Brigham Young University Journal of Public Law

Volume 24 | Issue 2 Article 7

3-1-2010

Flexing Judicial Muscles: Did the Ninth Circuit Abandon Judicial Restraint in *United States v. Comprehensive Druge Testing, Inc.*?

Allen H. Quist

Flexing Judicial Muscles: Did the Ninth Circuit Abandon Judicial Restraint in *United States v. Comprehensive Drug Testing, Inc.*?

"Caution is the eldest child of wisdom."
Victor Hugo[1]

I. INTRODUCTION

As we march into the information age, some scholars fear that Fourth Amendment jurisprudence has lagged behind.[2] This fear is particularly prevalent in the realm of computer searches and seizures. Computers, some argue, are different from desks, closets, and other containers because their storage capacity is virtually unlimited.[3] Moreover, modern computers perform a variety of functions, including "postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more."[4] Due to a computer's unique capacity and its many functions, civil libertarians argue that such electronic devices deserve special Fourth Amendment protections. While these arguments are common in academic circles,[5] they rarely find their way into actual court decisions.[6] The notable exception is the Ninth Circuit's recent en banc decision in *United States v. Comprehensive Drug Testing, Inc.*[7]

In *Comprehensive Drug Testing*, the Ninth Circuit engaged in judicial trailblazing by promulgating a set of five "guidelines" that

1. Victor Hugo, Famous Quotes & Authors, http://www.famousquotesandauthors.com/topics/caution_quotes.html (last visited Feb. 3, 2010). This maxim captures the spirit of the common law tradition that legal rules should evolve slowly over time. As this case note will demonstrate, the Ninth Circuit abandoned caution in favor of brash judicial action in *Comprehensive Drug Testing*.

2. Marc Jonathan Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1363 (2004); Morgan Cloud, *Rube Goldberg Meets the Constitution: The Supreme Court, Technology and the Fourth Amendment*, 72 MISS. L. J. 5, 49 (2002).

3. Posting of *Computer Searches and Plain View* to UNC School of Government Blog, http://sogweb.sog.unc.edu/blogs/ncclaw/?p=715 (last visited Nov. 14, 2009) ("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.").

4. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 569 (2005).

5. *Id.*

6. *See, e.g.*, United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999).

7. 579 F.3d 989 (9th Cir. 2009) (en banc).

govern the issuing of search warrants and subpoenas for electronically stored information. These guidelines, which amount to bright-line rules, are overly broad and reach far beyond the confines of any case or controversy.[8] While the court's desire to provide magistrates with clear guidance is laudable, it is ultimately misguided. The rules established by the court place too heavy a burden on investigating agencies and overlook past precedent. Moreover, assuming that the rules are workable, the computer forensics field is rapidly changing, and, as a result, the court's decision will quickly become outdated.[9]

This Note begins by providing background information on how courts have applied the Fourth Amendment to electronic searches. Part III provides a summary of the facts and reasoning in *Comprehensive Drug Testing*. Part IV contains an analysis of the plain view doctrine and highlights some of the problems with the court's decision. This section is subdivided into four subsections. Subsection A argues that the plain view doctrine should not be abandoned in electronic searches. Subsection B demonstrates how the court's decision is burdensome, premature, and overly broad. Subsection C addresses how the court could have reached the same result without promulgating the guidelines. Subsection D outlines my predictions for the future implications of *Comprehensive Drug Testing*. Finally, Part V provides a brief summary of the analysis contained in part IV.

II. BACKGROUND

A. Searching Among Intermingled Documents

Courts have struggled to limit computer searches in ways that effectively balance privacy and law enforcement interests. This is because computers often contain information that has nothing to do with a particular investigation. Consequently, courts must find ways to "separate the wheat from the chaff"[10] without violating the Fourth Amendment's prohibition on general searches.[11] For electronic devices,

8. *Id.* at 1012 (Callahan, J., concurring).

9. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805 (2004) ("When technology is in flux, Fourth Amendment protections should remain relatively modest until the technology stabilizes.").

10. Derek Regensburger, *Bytes, Balco, and Barry Bonds: An Exploration of the Law Concerning the Search and Seizure of Computer Files and an Analysis of the Ninth Circuit's Decision in* United States v. Comprehensive Drug Testing, Inc., 97 J. CRIM. L. & CRIMINOLOGY 1151, 1204 (2007).

11. The Warrant Clause of the Fourth Amendment categorically prohibits the issuance of any warrant except one 'particularly describing the place to be searched and the persons or things to be seized.' The manifest purpose of this particularity requirement was to prevent general searches. By limiting the authorization to search to the specific

this sifting process is difficult because information on computers can easily be concealed or mislabeled with incorrect file names or extensions.[12] For example, an individual wishing to conceal a file might label it "pesto.recipe in lieu of blackmail.photos."[13] Thus, ex ante restrictions that limit computer searches to certain keywords or file types may cripple an investigator's ability to uncover evidence that is within the scope of an investigation.[14] To address problems of intermingled electronic records, courts have analogized to cases involving non-electronic records.

For instance, in *United States v. Beusch*, the defendants in a bank fraud case objected to the government's seizure of two ledgers and a file.[15] Defendants argued that the relevant portions of the documents were easily identifiable and separable, and that the government's seizure was impermissible because it swept up information outside the warrant.[16] Rejecting this argument, the court concluded that "[t]he fact that an item seized happens to contain other incriminating information not covered by the terms of the warrant does not compel its suppression, either in whole or in part."[17] The court reasoned that although individual files and ledgers are "theoretically separable, [they] in fact constitute one volume or file folder."[18] However, the court provided a caveat, noting that the seizures of *sets* of ledgers or files may not be permissible.[19]

The distinction between a single ledger and a set of ledgers became important in *United States v. Tamura*.[20] In *Tamura*, government agents investigating a kickback scheme secured a warrant to search and seize specific records from a company's accounting department.[21] In the course of the search, the agents realized that finding the appropriate documents would be time-consuming.[22] As a result, the agents decided to

---

> areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.

Maryland v. Garrison, 480 U.S 79, 84 (1987).

12. *Comprehensive Drug Testing*, 579 F.3d at 995 (noting that in addition to containing mislabeled files, a computer might have "booby traps that 'destroy or alter data if certain procedures are not scrupulously followed' . . . or data might be encrypted or compressed, requiring passwords, keycards or other external devices to retrieve.") (citing Warrant Affidavit at 3).

13. *Id.* at 995.

14. Kerr, *supra* note 4, at 571–72; *see also* United States v. Hill, 322 F. Supp. 2d 1081, 1090–91 (C.D. Cal. 2004).

15. United States v. Beusch, 596 F.2d 871, 876 (9th Cir. 1979).

16. *Id.* at 877.

17. *Id.*

18. *Id.*

19. *Id.*

20. 694 F.2d 591 (9th Cir. 1982).

21. *Id.* at 594.

