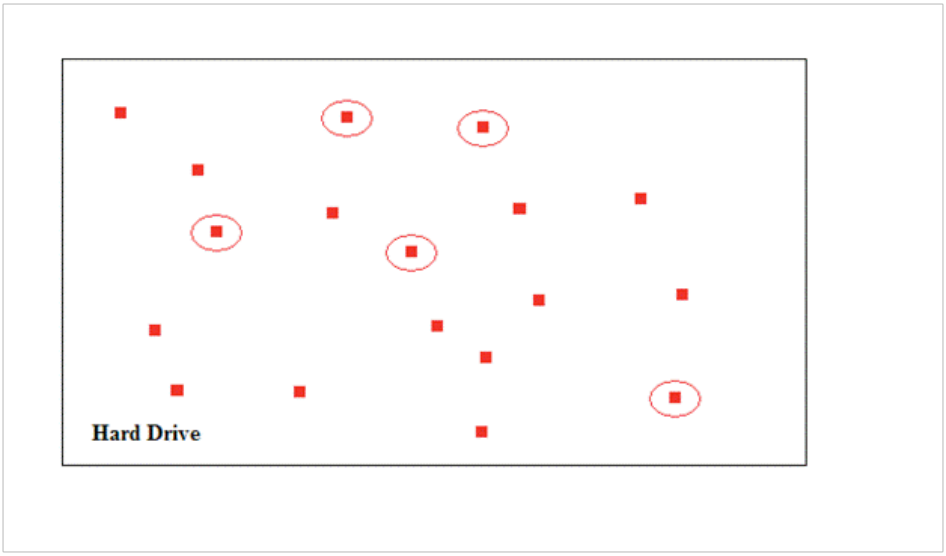

Figure 1.

The *BALCO V* court suggests not only that search protocols be followed, but also that files should be segregated off-site by neutral personnel, and that the plain view doctrine be forsworn. An accurate analogy would be to require the police to allow a neutral third party to separate items that are searchable from those that are not before searching a house. Then, they are only to search the segregated materials with a search protocol, seizing only resultant documents. Referring back to Figure 1, it would allow the police to search only the circled dots (representing segregated evidence) of the hard drive, finding relevant evidence, but losing the ability to sort through relevant evidence with common senses—even evidence that would be tangentially related to the crime. Such requirements effectively bind the police to what they list in the warrant, and if they are too imprecise or too broad in their descriptions they could lose vital evidence forever.[70]

IV. SEARCH PROTOCOLS, PLAIN VIEW, AND EX ANTE REVIEW: A NEW STANDARD

Due to its complex, all-encompassing nature, electronic evidence deserves a sui generis standard that is both sensible and has root in precedent. First, police officers should write specific search protocols designed to find files of a given type into the warrant to satisfy particularity. Next, all files found after such a search should be subject to the plain view doctrine, as

70. Of course, this argument could *foreseeably* be made for any piece of evidence, no matter the privacy interest. The rule discussed by concurrence of *BALCO V* would prohibit even contraband, in which there is no legitimate privacy expectation, from being seized when it is all but "in plain view." *See Caballes*, 543 U.S. at 408. This directly contradicts existing Supreme Court jurisprudence. *See supra* note 65.

those files would logically satisfy the traditional three-prong test for plain view. Although this standard leaves a substantial amount of ambiguity in the precise confines of the search 'area,' the courts and future legal scholarship are uniquely suited to this task. I address merely a theorization of constitutional standards; all electronically stored evidence particularly listed in terms of a search protocol in a warrant should be subject to plain view. In evaluating the basis of such a sui generis standard for electronic searches and the plain view doctrine, particularity and the plain view doctrine are discussed in turn.

A. Particularity

The ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs, and accordingly makes the particularity requirement that much more important.[71] Because of the sheer volume of private and personal data, it would be impractical to allow police to search file by file; the analogy would be to a house filled to the top with personal files and folders, some of which contain the information in the warrant.[72] Additionally, forensic software allows the police to search much more broadly; if the analogy were made, once again, to a house, processes such as file hashing allow people to search within the walls themselves.[73] This would leave little for the Fourth Amendment to protect. Jurisprudence has already produced an answer: particularity.

