COMMENTS

COMPUTER SEARCHES IN PLAIN VIEW: AN ANALYSIS OF THE NINTH CIRCUIT'S DECISION IN *UNITED STATES V. COMPREHENSIVE DRUG TESTING, INC.*

Alison Bonelli[*]

TABLE OF CONTENTS

---

* J.D. Candidate, University of Pennsylvania Law School; B.A. 2006, Georgetown University. Special thanks to Professor Bibas for his feedback; the editors of the *University of Pennsylvania Journal of Constitutional Law* for their tremendous editing; and my mother, Patricia Bonelli, for her invaluable guidance and support.

While A-Rod and Sammy Sosa lent the Ninth Circuit's August 2009 opinion in *United States v. Comprehensive Drug Testing, Inc.* a generous dose of star power, the case was about much more than Major League Baseball. It not only involved the investigation that led to the shocking revelation that four of baseball's most beloved players—Alex Rodriguez, David Ortiz, Manny Ramirez, and Sammy Sosa—tested positive for steroid use in 2003,[1] but also created shockwaves among observers and commentators for its implications regarding the Fourth Amendment. While much of the media frenzy associated with the case focused on the "Steroid Era" of baseball, the decision raised serious questions regarding the extent to which law enforcement officials may seize digital evidence in compliance with the Fourth Amendment.[2]

---

1 Michael S. Schmidt, *Stars of Red Sox Title Years Are Linked to Doping*, N.Y. TIMES, July 31, 2009, at A1 ("Baseball first tested for steroids in 2003, and the results from that season were supposed to remain anonymous. But for reasons that have never been made clear, the results were not destroyed and the first batch of positives has come to be known among fans and people in baseball as 'the list.'").

2 *See, e.g.*, Michael McCann, *Remaining Names on Drug List Likely to Remain Under Seal Indefinitely*, SPORTS ILLUSTRATED, Aug. 26, 2009, http://sportsillustrated.cnn.com/2009/writers/michael_mccann/08/26/mlb.drug.list.ruling/index.html ("While *U.S. v. Comprehensive Drug Testing* serves as an important decision for the Fourth Amendment's application to electronically stored information, it also impacts the potential disclosure of the remaining 97 names, which have been sealed by court order.").

What began as a Ninth Circuit opinion designed to address whether federal agents exceeded the scope of their search warrant in seizing electronic records about steroid use for over one hundred Major League Baseball players, quickly developed into a preventative guide on avoiding the dangers inherent in computer searches.[3] In response to the notion that current Fourth Amendment jurisprudence is tailored around the search and seizure of physical objects and is ill-equipped to accommodate the rapidly growing and changing needs of an increasingly electronic world, the Ninth Circuit's en banc majority opinion in *Comprehensive Drug Testing, Inc.* set out strict and detailed guidelines to be followed by all federal officials conducting computer searches. These requirements included the elimination of the plain view exception to the warrant requirement and the specification that all segregation and redaction of electronic data during a police investigation must be conducted by an independent third party or trained computer forensic personnel.

While these guidelines were later relegated to a non-binding concurrence in an amended opinion authored by the Ninth Circuit in September 2010,[4] the limitations on agents as set forth in the en banc opinion are critical to understanding the complex law that is developing around searches and seizures of electronic data, particularly how the plain view exception to the warrant requirement should be applied to computer searches. Part I of this Comment will attempt to address this issue by first providing an overview of the Fourth Amendment and warranted searches, highlighting the difference between computer and physical searches in the application of the plain view doctrine. It will then discuss the plain view doctrine as it existed before *Horton v. California* and the abrogation of the inadvertence requirement, arguing that the doctrine, post-*Horton*, is becoming increasingly inadequate in the face of advancing technology. Parts II, III, and IV will examine the case law surrounding computer searches and the plain view doctrine in the Ninth Circuit, as well as that Circuit's recent decisions in *United States v. Comprehensive Drug Testing, Inc.*—both the original en banc opinion and the amended version—and will discuss the various reasons the Ninth Circuit appropriately decided to amend the decision. Finally, Parts V and VI will describe

3 United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 993 (9th Cir. 2009) ("This case is . . . about the procedures and safeguards that federal courts must observe in issuing and administering search warrants and subpoenas for electronically stored information.").

4 United States v. Comprehensive Drug Testing, Inc., No. 05-10067, 2010 WL 3529247 (9th Cir. Sept. 13, 2010) (*per curiam*).

the circuit split that exists around how the plain view doctrine should be applied to computer searches and will argue that the intent-based approach of the Seventh and Tenth Circuits, which restores the inadvertence requirement to the plain view doctrine, is the better and more effective alternative.