22. *Id.* at 595.

seize numerous cardboard boxes and file drawers full of information so that they could conduct the search in another location.[23] The court held that this seizure was unacceptable.[24] In dicta, the court suggested two ways that the government could avoid violating the Fourth Amendment when documents are too intermingled to separate on site: (1) the government can seal and hold the documents until the issuing magistrate provides further authorization, or (2) if law enforcement officials know that the documents will be intermingled, they can apply for special authorization to remove the files *before* executing the search.[25]

In subsequent cases, both the Ninth and Tenth Circuits have made it clear that warrants containing prior approval for off-site review of intermingled documents satisfy the Fourth Amendment. In *United States v. Hay*,[26] the Ninth Circuit found that the search and seizure affidavit had sufficiently established the need to remove the defendant's entire computer system.[27] Specifically, the affidavit "justified taking the entire system off site because of the time, expertise, and controlled environment required for a proper analysis. This, together with the magistrate judge's authorization to do so, [made] inapposite *United States v. Tamura*."[28] Similarly, in *United States v. Brooks*,[29] the court upheld a warrant authorizing the off-site search of computer equipment.[30]

In addition to granting prior approval for off-site review, magistrates guide the discovery of newly uncovered evidence. In *United States v. Carey*,[31] officers seized a computer they suspected contained evidence of drug transactions.[32] The warrant permitted the officers to search for "names, telephone numbers, ledger receipts, addresses, and other

23. *Id.*

24. *Id.* at 597.

25. *Id.* at 595–96. Not all courts have applied *Tamura's* approach to the electronic records context. *See, e.g.*, United States v. Comprehensive Drug Testing, Inc., 513 F.3d 1085, 1107 (9th Cir. 2005). ("One district court in Michigan explained: 'The Court declines to follow *Tamura*, at least in this case, because *Tamura* did not involve computer files and therefore did not consider the specific problems associated with conducting a search for computerized records.' United States v. Scott-Emuakpor, 2000 U.S. Dist. Lexis 31118, 2000 WL 288443, at *8 (W.D. Mich). Although declining to apply *Tamura's* pragmatic approach to computer searches, Judge Quist stated: 'This is not to suggest that seizure of all computer disks is permissible whenever the warrant authorizes the seizure of computer records.' *Id.* Another court, also referencing *Tamura*, noted that in the modern computer context a 'suggestion by a panel of the Ninth Circuit in a 20-plus year old case is not persuasive.' United States v. Kaufman, 2005 U.S. Dist. Lexis 21006, at *12, 2005 WL 2304345, at *4 n.3 (D. Kan).").

26. 231 F.3d 630 (9th Cir. 2000).

27. *Id.* at 637.

28. *Id.*

29. 427 F.3d 1246 (10th Cir. 2005).

30. *Id.* at 1251.

31. 172 F.3d 1268 (10th Cir. 1999).

32. *Id.* at 1270.

documentary evidence pertaining to the sale and distribution of controlled substances."[33] As a technician was searching the computer, he opened a "JPG"[34] file containing child pornography.[35] The technician testified that he opened the image file because he believed it might contain photographs related to drug activity.[36] After opening the image, the technician downloaded over 244 image files, which he believed contained pornographic material.[37] The court concluded that the technician's search of all but the first image exceeded the scope of the warrant.[38] Upon discovering the first image, he should have gone to a magistrate to obtain a new warrant allowing him to search for child pornography.[39] Like in *Tamura*, the court in *Carey* noted that "officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search through the documents."[40]

Thus, a general understanding of the law as illustrated above is that in order to perform an off-site search of intermingled documents, the warrant must grant permission for such an off-site search; furthermore, if a search of electronic documents uncovers criminal activity outside the scope of the warrant, the search must be stopped until an additional warrant is obtained. This consensus conforms with United States Supreme Court precedent. In *Andresen v. Maryland*,[41] the defendant unsuccessfully challenged the seizure of business records.[42] Giving deference to magistrate judges, the Court noted that "responsible officials, including judicial officials, must take care to assure that [searches of intermingled documents] are conducted in a manner that minimizes unwarranted intrusions upon privacy."[43] Moreover, the Court found that when searching intermingled documents, "it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized."[44] If a cursory examination reveals criminal activity outside

33. *Id.*

34. A "JPG" file extension is attached to files containing photographs and other images. However, it is possible to hide text within "JPG" files. The technician conducting the search testified that he had never "experienced an occasion in which the label 'JPG' was used by drug dealers to disguise text files." *Id.* at 1270 n.2.

35. *Id.* at 1271.

36. *Id.*

37. *Id.*

38. *Id.* at 1273.

39. *Id.* at 1275–76.

40. *Id.* at 1275.

41. 427 U.S. 463 (1976).

42. *Id.*

43. *Id.* at 482.

44. *Id*.

the scope of the warrant, the question then becomes whether the plain view doctrine, an exception to the warrant requirement, applies.

B. The Plain View Doctrine

Contrary to the court's decision in *Comprehensive Drug Testing*, cases in both the Ninth and Tenth circuits have extended the plain view doctrine to electronic searches. The plain view doctrine allows officers to seize incriminating evidence found during an otherwise lawful search. Under the doctrine, an officer may seize incriminating evidence without a warrant if three conditions are met: "(1) the officer was lawfully in a position from which to view the object seized in plain view; (2) the object's incriminating character was immediately apparent . . . and (3) the officer had a lawful right to access the object itself."[45]

In most circuits, the contours of the plain view doctrine as it applies to electronic searches are unclear. For example, in *Carey*, the Tenth Circuit pointed out that "the question of what constitutes 'plain view' in the context of computer files is intriguing and appears to be an issue of first impression for this court, and many others."[46] Although the *Carey* court claimed to avoid the plain view question,[47] its holding seems to suggest a return to the inadvertence requirement abandoned in *Horton*.[48] As discussed above, in *Carey*, the court found that a computer technician violated the Fourth Amendment when he abandoned his drug-trafficking search upon discovering evidence of child pornography. The court, however, indicated that since the *first* pornographic image was *inadvertently* discovered, its seizure may have been permissible.[49] Later Tenth Circuit decisions have narrowly interpreted *Carey*. For example, in *United States v. Grimmett*,[50] the court noted that *Carey* "simply stands for the proposition that law enforcement may not expand the scope of a search beyond its original justification."[51] The Ninth Circuit has taken a similar approach.

---

45. United States v. Soussi, 29 F.3d 565, 570 (10th Cir. 1994) (citing Horton v. California, 496 U.S. 136–37 (1990)). Before *Horton v. California*, a fourth condition focused on the officer's subjective intent by requiring that discovery of the evidence be inadvertent. However, in *Horton*, the Court abandoned this requirement. *See* Kerr, *supra* note 4, at 577–78 (suggesting that bringing back the inadvertence requirement in the electronic context may provide an effective means of limiting computer searches).

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

47. *Id.*

48. David J. S. Ziff, *Fourth Amendment Limitations on the Execution of Computer Searches Conducted Pursuant to a Warrant*, 105 COLUM. L. REV. 841, 865–66 (2005).

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

50. 439 F.3d 1263 (10th Cir. 2006).

51. *Id.* at 1268.