In the computer search context, particularity has generally been applied as specification of the types of files searched for,[74] whether referring to file extension or general description. Particularity specifies what you are searching for, so that makes sense. However, electronic searches require police to search electronic media "blind," because they do not know what is inside. Both because searches into electronics are blind and computers are so voluminous in information, the police should have guidelines to search computers without running afoul of the Fourth Amendment. Courts should write them into the warrants.

With a warrant of specific procedures for searching files and their names, types, structure, metadata, and other data relating to them the court would refine the particularity requirement and police warrants on the front

71. *See* U.S. v. Otero, 563 F3d 1127, 1132 (10th Cir. 2009) (standing for the proposition) *cert. denied*, Otero v. U.S., 130 S. Ct. 330 (2009). *See also In re Search of 3817 W. West End*, 321 F.Supp.2d at 958-60 (N.D. Ill. 2004) (holding that special nature of computers begs for requirement of search protocols); *BALCO IV*, 579 F.3d at 1019 (Bea, J., dissenting).

72. *BALCO IV*, 579 F.3d at 1019 (Bea, J., dissenting).

73. Wayne Jekot, *Computer Forensics, Search Strategies, and the Particularity Requirement*, 7 U. PITT. J. TECH. L. & POL'Y 2, 17-18 (2007) (stating that hash values, active files, deleted data, and partially overwritten files can be examined using forensic software)

74. U.S. v. Lacy, 119 F.3d 742, 746 (9th Cir. 1997) (holding warrant limited to search of documents linked to a computer bulletin board system suspected of transmitting pornography permissible); *Upham*, 168 F.3d at 535 (warrant sought picture files of sexually explicit behavior involving minors).

end, expediting the process and making it more fundamentally fair.[75] This way, in the context of a search, the police would be able to search a confined "space", which would be the search itself, without infringing on the Fourth Amendment rights.[76] Computer software available to the government is more than sufficient for this purpose,[77] largely because known data can be searched using file hashing and unknown data using file headers and metadata.[78]

B. Plain View

The plain view doctrine should allow the lawful seizure of electronically stored information "if police are lawfully in a position from which they view an object, if its incriminating character is immediately apparent, and if the officers have a lawful right of access to the object," so long as the discovery is immediately apparent as a result of using search protocols specified in the warrant.[79] Containers whose incriminating character is immediately apparent, such as metadata, a filename, or file type which tends to indicate that a file is child pornography, should be seized.[80] Not all of the search results would be subject to seizure; only those subject to plain view doctrine and those subject to the scope of the type or types of data indicated in the warrant.

75. *See In re Search of 3817 W. West End*, 321 F.Supp.2d at 957-59 (considering that a computer is a repository for enormous amounts of information, that the normal search-seizure procedure is turned on its head in searches of computers, and the probable presence of intermingled documents throughout in requiring that officers use search protocols to comport with particularity requirement); *Horton*, 496 U.S. at 138 ("[E]venhanded law enforcement is best achieved by the application of objective standards of conduct, rather than standards that depend upon the subjective state of mind of the officer."). The fairness component of such a requirement is particularly relevant in the context of computers, where often privacy interests are greater in light of the types of information and in the method within which electronic data is accessed. *See* United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001) ("Because computers can hold so much information touching on many different areas of a person's life, there is a greater potential for the 'intermingling' of documents and a consequent invasion of privacy when police execute a search for evidence on a computer.").

76. *See Tamura*, 694 F.2d at 595 (It is true that all items in a set of files may be inspected during a search, provided that sufficiently specific guidelines for identifying the documents sought are provided in the search warrant and are followed by the officers conducting the search).

77. Jekot, *supra* note 73, at 18 (stating that concerns about missed evidence because of changed file extensions or misleading file names are unfounded when using such software, because the software interrogates the data directly and looks to metadata, such as file headers, to determine file types and contents).

78. *See Id.*

79. *Dickerson*, 508 U.S. at 375.

80. Arkansas v. Sanders, 442 U.S. 753, 764 fn. 13 (1979) ("[S]ome containers (for example a kit of burglar tools or a gun case) by their very nature cannot support any reasonable expectation of privacy because their contents can be inferred from their outward appearance."). *See also* U.S. v. Walser, 275 F.3d 981, 987 (10th Cir. 2001) (finding that officer's opening of picture file named "bstfit.avi" did not make search overbroad).