I. THE FOURTH AMENDMENT AND THE PLAIN VIEW DOCTRINE

The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause . . . particularly describing the place to be searched, and the persons or things to be seized.[5]

The Fourth Amendment incorporates a strong preference for search warrants. In determining whether search warrants are required, the Court has viewed searches and seizures in light of a reasonableness test, as defined by *Katz v. United States*, which asks whether an individual has a reasonable expectation of privacy in the item or items searched or seized.[6] Traditionally, warrantless searches were generally considered unreasonable, save for a few "jealously and carefully drawn" exceptions.[7] The primary Fourth Amendment enforcement doctrine, the Exclusionary Rule, was first developed by the Supreme Court in 1914.[8] In *Weeks v. United States*, the Court held that any evidence obtained by the police in violation of the Fourth Amendment must be excluded from evidence in court.[9] Thus, evidence obtained without a warrant may be subject to the Exclusionary Rule.

Today, exceptions to the warrant requirement have largely swallowed the rule. Indeed, "[m]odern search and seizure law is astoundingly complex and contradictory."[10] A partial list of modern exceptions to the warrant requirement include: "exigent circumstances (such as flight or destruction of evidence), the direct observation of

---

5 U.S. CONST. amend. IV.

6 Katz v. United States, 389 U.S. 347, 353 (1967) ("[O]nce it is recognized that the Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.").

7 MARC L. MILLER & RONALD F. WRIGHT, CRIMINAL PROCEDURES: CASES, STATUTES AND EXECUTIVE MATERIALS 43 (3d ed. 2007).

8 Weeks v. United States, 232 U.S. 383, 398 (1914) ("We therefore reach the conclusion that the letters in question were taken from the house of the accused by an official of the United States acting under color of his office in direct violation of the constitutional rights of the defendant . . . . In holding them and permitting their use upon the trial, we think prejudicial error was committed.").

9 *Id.*

10 MILLER & WRIGHT, *supra* note 7, at 44.

crime, plain view, open fields, community caretaker functions, brief investigative stops, brief frisks for weapons, inventory searches, protective sweeps, automobile searches, border searches, school searches, [and] prison searches."[11]

Under the plain view exception to the warrant requirement, police officers may seize an object without a warrant if: 1) the officers are lawfully in the position from which they view the object; 2) the object's incriminating character is immediately apparent; and 3) the officers have a lawful right of access to the object.[12] In *Horton v. California*, the Supreme Court held that while inadvertence is a factor to be considered in determining the legitimacy of a plain view seizure, that factor alone is not dispositive.[13] In *Horton*, a California police officer obtained and executed a warrant to search the defendant's home for the proceeds of a robbery. While the officer did not find the proceeds, he did find and seize weapons in plain view.[14] Though the officer later admitted that he was interested in finding evidence unassociated with the robbery, the Supreme Court did not exclude the evidence from the search. The Court reasoned that the:

> suggestion that the inadvertence requirement is necessary to prevent the police from conducting general searches, or from converting specific warrants into general warrants, is not persuasive because that interest is already served by the requirements that no warrant issue unless it 'particularly describ[es] the place to be searched and the persons or things to be seized.'[15]

The scope of the search was not enlarged by the failure to mention weapons in the warrant. The Court used an analogy to illustrate their point: "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; the inadvertence rule will in no way reduce the number of places into which they may lawfully look."[16]

---

11 *Id.*

12 *See* 68 AM. JUR. 2D *Sales and Use Taxes* § 101 (1973) (describing the extended scope of given consent); *see also* Minnesota v. Dickerson, 508 U.S. 366 (1993) (holding that the police may seize an object if detected through touch during a protective search).

13 Horton v. California, 496 U.S. 128, 130 (1990) ("We conclude that even though inadvertence is a characteristic of most legitimate 'plain-view' seizures, it is not a necessary condition.").

14 *Id.* at 128.

15 *Id.* at 139 (internal citation omitted) (alteration in original).

16 *Id.* at 141 (quoting Coolidge v. New Hampshire, 403 U.S. 443, 517 (1971)).