In *United States v. Wong*,[52] police obtained a warrant to search a defendant's computer for evidence relating to a murder.[53] The warrant authorized officers to search computer files containing maps of where the victim's body was found, information relating to nine-millimeter firearms, and images of items found near the body.[54] A forensic expert determined that the information in the warrant could be stored in plain text, special text, or graphics files.[55] While searching through graphic files, the technician discovered child pornography.[56] After noting the location of the files, he continued to search for evidence related to the murder.[57] Investigators later used the technician's discovery to obtain another warrant to search the defendant's business computer for evidence of child pornography.[58]

Applying the plain view doctrine, the court found that the child pornography files were properly admitted.[59] First, the technician was lawfully searching the computer when he found the incriminating images.[60] Second, the incriminating nature of the files was immediately apparent.[61] Third, the officer had a right to open graphic files pursuant to a valid search warrant.[62] Moreover, the technician complied with the *Carey* inadvertence requirement because he did not abandon his original search after discovering the illegal images.[63]

In addition to the reasoning in *Wong*, the court's analysis in *United States v. Adjani*[64] supports the applicability of the plain view doctrine to electronic searches. In *Adjani*, investigators were looking for evidence of extortion on a co-defendant's computer.[65] At the time of the search, the co-defendant was not a suspect; however, this changed after investigators discovered emails implicating her in the extortion conspiracy.[66] Over the protests of the co-defendant, the court admitted the emails, concluding that "[t]here is no rule . . . that evidence turned up while officers are rightfully searching a location under a properly issued warrant must be

52. 334 F.3d 831 (9th Cir. 2003).

53. *Id.* at 833

54. *Id.* at 834. The search warrant included images of monopoly money and references to "NWO" or "ZOG" because investigators found these items near the victim's body. *Id.*

55. *Id.*

56. *Id.* at 835.

57. *Id.*

58. *Id.*

59. *Id*. at 838.

60. *Id*.

61. *Id*.

62. *Id*.

63. *Id.*; United States v. Carey, 172 F.3d 1268, 1273 (10th Cir. 1999).

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

65. *Id.* at 1142.

66. *Id.*

excluded simply because the evidence found may support charges for a related crime (or against a suspect) not expressly contemplated in the warrant."[67]

While several cases have applied the plain view doctrine to computers, some legal scholars have argued that the doctrine should not apply, or should at least be limited, in the computer context.[68] These arguments are based on the notion that computers are unique and deserve special Fourth Amendment protections. The idea that computers are somehow different than other seizeable property was criticized by the Ninth Circuit in *United States v. Giberson*.[69]

In *Giberson*, officers executing a search warrant secured a computer that was surrounded by suspicious printouts relating to the production of fake IDs.[70] After securing a second warrant authorizing the search of the computer, a technician discovered images of child pornography.[71] This discovery did not alter the technician's search pattern: he continued to search for images related to the production of fake IDs, and at no time did he specifically search for child pornography.[72] The defendant argued that electronic devices are entitled to enhanced protection and that "the analogy between a computer and other 'containers' is not appropriate."[73]

The court rejected the defendant's special-protections argument, finding that neither record format nor storage capacity is relevant in the Fourth Amendment context.[74] According to the court, distinctions based

---

67. *Id.* at 1151.

68. Kerr, *supra* note 4, at 582–84.

69. 527 F.3d 882, 888–89 (9th Cir. 2008). *Giberson* is an important case because it was recently decided and is cited in *Comprehensive Drug Testing* four separate times. *See* Comprehensive Drug Testing, Inc., 579 F.3d 989, 1006, 1010–11, 1013 (9th Cir. 2009) (en banc).

70. *Giberson*, 527 F.3d at 885. Officers found social security cards and birth certificates next to the computer. *Id.*

71. *Id.*

72. *Id.*

73. *Id.* at 887.

74. *Id.* at 888. Scholar Thomas K. Clancy also rejected "the notion that there should be special rules for electronic evidence containers. Otherwise, in his 193, 211 (2005)).

74. *Giberson*, 527 F.3d at 888.

74. United States v. Gomez-Soto, 723 F.2d 649, 652, 654–55 (9th Cir. 1984).

74. *Giberson*, 527 F.3d at 888.

74. *Id.*

74. *Id.*

74. *Id.*

74. *Id.*

74. Regensburger, *supra* note 10, at 1166.

74. *Id.*

74. *Id.*

74. 42 U.S.C. § 2000aa (2009).

74. 28 C.F.R. § 59.4 (2009).

on record format are arbitrary and run contrary to prior precedent.[75] Previously, the Ninth Circuit had held that while microcassettes may store information differently than traditional paper, they still constitute seizable "records."[76] Similarly, the court concluded that distinctions based on storage capacity are arbitrary and raise more questions than they answer.[77] For example, why should officers "be permitted to search a room full of filing cabinets" but not a computer?[78] Would a special protections scheme reach external devices like flash drives that hold less information than a computer?[79] The court avoided bright-line rules based exclusively on the type of device being searched (i.e., the container).[80] Instead, the court anchored its analysis in a reasonableness inquiry.[81] While differences in record format and storage capacity are insignificant, the *location* of files at issue may be relevant.

C. Searches of Confidential Business Records

Professor Derek Regensburger argues that "[t]he search of business computers may require different rules . . . because such searches implicate unique concerns."[82] Unlike personal computers, business computers may contain thousands of records of individuals outside the scope of the investigation.[83] "This is particularly true of searches of innocent third parties, such as medical or law offices, which are merely the repositories for the records relevant to the investigation."[84]

In response to these concerns and pursuant to the Privacy Protection Act of 1980,[85] the Department of Justice promulgated a set of guidelines to govern the obtaining of documentary materials held by third parties.[86] According to the guidelines, no federal officer should apply for a warrant to search "a disinterested third party" unless the use of "less intrusive alternative means of obtaining the materials would substantially

74. *Id.*view, filing cabinets, diaries, books, floppy drives, hard drives, paper bags, and other storage devices would 'all require different rules.'" Regensburger, *supra* note 10, at 1162–63 (quoting Thomas K. Clancy, *The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L .J. 193, 211 (2005)).

75. *Giberson*, 527 F.3d at 888.

76. United States v. Gomez-Soto, 723 F.2d 649, 652, 654–55 (9th Cir. 1984).

77. *Giberson*, 527 F.3d at 888.

78. *Id.*

79. *Id.*

80. *Id.*

81. *Id.*

82. Regensburger, *supra* note 10, at 1166.

83. *Id.*

84. *Id.*

85. 42 U.S.C. § 2000aa (2009).

86. 28 C.F.R. § 59.4 (2009).

jeopardize the availability or usefulness of the materials sought."[87] The guidelines define a disinterested third party as a person or group "not reasonably believed to be . . . a suspect" in the offense to which the materials relate.[88] If a search of a disinterested third party is conducted, it should be done "in such a manner as to minimize, to the greatest extent practicable, scrutiny of confidential materials."[89]

According to Professor Regensburger, "few cases have explored the limitations these regulations impose on searches of medical or law offices."[90] The cases that do exist suggest that the government cannot act as though the regulations are "nonexistent"[91] but may satisfy them if a warrant specifies certain documents and requires the prosecution to seek further guidance from the court before inspecting files.[92] However, the regulations lack efficacy, as "failure to comply with [them] is not an issue which may be litigated or form the basis for the suppression or exclusion of evidence."[93]

III. *UNITED STATES V. COMPREHENSIVE DRUG TESTING*

A. Factual Background

Comprehensive Drug Testing involved the government's investigation into illegal steroid use among major league baseball players.[94] The investigation centered on the Bay Area Lab Cooperative ("Balco"), which the government suspected of providing illegal steroids to athletes.[95] While investigating Balco, the government learned that several players had tested positive under a confidential testing program designed to determine the prevalence of steroid use in professional baseball.[96] A third-party, Comprehensive Drug Testing, Inc. ("CDT"), administered the program.[97] Another company, Quest Diagnostics, Inc. ("Quest"), performed the actual tests and maintained the urine samples.[98] Neither CDT nor Quest were suspected of wrongdoing.