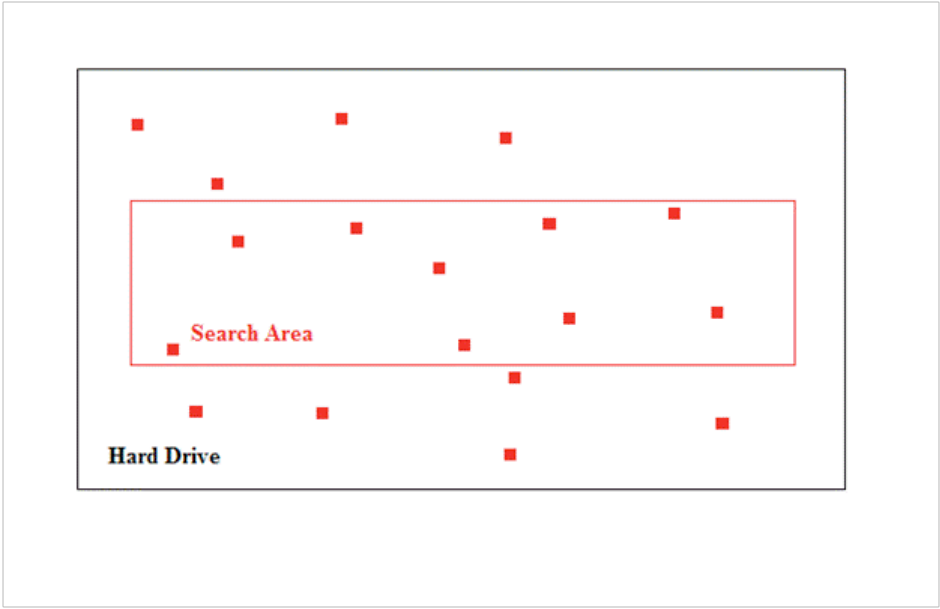

Figure 2.

Figure 2 gives a graphical representation of how this system would work. First, it would be self-regulating; the particularity doctrine would limit what could be gathered pursuant to plain view. Utilizing the analogy of a house, then, police would be able to travel through the house (or the hard drive, represented by the black-bordered rectangle) to rooms (or files which match search criteria, represented by the red dots within the red-bordered rectangle) where evidence would be likely to be found. Evidence in that room that stuck out and was apparently contraband or illegal would satisfy the plain view doctrine's three-prong test (represented by the data within the search area rectangle). In this case, the use of the term "type" could refer to file extension, file category, or category of contraband; in any search of the three aforementioned types, the police would be "lawfully present" because they will have obtained a judicial authorization for their presence, just as in the real-world case of a home. At the extreme, searching for file types may not be different from a broad search. However, any ambiguity resulting from the definition of a file type should be resolved by further identification of the files to be searched for.[81]

81. Of course, this note cannot prescribe a specific guideline for every such condition. However, it would be unnecessary and futile to do so at any rate, because the courts of this country practice the "common law method of reasoned decisionmaking, by which rules evolve from cases over time." *BALCO IV*, 579 F.3d at 1018 (Bea, J., dissenting).

V. CONCLUSION

BALCO V comes far too close to overruling established doctrine. Cases following traditional approaches, however, allow a person's entire personal repository to be searched. Courts should limit warrants to the scope of parameters of search and types of data set forth in the warrant instead of requiring officers to forswear the rule or permitting the unregulated, off-site search of entire computer systems; data found pursuant to valid procedures would then be subject to the plain view doctrine. This approach both acknowledges the need of law enforcement of a vital tool of evidentiary discovery and of the courts to safeguard fundamental rights to privacy.

Alexander E. Vaughn[*]

* J.D./M.B.A Candidate, Class of 2012, University of Alabama School of Law. B.S. (Criminal Justice, 2008), Troy University. I would like to thank Professor Bryan Fair for creative direction, Karthik Subramanian for all of his assistance, and Bobby, Deanne, and Elizabeth Vaughn for their inspiration and heartfelt confidence.