A. Computer Searches Versus Physical Searches

"Existing rules of criminal procedure are naturally tailored to the facts of physical-world crimes."[17] In *United States v. Katz*, the Supreme Court famously stated that the Fourth Amendment protects "people, not places."[18] Yet, as Justice Harlan noted in his *Katz* concurrence, the protection provided to people "requires reference to a 'place.'"[19] While some courts have attempted to liken computers to physically-closed containers, such as suitcases,[20] in an attempt to fit computer searches into existing Fourth Amendment jurisprudence, other courts and commentators have advocated for a "special approach" to the investigation of electronic data.[21]

The particularity requirement, explicit in the text of the Fourth Amendment, requires that a search warrant describe the place to be

---

17 Orin S. Kerr, *Digital Evidence and the New Criminal Procedure,* 105 COLUM. L. REV. 279, 290 (2005) [hereinafter Kerr, *Digital Evidence*]. Kerr, a professor at George Washington University Law School, has written extensively on the differences between physical and electronic searches and the difficulties of applying the Fourth Amendment to digital evidence. *See also* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531 (2005) [hereinafter Kerr, *Searches and Seizures*] (discussing how the Fourth Amendment applies to electronic storage devices).

18 Katz v. United States, 389 U.S. 347, 353 (1967).

19 *Id.* at 361; *see also* Kerr, *Digital Evidence, supra* note 17, at 290 ("Under Justice Harlan's formulation, the Fourth Amendment remains heavily tied to places . . . .").

20 *See* Donald Resseguie, *Computer Searches and Seizures*, 48 CLEV. ST. L. REV. 185, 204–05 n.197 (2000) ("A number of other cases allowed for wholesale seizure of computer equipment for later off-site sorting without additional approval from a magistrate essentially applying the closed container analogy to computer equipment. *See* United States v. Longo, 70 F. Supp. 2d 225 (W.D.N.Y. 1999) (allowing broad search of computer files); United States v. Gawrysiak, 972 F. Supp. 853 (D.N.J. 1997) (seizing all computer files without determination of those relevant to the scope of the search warrant was permissible and did not allow for blanket suppression of all evidence), *aff'd*, 178 F.3d 1281 (3d Cir. 1999); United States v. Kufrovich, 997 F. Supp. 246 (D. Conn. 1997) (permitting blanket seizure of computer without any on-site sorting for evidence relevant to the crime under investigation); United States v. Stewart, No. CRIM.A. 96-583, 1997 WL 189381 (E.D. Pa. Apr. 16, 1997) (allowing seizure of all computer hardware and software along with a large quantity of documents for later review off-site); United States v. Hersch, No. CRIM.A. 93-10339-Z, 1994 WL 568728 (D. Mass. Sept. 27, 1994) (finding that a search warrant calling for the seizure of all computer hardware, software and related equipment was not a general search given the complexity of the scheme under investigation).").

21 *See* 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, 1155 (2007) (acknowledging these approaches and noting that "a computer . . . is anything and everything a user wants it to be—a file cabinet containing thousands of personal files or business records, a personal accountant, a photo album, a music or movie player, a virtual desk complete with calendar and Rolodex, a research librarian, or a video game machine").

searched or the item to be seized.[22] This requirement ensures that the scope of the police's search remains as narrow as possible. With physical evidence, this is a fairly straight-forward requirement. A warrant is suitably particular if it details "general classifications of the items to be seized," which would allow an officer to "ascertain and identify with reasonable certainty" the items to be seized.[23] Further, "[t]he seizure must be limited to the evidence described in the warrant—which itself is limited by the scope of probable cause to believe that the evidence is on the premises—as well as other evidence discovered in plain view during the course of the search."[24] In physical places, the particularity requirement restricts the scope of a search to a home, room, closet, or drawer, and prevents a specific warrant from becoming a general warrant.[25] Under the Fourth Amendment, "investigators executing a warrant can look anywhere in the place to be searched where evidence described in the warrant might conceivably be located. In traditional investigations for physical evidence, this rule means that officers cannot look in places smaller than the evidence they wish to seize."[26]

It has been argued that electronic searches cannot be limited in the same way. Electronic evidence is almost always located anywhere on a computer in files that appear identical. Further, those files are often "mislabeled, hidden, or otherwise stored in a way that the investigator can never rule out a particular part of the hard drive ex ante."[27] Within that massive amount of data, it is often difficult for of-

22 *See, e.g.*, Maryland v. Garrison, 480 U.S. 79, 84 (1987) ("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.'").

23 Regensburger, *supra* note 21, at 1156 (quoting United States v. George, 975 F.2d 72, 75 (2d Cir. 1992) (internal quotation marks omitted)).

24 Kerr, *Digital Evidence, supra* note 17, at 299.

25 *See id.* at 302 ("In physical space, the particularity requirement limits the scope of a search to a place on the order of a house or apartment. Limiting the space to be searched serves as a key limitation on the scope of the search."); *see also* Maryland v. Garrison, 480 U.S. at 86 ("The manifest purpose of this particularity requirement was to prevent general searches. By limiting the authorization to search to the specific 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.").