87. *Id*.
88. *Id.* § 59.2(b)-(b)(1).
89. *Id.* § 59.4(b)(4).
90. Regensburger, *supra* note 10, at 1168.
91. Klitzman v. Krut, 744 F.2d 955, 962 (3d Cir. 1984).
92. *In re* Impounded Case, No. 875190, 840 F.2d 196, 201 (3d Cir. 1988).
93. Regensburger, *supra* note 10, at 1168.
94. Comprehensive Drug Testing, Inc., 579 F.3d 989 (9th Cir. 2009) (en banc). The facts surrounding *Comprehensive Drug Testing* are complex; consequently, this discussion will focus on information that relates directly to this Note.
95. *Id.* at 993.
96. *Id.*
97. *Id.*
98. *Id*.

The government sought to seize information from CDT and Quest by employing subpoenas and warrants in three different jurisdictions. In the Northern District of California, the government obtained a subpoena seeking all of CDT's "drug testing records and specimens" relating to Major League Baseball.[99] In the District of Nevada, the government obtained a warrant for urine specimens stored at Quest's Las Vegas laboratory.[100] In the Central District of California, investigators secured a warrant authorizing a search of CDT's facilities for evidence pertaining to ten specific players.[101]

During the government's search of CDT's facilities, it located a computer directory labeled "Tracey" that appeared to contain all of the files for the company's sports testing programs.[102] Investigators made a copy of the entire directory for off-site review. Because the directory "contained numerous subdirectories and hundreds of files,"[103] its removal was permissible under the warrant.[104] During off-site analysis, a case agent searched for "information pertaining to *all* professional baseball players and used it to generate additional warrants and subpoenas to advance the investigation."[105] Investigators found incriminating information in a Microsoft Excel spreadsheet that contained drug test results.[106] The names of the ten players mentioned in the warrant issued in the Central District of California were interspersed with the names of other players. To see the test results, the agent had to scroll to the right until he reached the results column of the spreadsheet.[107]

Following the seizure, CDT and the Major League Baseball Players Association moved for return of the property pursuant to Federal Rule of Criminal Procedure 41(g).[108] They argued that the government had failed to follow *Tamura* and had used the fruits of an illegal search to expand their investigation beyond the ten players previously identified.[109] The

---

99. *Id.*

100. *Id.*

101. *Id.*

102. *Id.* at 996.

103. Comprehensive Drug Testing, Inc., 513 F.3d 1085, 1092–93 (9th Cir. 2008).

104. The warrant provided that

> [i]f the computer equipment and storage devices cannot be searched on-site in a reasonable amount of time, then the computer personnel will determine whether it is practical to copy the data during the execution of the search in a reasonable amount of time without jeopardizing the ability to preserve the data.

Id. at 1093.

105. *Comprehensive Drug Testing*, 579 F.3d at 999.

106. *Id.* at 1016 (Bea, J., concurring in part and dissenting in part).

107. *Id.*

108. *Id.* at 993 (majority opinion).

109. *Comprehensive Drug Testing*, 513 F.3d at 1105.

Central District of California "found that the government had failed to comply with the procedures specified in the warrant and, on that basis and others, ordered the property returned."[110] Similarly, the District of Nevada required the government to return property seized from Quest, and the Northern District of California quashed the government's subpoenas.[111] *Comprehensive Drug Testing* is the consolidated appeal in which the government challenged these district court decisions.

B. The Panel Decision

1. Opinion

The three-judge panel upheld the seizure of intermingled documents, concluding that the government did not demonstrate callous disregard in conducting its search.[112] In so holding, the panel reversed the decisions made by the lower courts.

According to the panel, the government acted in accordance with *Tamura* when it "obtained advance authorization to seize intermingled documents based upon a search warrant protocol that had been carefully outlined and supported."[113] The search protocol permitted the files to be removed upon a computer specialist's determination that the records could not easily be separated on-site.[114] Agent Abboud, a computer analyst, made this determination when he decided that "on-site review would not be feasible in a reasonable amount of time."[115]

In addition to following *Tamura*, the government conducted its search of CDT and Quest in a reasonable manner. Instead of seizing the whole computer, the government made a copy of the Tracey directory, which enabled CDT to continue its regular business operations.[116] Moreover, seizing the entire Tracey directory was reasonable because

---

110. *Comprehensive Drug Testing*, 579 F.3d at 993–94.

111. *Comprehensive Drug Testing*, 513 F.3d at 1090.

112. *Id.* at 1103.

113. *Id.* at 1110.

114. *Id.* The warrant provided that

> [u]pon searching the premises, law enforcement personnel trained in searching and seizing computer data (the 'computer personnel') will make an initial review of any computer equipment and storage devices to determine whether these items can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve data. . . . If the computer personnel determine that it is not practical to perform an on-site search or make an onsite copy of the data within a reasonable amount of time, then the computer equipment and storage devices will be seized and transported to an appropriate law enforcement laboratory for review.

Id.

115. *Id.*

116. *Id.*

electronically stored information is often unusable if embedded information surrounding the file is missing.[117] Thus, by seizing the entire directory, the government was ensuring that it could recover information specified in the search warrants.

Interestingly, the court did not reach the government's plain view argument. According to the panel, the plain view doctrine is inapplicable "because the evidence fell within the scope of the search warrant."[118] Thus, the court concluded the seizure was justified and the information seized provided a legitimate basis for expanded warrants.[119]

Finally, the court overturned the district court's ruling on the 41(g) order, noting that evidence need not be returned so long as the government "needs it and its conduct in acquiring the evidence was not 'sufficiently reprehensible.'"[120]

2. Dissent

In his dissent, Judge Thomas argued that the majority invented a new and unwarranted justification for approving seizures.[121] According to Judge Thomas, the majority held that "boilerplate terms of a computer search warrant justify both the seizure of massive amounts of confidential medical information about persons not suspected of any criminal activity *and* the subsequent warrantless search of the information."[122] Thomas further argued that this justification for approving searches and seizures should be abandoned because it would "allow the government unprecedented easy access to confidential medical and other private information about citizens who are under no suspicion of having been involved in criminal activity."[123]

---

117. *Id.* at 1110–11. According to the Federal Judicial Center:

> [S]ome computer-based transactions do not result in a conventional document, but instead are represented in integrated databases. Even less-complex ESI [electronically stored information] may be incomprehensible and unusable when separated from the system that created it. For example, a spreadsheet produced in portable document format (PDF) may be useless because embedded information, such as computational formulas, cannot be seen or discerned. Finally, deleting an electronic document does not get rid of it, as shredding a paper document would.

Id.

118. *Id.* at 1112.

119. *Id.*

120. Aaron Seiji Lowenstein, *Search and Seizure on Steroids:* United States v. Comprehensive Drug Testing *and Its Consequences for Private Information Stored on Commercial Electronic Databases* (May 2007), http://works.bepress.com/cgi/viewcontent.cgi?article=1000&context=aaron_lowenstein.

121. *Comprehensive Drug Testing*, 513 F.3d at 1117 (Thomas, J., concurring in part and dissenting in part).

122. *Id.*

123. *Id.* Moreover,

In addition to inventing a new justification for seizures, Judge Thomas argued that the court improperly ignored the government's plain view argument.[124] Judge Thomas addressed this argument and rejected it, claiming that the government failed to provide any reason why the plain view doctrine should apply to computers.[125] He further noted that "every district judge involved in this case"[126] had rejected the government's plain view doctrine.[127]

As an alternative to the majority's approach, Judge Thomas proposed that magistrates "examine the co-mingled data that the government proposes to seize to make sure that private information that the government is not authorized to see remains private."[128] This approach appears to have influenced the en banc decision that followed because, like the en banc decision, it focused on increasing the responsibilities of magistrates in cases involving intermingled data.

> [a]t a time our medical institutions are working diligently to provide physicians with easy nationwide electronic access to patient records in order to improve the care and treatment of our citizens, the [majority] opinion poses a very serious threat to the confidentiality of patient records and ultimately to the effective delivery of health care itself.

Id.

124. *Id.*

125. *Id.* at 1124.

126. *Id.* at 1117.

127. Judge Illston of the Northern District of California made the following statement:

> I find absolutely staggering the implications about what you say about the plain view doctrine in the computer set up. In a way nothing is plain view because with the disk you look at it, you don't see anything until you stick it in the computer and it does take quite a lot of work really to bring it up on the screen. So, it's not in plain view in the sense of walking into the room and seeing the scale on the desk. It takes a whole lot of work to get there. First off, none of it is cursory, there are whole industries that have developed in order to make it possible for the disk to show up on the screen that way. So it's not cursory review. I don't think it's plain view. I don't think I have to go that far or make that kind of choice with respect to issues that are certainly going to arise. . . . Where it requires sorting through information which really is on a data base, somehow it's being organized in different formats, you could organize it in a format based on the ten names, instead of taking it in other kinds of formats, then scrolling across and taking names and information off the screen, when it's clearly information that isn't part of what was originally within the authorized search warrant, I just think is impermissible.

Id. at 1124.

128. United States v. Comprehensive Drug Testing, Inc., 473 F.3d 915, 964–65 (9th Cir. 2006) (Thomas, J., concurring in part and dissenting in part) (withdrawn and superseded by 513 F.3d 1085 (9th Cir. 2008).

C. The En Banc Decision

1. The majority opinion

On rehearing en banc, the court found that the district courts had acted appropriately by requiring the government to return copies of the seized evidence.[129] In reaching this conclusion, the court promulgated five new guidelines:

> (1) Magistrates should insist that the government waive reliance upon the plain view doctrine in digital evidence cases.
> (2) Segregation and redaction must be either done by specialized personnel or an independent third party. If the segregation is to be done by government computer personnel, [the government] must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant.
> (3) Warrants and subpoenas must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other judicial fora.
> (4) The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents.
> (5) The government must destroy or, if the recipient may lawfully possess it, return non-responsive data, keeping the issuing magistrate informed about when it has done so and what it has kept.[130]

First, the court found that the plain view doctrine should not apply to computers. If the government cannot be sure where the information is stored on the computer, it may search the entire computer. Thus, when files are intermingled (which is always the case in electronic searches) the plain view doctrine turns "a limited search for particular information into a general search of office file systems and computer databases."[131] According to the court, such a search would "make a mockery of *Tamura* and render the carefully crafted safeguards in the Central District warrant a nullity."[132] Thus, the court concluded that the plain view doctrine could

129. United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1006 (9th Cir. 2009) (en banc).

130. *Id.*

131. *Id.* at 998.

132. *Id.*

not be used to expand the warrant to include other names found in the Tracey directory.

Second, the court required that searches of intermingled data be conducted by specialized personnel or by an independent third party. If the search is conducted by specialized personnel, the government must agree that such personnel will not disclose information beyond the scope of the warrant without a magistrate's approval.[133] Moreover, in cases where the search revolves around an innocent third party, and "the privacy interests of numerous other parties who are not under suspicion of criminal wrongdoing are implicated by the search, the presumption should be that the segregation of the data will be conducted by, or under the close supervision of, an independent third party selected by the court."[134] In *Comprehensive Drug Testing*, the government failed to satisfy this rule when Agent Novitsky—the lead investigator—opened and viewed the intermingled contents of the Tracey directory.[135]

Third, the court found that the government must disclose the *actual* degree of risk that the evidence will be concealed or destroyed.[136] In this case, the government did not disclose to District Court Judge Johnson that "[CDT] had agreed to keep the data intact until its motion to quash the subpoena could be ruled on by the Northern California district court, and that the United States Attorney's Office had accepted this representation."[137]

Fourth, the court held that the government must outline and follow specific search protocols. Moreover, specific search tools may only be used if there is probable cause to believe the information will be found. The court found that the government had not established specific search protocols to ensure that the search was limited to the ten names listed in the warrant.[138]

Finally, once the government has segregated the documents, the information outside the terms of the warrant must "be destroyed or, at least so long as they may be lawfully possessed by the party from whom

---

133. *Id.* at 1006–07.

134. *Id.* at 1000.

135. United States v. Comprehensive Drug Testing, Inc., 513 F.3d 1085, 1111 (9th Cir. 2008).

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

137. *Id.* at 998.

138. *Id.* at 999. The court provided an example to illustrate the fourth guideline:

> [T]he government has sophisticated hashing tools at its disposal that allow the identification of well-known illegal files (such as child pornography) without actually opening the files themselves. These and similar search tools may not be used without specific authorization in the warrant, and such permission may only be given if there is probable cause to believe that such files can be found on the electronic medium to be seized.

Id.

they were seized, returned along with the actual physical medium that may have been seized (such as a hard drive or computer)."[139]

The procedures established by the court provide guidance for handling cases involving computer searches.[140] However, the court noted that in the end reviewing judges must trust "the good sense and vigilance of our magistrate judges, who are in the front line of preserving the constitutional freedoms of our citizens while assisting the government in its legitimate efforts to prosecute criminal activity."[141]

D. Super En Banc?

Unlike other circuits, the Ninth Circuit is so large that en banc decisions are made by eleven of the twenty-eight authorized judgeships. However, "[Ninth] circuit rules provide for review by the *full* court upon the request of any judge."[142] A super-en-banc[143] "has never happened since the limited en banc rule was adopted by the Court in 1980."[144] While unprecedented, the Ninth Circuit is currently considering the possibility of conducting a super-en-banc review of *Comprehensive Drug Testing*. On November 4, 2009, Judge Kozinski entered an order asking the parties to brief whether the case should be reheard by the full en banc court.[145] The ruling in *Comprehensive Drug Testing* placed a heavy burden on investigative agencies by taxing already stretched resources; consequently, on November 23, 2009, the government filed a brief in support of a rehearing en banc by the full court.[146]

---

139. *Id.* at 1000.

140. *Id.* at 1006.

141. *Id.*

142. Statement of Circuit Judge Alex Kozinski to the House Judiciary Subcommittee on Courts, http://www.fedbar.org/Kozinski_testimony.pdf (emphasis added).

143. Orin Kerr, DOJ Files Brief Supporting Super-En-Banc in *CDT* (Nov. 24, 2009), http://volokh.com/2009/11/24/doj-files-brief-supporting-super-en-banc-in-cdt/.