26 Kerr, *Digital Evidence, supra* note 17, at 304.

27 *Id.* Courts have often recognized the dangers in limiting an officer's ability to freely search a computer. *See, e.g.*, United States v. Hill, 459 F.3d 966, 978 (9th Cir. 2006) ("'Computer records are extremely susceptible to tampering, hiding, or destruction, whether deliberate or inadvertent.' Images can be hidden in all manner of files, even word processing documents and spreadsheets. Criminals will do all they can to conceal contraband, including the simple expedient of changing the names and extensions of files to disguise their content from the casual observer." (internal citation omitted)).

ficers to pinpoint the location of the responsive digital evidence. Evidence may be contained in files on a hard drive of a computer and may also be hidden from view by encryption "or other security methods."[28] As a result, it is often necessary to search the entire computer to find the responsive information.

Courts have taken vastly different approaches in dealing with complex computer searches. Some courts have found the warrant particularity requirement satisfied even though the warrant only generally describes the computer or media to be searched.[29] Because of a computer's massive storage capacity, other courts "have been loath to authorize broad searches which allow agents seeming unfettered discretion in deciding what files to seize and how they should be searched."[30] Indeed, a warrant simply limiting a search to a computer may be insufficient to restrict the scope of a search: five years ago, the hard drive "on a typical new home computer stored at least forty gigabytes of information, roughly equivalent to twenty million pages of text or about half the information stored in the books located on one floor of a typical academic library."[31] Further, "limiting a search to a particular computer is something like limiting a search to a city block; ten years from now, it will be more like limiting a search to the entire city."[32]

---

28 Regensburger, *supra* note 21, at 1156.

29 United States v. Lacy, 119 F.3d 742, 746–47 (9th Cir. 1997) ("Both warrants described the computer equipment itself in generic terms and subjected it to blanket seizure. However, this type of generic classification is acceptable 'when a more precise description is not possible,' and in this case no more specific description of the computer equipment sought was possible. The government knew Lacy had downloaded computerized visual depictions of child pornography, but did not know whether the images were stored on the hard drive or on one or more of his many computer disks. In the affidavit supporting the search warrant application, a Customs agent explained there was no way to specify what hardware and software had to be seized to retrieve the images accurately." (quoting United States v. Cardwell, 680 F.2d 75, 78 (9th Cir. 1982) (citations omitted)).

30 Regensburger, *supra* note 21, at 1157; *see, e.g.*, United States v. Carey, 172 F.3d 1268, 1276 (10th Cir. 1999) (holding that the search of a computer containing pornographic image files went beyond the scope of a warrant permitting the search of a computer for evidence of drug trafficking).

31 Kerr, *Digital Evidence, supra* note 17, at 302; *see also* Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J. L. & TECH. 75, 105 (1994) ("Since electronic storage is likely to contain a greater quantity and variety of information than any previous storage method, computers make tempting targets in searches for incriminating information. However, this very quantity and variety of information increases the likelihood that highly personal information, irrelevant to the subject of the lawful investigation, will also be searched or seized.").

32 Kerr, *Digital Evidence*, *supra* note 17, at 303.

An alternative approach to computer searches was advocated by Raphael Winick in 1994.[33] He recognized the potential dangers in applying a traditional Fourth Amendment analysis to computers that can store "massive quantities" of data.[34] His approach was comprised of two steps. First, the officer must seek permission to remove a computer from the premises.[35] Once that permission is granted, the officers must get a second warrant that details precisely what types of files are to be searched and exactly how the files will be searched.[36] Winick also proposed a procedure to deal with intermingled documents in computer searches:

> "[W]here 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. If the officers know prior to the search that transporting large quantities of documents or hardware is likely, they can apply to the magistrate issuing the warrant for permission to remove such material; permission should be granted only when on-site sorting of relevant and irrelevant material is infeasible and no other practical alternative exists."[37]

Orin Kerr has rejected Winick's approach in favor of one that proposes that "forensic examiners, not magistrates, are the persons who are best able to dictate the search parameters."[38] Without first looking at the files on a hard drive, Kerr argued, it is practically impossible to know what a particular search requires. "The ability to target information described in a warrant is highly contingent on a number of factors that are difficult or even impossible to predict ex ante."[39] Kerr further noted that because of these difficulties, "magistrate judges are poorly equipped to evaluate whether a particular search protocol is the fastest and most targeted way of locating evidence stored on a hard drive."[40]

---

33 Winick, *supra* note 31.

34 *Id.* at 89.