144. Kozinski, *supra* note 142.

145. Order, United States v. Comprehensive Drug Testing, Inc., No. 05-10067 (9th Cir. Nov. 4, 2009), *available at* http://volokh.com/wp/wp-content/uploads/2009/11/CDTOrder.pdf. (stating that Judge Kozinski's order was as follows: "By November 25, 2009, the parties shall file simultaneous briefs addressing whether this case should be reheard en banc by the full court.").

146. Orin Kerr, DOJ Files Brief Supporting Super-En-Banc in *CDT* (Nov. 24, 2009), http://volokh.com/2009/11/24/doj-files-brief-supporting-super-en-banc-in-cdt/.

IV. ANALYSIS

A. The Plain View Doctrine Should Not Be Abandoned in the Electronic Search Context

In *Comprehensive Drug Testing*, the court rejected the government's plain view argument and held that in future cases "[m]agistrates should insist that the government waive reliance upon the plain view doctrine in digital evidence cases."[147] The court's unprecedented holding is partially based on an apparent misapplication of *Tamura*.

The en banc decision overlooks the fact that *Tamura* "is a solution to the problem of overbroad *seizures*, not overbroad searches. The defendant in *Tamura* did not challenge either the warrant or the search of the documents; rather, it was only the seizure that was challenged."[148]

In *Comprehensive Drug Testing*, the court incorrectly applied *Tamura* to a search of documents occurring after a valid *Tamura* seizure. The initial seizure of the entire Tracey directory was valid because the government had obtained advanced authorization for segregating the materials off-site.[149] Thus, the government did not make "a mockery of *Tamura*."[150]

Once the special requirements of *Tamura* have been satisfied, the search of intermingled documents should be treated no differently than other searches. It makes no sense to allow investigators to rely on the plain view doctrine when they are looking for small items in a house and not when they are looking for a file on a computer. Small items, like a single electronic file, can be hidden virtually anywhere. Moreover, "there can be no doubt that the search of a person's entire *home* presents the opportunity for officers to observe vast amounts of information about a person's private life."[151] Thus, if the plain view doctrine applies during

147. United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1006 (9th Cir. 2009) (en banc).

148. Ziff, *supra* note 48, at 859.

149. *Comprehensive Drug Testing*, 579 F.3d at 996. The affidavit supporting the search warrant explained that, if necessary, the agents could conduct an off-site search. *Id.*

150. *Id.* at 998.

151. Ziff, *supra* note 48, at 871.

> In the case of a search for documents or other small items in a person's home, officers are permitted to go 'through the residence with a fine tooth comb.' For example, in one case from the Seventh Circuit, an officer was permitted to examine a notebook pursuant to a warrant to search for cocaine because cocaine 'is commonly distributed . . . in small vials and envelopes and, thus, is easily concealable in confined areas, such as notebooks,' even though the agent testified that he intended to look for things other than cocaine. Indeed, while courts must always be vigilant against overbroad searches, 'searches of computer records are no less constitutional than searches of physical records.
>
> *Id.* (citations omitted).

the search of small items in one's home, it should also apply while looking for files on a person's computer.

In addition to misapplying *Tamura*, the court seemed to resurrect the pre-*Horton* inadvertence requirement. In *Horton*, the U.S. Supreme Court concluded that the subjective intent of officers does not affect the scope of a warrant.[152] The Court later noted that "the fact that the officer does not have the state of mind which is hypothecated by the reasons which provide the legal justification for the officer's action does not invalidate the action taken as long as the circumstances, viewed objectively, justify that action."[153]

Judge Thomas's dissent in the panel decision provides evidence that the court may have relied on the government's subjective intent. According to Judge Thomas:

> The record reflects no forensic lab analysis, no defusing of booby traps, no decryption, no cracking of passwords and certainly no effort by a dedicated computer specialist to separate data for which the government had probable cause from everything else in the Tracey Directory. Instead, as soon as the Tracey Directory was extracted from the CDT computers, the case agent assumed control over it, examined the list of all professional baseball players and extracted the names of those who had tested positive for steroids.[154]

Even more damning was U.S. Attorney Nedrow's statement that Agent Novitsky intended to "briefly peruse [the Tracey directory] to see if there was anything above and beyond that which was authorized for seizure in the initial warrant."[155] However, following the analysis in *Horton*, the fact that the government was unusually efficient in its search or may have intended to use the plain view doctrine to find more steroid users is irrelevant because (1) the search itself was valid and (2) the government's intent should be irrelevant.[156]

In addition to ignoring *Horton*, at least one en banc judge overlooked the implications of the *Beusch* decision. Judge Bea, concurring in part

---

152. Horton v. California, 496 U.S. 128, 138–40 (1990).

153. Scott v. United States, 436 U.S. 128, 138 (1978).

154. *Comprehensive Drug Testing*, 579 F.3d at 999.

155. *Id*.

156. The court's violation of *Horton* parallels the Tenth Circuit's decision in *Carey*.

> *Carey's* violation of *Horton* was recognized by Jim Dowel in *Criminal Procedure: Tenth Circuit Erroneously Allows Officers' Intentions to Define Reasonable Searches*: United States v. Carey. In response to *Carey*, Dowell proposed an objective test to replace *Carey's* inadvertence requirement. Under the test, courts objectively evaluate officers' 'objective judgments about which files could reasonably contain the evidence sought.'

Ziff, *supra* note 48, at 857.

and dissenting in part, argued that the incriminating nature of the other names in the Tracey directory was not "immediately apparent" and thus the names were not in "plain view."[157] The names of the players tested by CDT were contained in a single Excel spreadsheet file. To "avoid scrolling to the right and viewing the results column for all of the ballplayers instead of just for the targeted ten," Judge Bea proposed a particular search protocol.[158] As Judge Bea suggests, the names in the spreadsheet were "theoretically separable." However, according to *Beusch*, information contained in a single file need not be separated and "[t]he fact that an item seized happens to contain other incriminating information not covered by the terms of the warrant does not compel its suppression, either in whole or in part."[159] Thus, because the spreadsheet was a single file, the government was under no obligation to remove the ten names with surgeon-like precision.

Finally, instead of abandoning the plain view doctrine entirely, the court should have struck a more measured tone. Judge Callahan could not "subscribe to the majority's generalized requirement that the government foreswear reliance on the plain view doctrine in digital evidence cases or that magistrate judges insist on such a waiver by the government."[160] According to Judge Callahan, the plain view doctrine is applicable in other electronic contexts. For example, in *Wong*, the court applied the doctrine "to discovery of child pornography in the context of a valid search of a computer for evidence related to a murder investigation."[161] Thus, even assuming that plain view should not apply

---

157. *Comprehensive Drug Testing*, 579 F.3d at 1016 (Bea, J., concurring in part and dissenting in part).

158. *Id.* According to Judge Bea, all Agent Novitsky had to do to avoid viewing the other names was the following:

> While depressing and holding the Control key, he would click on the numbers on the left side of the spreadsheet that corresponded to the rows that contain the names of the targeted ballplayers. The rows containing those ballplayers' names would become highlighted. Novitsky would then release the Control key. He would next go to the top of the screen, click on the "Edit" menu, and choose "Copy." Then, he would click on the "File" menu at the top of the screen, and choose "New Blank Workbook." When the new blank spread-sheet appeared on the screen, he would click on the "Edit" menu in the new blank spreadsheet and choose "Paste." The rows of the ten targeted ballplayers selected in the original spreadsheet and *only those rows* would appear in the new spreadsheet. Novitsky would then scroll to the right in the new blank spreadsheet and would see only the testing results for the targeted ballplayers for whom he had probable cause to search and seize.

Id. at 1016 n.2.

159. United States v. Beusch, 596 F.2d 871, 876 (9th Cir. 1979).

160. *Comprehensive Drug Testing*, 579 F.3d at 1011 (Callahan, J., concurring in part and dissenting in part).

161. *Id.*; United States v. Wong, 334 F.3d 831, 838 (9th Cir. 2003).

in this particular case, the wholesale abandonment of the doctrine was unwarranted.[162]

B. Problems with the En Banc Decision

1. The guidelines place too heavy a burden on investigating agencies

The guidelines established by the Ninth Circuit in *Comprehensive Drug Testing* place too heavy a burden on investigating agencies by requiring the government to use "specialized personnel or an independent third party"[163] to segregate and redact electronic information.[164] Due to pressure on already tight government budgets, using independent third parties raises cost-related concerns. Moreover, the use of specialized personnel within the agency has serious drawbacks.

Professor Derek Regensburger illustrated some of the problems with using specialized personnel within an agency, commonly known as taint teams,[165] to segregate data.[166] According to Regensburger, "the obvious drawback to this approach is that it exposes potentially confidential

---

162. *Compare* Ziff, *supra* note 48, *with* Orin Kerr, An Analysis of *United States v. Comprehensive Drug Testing* (Dec. 9, 2008), http://volokh.com/posts/chain_1228354570.shtml ("Plain view needs to be narrowed, and in my view, may ultimately need to be abandoned in digital searches altogether. The plain view exception is based on an understanding of the role of the particularity requirement that is inaccurate for digital searches: The particularity requirement imposes much less of a limitation in the digital search context, and I think ultimately the most serious way to restore the role of the particularity requirement in digital evidence cases is to limit or abolish plain view; otherwise the exception swallows the rule.").

163. The second guideline provides that

> [s]egregation and redaction must be either done by specialized personnel or an independent third party. If the segregation is to be done by government computer personnel, it must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant.

Comprehensive Drug Testing, 579 F.3d at 1006 (majority opinion).

164. Judge Callahan believes that this guideline

> raises practical, cost-related concerns. With respect to using an in-house computer specialist to segregate data, the majority's guideline essentially requires that law enforcement agencies keep a "walled-off," non-investigatory computer specialist on staff for use in searches of digital evidence. To comply, an agency would have to expand its personnel, likely at a significant cost, to include both computer specialists who could segregate data and forensic computer specialists who could assist in the subsequent investigation. The alternative would be to use an independent third party consultant, which no doubt carries its own significant expense. Both of these options would force law enforcement agencies to incur great expense, perhaps a crushing expense for smaller police departments that already face tremendous budget pressures.

Id. at 1013 (Callahan, J., concurring in part and dissenting in part).

165. Taint teams consist of government personnel who are not otherwise involved in the case under investigation. These teams review all the electronic records and identify the portions of those records that the investigators who are handling the case should not see.

166. Regensburger, *supra* note 10, at 1166.

information to the eyes of the taint team. It also relies heavily on the integrity of the personnel involved not to breach the Chinese Wall."[167] These risks are not merely theoretical; taint teams "have been implicated in the past in leaks of confidential information to prosecutors."[168] In one case, a taint team turned over tapes of attorney-client conversations to the prosecuting team.[169] This incident demonstrates the problem with taint teams as "[t]he government's fox is left in charge of the appellants' henhouse, and may err by neglect or malice, as well as by honest differences of opinion."[170] These concerns may explain why "court response has been equivocal to the use of taint teams."[171]

Thus, practical concerns and financial burdens make the guidelines too much of a burden on investigating agencies. Specifically, the taint team requirement should be abandoned.[172] Instead of using taint teams, the government should continue "using the more traditional alternatives of submitting disputed documents under seal for in camera review by a neutral and detached magistrate or by court-appointed special masters."[173] In addition to being the more efficient approach, using magistrates is supported by case law.

2. The guidelines are premature because computer forensics is rapidly evolving

Professor Orin Kerr has argued for a laissez-faire application of the Fourth Amendment to evolving technologies.[174] According to Kerr, "[w]hen technology is in flux, Fourth Amendment protections should remain relatively modest until the technology stabilizes."[175] There is no question that computer forensics is rapidly changing as "[i]nvestigators and sophisticated wrongdoers inevitably play a cat-and-mouse game in which suspects try to hide evidence and forensic analysts try to find

167. *Id.* at 1170. The "Chinese Wall" refers to the separation between members of the taint team and the prosecution team.

168. *Id.* at 1171.

169. *In re* Grand Jury Subpoenas, 454 F.3d 511, 523 (6th Cir. 2006).

170. *Id.*

171. Regensburger, *supra* note 10, at 1170. Nonetheless, while "the use of taint teams is 'unwise' and creates an 'appearance of unfairness,' [one district court] found their use does not offend the Constitution absent a showing of harm resulting from disclosure of the privileged information." *Id*. at 1171 (citing United States v. Neill, 952 F. Supp. 834, 841 (D.D.C. 1997)).

172. Furthermore, as Judge Callahan notes, "the majority offers no support for its protocol requiring the segregation of computer data by specialized personnel or an independent third party." United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1013 (9th Cir. 2009) (en banc) (Callahan, J., concurring in part and dissenting in part); *see id*. at 1000–01, 1006 (majority opinion).

173. Regensburger, *supra* note 10, at 1171.

174. Kerr, *supra* note 9.

175. *Id.* at 805.

it."[176] Some experts forecast the development of sophisticated search tools that focus on evidence described in the warrant. While a "Perfect Tool"[177] may never emerge, forensic searches will probably become increasingly sophisticated in the near future.

With changes on the horizon, Judge Callahan's more cautious analysis is appropriate. According to Judge Callahan, "[a] measured approach based on the facts of a particular case is especially warranted in the case of computer-related technology, which is constantly and quickly evolving."[178] Judge Callahan's approach fits with Kerr's theory that "we should look first to Congress when technology is changing rapidly."[179] Kerr believes that by focusing on legislative rules "the legal system [will be able] to generate better rules—rules that are more nuanced, clear, and that optimize the critical balance between privacy and public safety more effectively when technology is in flux."[180]

3. The guidelines are too broad

The most troubling aspect of *Comprehensive Drug Testing* is not the ruling itself, but the expansive guidelines tacked on at the end of the decision. These guidelines,[181] which really amount to bright-line rules,[182] are not anchored in a case or controversy.[183] Moreover, based on the

176. Kerr, *supra* note 4.

177. *Id.* at 570.

178. United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1013 (9th Cir. 2009) (en banc) (Callahan, J., concurring in part and dissenting in part). Judge Bea agreed with Judge Callahan on this point: "The common law method permits us to evaluate different cases over time to discern the most sensible rule given the technologies that develop; I'm afraid the majority opinion short-circuits this process in an area where the capabilities of computer software are *still rapidly evolving*." *Id.* at 1018 (Bea, J., concurring in part and dissenting in part) (emphasis added).

179. Kerr, *supra* note 9, at 806.

180. *Id.*

181. According to Judge Callahan, even though "the majority's [plain view] guideline is framed in terms of what a magistrate 'should insist,' the practical effect of this guideline is to prescribe a mandatory procedure. *Comprehensive Drug Testing*, 579 F.3d at 1013 n.8 (Callahan, J., concurring in part and dissenting in part).

182. Judge Bea, concurring in part and dissenting in part, cautioned that "we must treat our establishment of brightline rules with great care and deliberation; at the very least, amici should have an opportunity to weigh in on the dramatic doctrinal shift the majority's guidelines contemplate." *Id.* at 1018 (Bea, J., concurring in part and dissenting in part). For a discussion of some of the benefits and drawbacks of bright-line rules, see Pierre Schlag, *Rules and Standards*, 33 UCLA L. REV. 379 (1986). One common drawback of such rules is that "[b]y specifying a sharp line between forbidden and permissible conduct, [they] permit and encourage activity up to the boundary of permissible conduct." *Id.* at 384–85.

183. *See* Sonnenschein Nath & Rosenthal LLP, Publications, *Attorneys, Academics Sort Through Landmark Case on Computer Searches*, http://www.sonnenschein.com/pubs/publications/Marc-Zwillinger-Electronic-Commerce-Law.html ("The Ninth Circuit's opinion does not make clear whether its imposition of the new restrictions is based on the Fourth Amendment or, instead, on the circuit court's supervisory authority over the district courts' issuance of warrants. The source of the court's authority not only has impact in

facts before it, the court's actual holding was quite narrow: (1) government was barred under the doctrine of issue preclusion from contesting determination that it callously disregarded affected players' constitutional rights; (2) district court did not abuse its discretion by requiring the government to return copies of the seized evidence; and (3) district court did not abuse its discretion in quashing the government's subpoena.[184]

The guidelines, in contrast, constitute expansive dicta that guide the procedure and ultimately the outcome of all future digital evidence cases. Judge Callahan noted that "[r]ather than adopting this efficient but overbroad approach, the prudent course would be to allow the contours of [digital evidence rules] to develop incrementally through the normal course of fact-based case adjudication."[185] Thus, as prophylactic dicta, the guidelines represent an attack on the common law approach to jurisprudence.[186]

In addition to lacking a clear foundation, the guidelines fall prey to the bane of all bright-line rules: over-inclusiveness. The case before the court in *Comprehensive Drug Testing* is uncommon because it involves the seizure of medical records implicating unidentified third parties. In the electronic context, it is far more common for cases to involve child pornography. Consequently, the court is using an outlier case to establish procedures for all future electronic evidence cases.

C. How the Court Should Have Ruled

The court should have reached the same result without promulgating the expansive guidelines outlined in the decision. First, instead of using the guidelines, the court could have narrowed its decision to cases involving medical data. The medical privacy issue is "one of the things that gets folks worked up"[187] about the *Comprehensive Drug Testing* decision. In recent years, "personal health information on hundreds of thousands of people has been compromised because of security lapses at hospitals, insurance companies and government agencies. These

---

matters of civil liability and retroactivity, it also will greatly affect the applicability of the new protocols outside the Ninth Circuit.").

184. *Comprehensive Drug Testing*, 579 F.3d at 989 (majority opinion).

185. *Id.* at 1013 (Callahan, J., concurring in part and dissenting in part).

186. According to Judge Bea,

> the establishment of guidelines (which are little more than dicta but are nonetheless binding precedent in [the Ninth circuit], *see Brand X Internet Servs. v. FCC*, 345 F.3d 1120, 1130 (9th Cir. 2003)) in the manner chosen by the majority goes against the grain of the common law method of reasoned decision making, by which rules evolve from cases over-time.

Id. at 1018 (Bea, J., concurring in part and dissenting in part).

187. Kerr, *supra* note 162.

breaches occurred despite federal privacy rules issued under a 1996 law."[188] Understandably, many people—including members of the judiciary—are concerned about medical privacy. "Congress could avoid some of the difficulties here by expanding the Privacy Protection Act[189] to include special rules for searches involving medical records."[190]

A second way the court could have limited its decision is by narrowing it to searches involving the confidential business records of innocent third parties. Searches of third party business computers are easily distinguishable from personal computer searches because the former often involve thousands of records relating to individuals outside the scope of the investigation.[191] The court could have found that the Privacy Protection Act of 1980 requires special protections in the third party context to "minimize, to the greatest extent practicable, scrutiny of confidential materials."[192] This interpretation would be reasonable even though few cases have explored the contours of the Act.[193]

D. The Future of Comprehensive Drug Testing

With its sweeping new rules, the en banc decision in *Comprehensive Drug Testing* may be short lived. According to Orin Kerr, as of December 20, 2009, "no federal court has agreed with *CDT* in a written opinion since the decision came down in August."[194] The Seventh Circuit recently declined to follow *Comprehensive Drug Testing*, concluding that "there 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."[195]

Some legal experts believe there is a good chance that the U.S. Supreme Court will review the decision if the government appeals.[196] Others are not so sure. According to Kerr, "the justices might prefer to wait for future Ninth Circuit opinions to clarify the authority [the court] was relying upon in [CDT] and some of the other murkier aspects of the

188. Robert Pear, *Privacy Issue Complicates Push to Link Medical Data*, N.Y. TIMES, Jan. 17, 2009, *available at* http://www.nytimes.com/2009/01/18/us/politics/18health.html.

189. 42 U.S.C. § 2000aa (2009).

190. Kerr, *supra* note 162.

191. Regensburger, *supra* note 10, at 1166.

192. 28 C.F.R. § 59.4 (2009).

193. Regensburger, *supra* note 10, at 1168.

194. Orin Kerr, *Cuffing Digital Detectives* (Dec. 20, 2009), http://volokh.com/2009/12/20/cuffing-digital-detectives/

195. United States v. Mann, 592 F.3d 779, 785 (7th Cir. 2010).

196. *See* Sonnenschein Nath & Rosenthal LLP, *supra* note 183.

[case]."[197] One way or another, this case will continue to receive significant attention in the coming months.

V. CONCLUSION

In *Comprehensive Drug Testing*, the Ninth Circuit radically changed the legal landscape surrounding computer searches by creating a set of guidelines. These guidelines are expansive and require the government to waive its reliance on the plain view doctrine in digital evidence cases. By eliminating the plain view doctrine in the digital evidence cases this court handed down a decision inconsistent with past case law and Fourth Amendment jurisprudence. The court's decision was burdensome, premature, and too broad. It would have been more appropriate for the court to have decided the case on more narrow grounds such as medical data privacy or innocent third party involvement. While it is difficult to determine the future of *Comprehensive Drug Testing*, the case has a good chance of being reviewed by a super en banc or by the U.S. Supreme Court.

Allen H. Quist[*]

197. *Id.*

[*] J.D. candidate, 2011, J. Reuben Clark School of Law, Brigham Young University. I would like to thank Professor Ken Wallentine for guiding me to *Comprehensive Drug Testing* and giving me the tools to write about it in a meaningful way. I am also grateful to Aaron Quist, Sarah Jacquier, and the *Brigham Young Journal of Public Law* staff for their contribution to this Note.