35 *Id.* at 107; *see also* Regensberger, *supra* note 21, at 1158 (stating that the first prong of Winick's test "requires that officers apply for permission to remove a computer and storage media from the premises").

36 Winick, *supra* note 31, at 108.

37 *Id.* at 105–06.

38 Regensberger, *supra* note 21, at 1161; *see also* Kerr, *Searches and Seizures*, *supra* note 17, at 572 (arguing that an ex ante strategy "wrongly assumes that prosecutors and magistrate judges have the knowledge needed to articulate search strategies before the search begins").

39 Kerr, *Searches and Seizures, supra* note 17, at 575.

40 *Id.*

B. The Perils of the Plain View Doctrine and Computer Searches

The plain view exception to the warrant requirement, when applied to computer files, further highlights the difficulty in applying traditional Fourth Amendment principles to digital media. The plain view doctrine is only satisfied when, among other things, an officer conducts a narrowly tailored search that is reasonably related to the target of the search. "Though the plain view doctrine increases the amount of evidence an officer can possibly seize, it also limits the manner in which the police conduct searches."[41] In a physical search, warrants limit officers to physical places, such as rooms and buildings. In computer searches, those physical limitations do not exist, making it difficult, if not impossible, to narrowly tailor a search. For example, "[t]hough a warrant may describe a certain type of file, [such as] a text file, it is difficult to conduct a search only of text files."[42] Seizing a computer for a few responsive files is comparable to seizing an entire house and carting off its contents "to mine them for evidence of crime, which the Fourth Amendment prohibits."[43] If the entire contents of a computer may be searched and seized, without limitation, it is distinctly possible that an officer may use the plain view doctrine to justify the seizure of any evidence that falls outside the scope of the warrant.

Additionally, in order for evidence to be admitted under the plain view doctrine, the incriminating nature of that evidence must be immediately apparent and in plain view of the investigators. With computer searches "[o]fficers neither stand within the confines of the computer nor rely on their ambient vision to immediately identify elements of the digital landscape."[44] Rather, officers work with the contents of a computer in a very abstract way. "A user must execute a file to reveal its hidden contents. Accordingly, a directory is not obviously incriminating until it is investigated."[45] Under the plain view doctrine, officers may be able to seize any of these files.[46]

The potential freedom of officers to seize electronic information outside the scope of a warrant through the plain view doctrine is troublesome, particularly when it is considered that inadvertence is no longer a requirement of that doctrine. The justifications for eli-

---

41 Andrew Vahid Moshirnia, *Separating Hard Fact from Hard Drive: A Solution for Plain View Doctrine in the Digital Domain*, 23 HARV. J.L. & TECH. 609, 612 (2010).

42 *Id.* at 612–13.

43 Kerr, *Digital Evidence*, *supra* note 17, at 300.

44 Moshirnia, *supra* note 41, at 612.

45 *Id.*

46 *Id.*

minating the inadvertence requirement in *Horton v. California* are no longer valid in the context of computer searches.[47] Since narrowly tailoring a computer search is difficult, the check against general warrants as described in *Horton* may not exist.[48] Additionally, the particularity requirement in the Fourth Amendment—that no warrant shall issue unless it "particularly describ[es] the place to be searched, and the persons or things to be seized"—may be difficult to enforce in the context of computer searches and will not protect against general searches, as *Horton* said it would.[49] Courts and commentators have understandably struggled to apply the plain view doctrine in an electronic context.[50] While some courts have abandoned plain view, others have attempted to adapt the doctrine to fit digital searches.[51]

II. THE NINTH CIRCUIT'S APPROACH TO THE PLAIN VIEW DOCTRINE AND COMPUTER SEARCHES BEFORE *COMPREHENSIVE DRUG TESTING, INC.*

Because the Ninth Circuit has taken the most drastic stance in regulating computer searches, this comment focuses on the line of decisions that arrived at the current state of the law in that jurisdiction. However, when considering alternative approaches, the view of other circuits will be discussed.[52] Until the groundbreaking en banc decision in *U.S. v. Comprehensive Drug Testing, Inc.* in August 2009, the Ninth Circuit had often rejected the use of strict search protocols and contemplated the use of the plain view exception to the warrant requirement during computer searches. Prior to *Comprehensive Drug Testing, Inc.*, the Ninth Circuit generally refused to apply a unique approach to computer searches and instead used a traditional closed container analysis. Over the past several years (and up until the *Com-*

47 *See supra* Part I.

48 *Id.*

49 U.S. CONST. amend. IV.

50 Orin Kerr, among other commentators, is an advocate of "rethink[ing] the plain view exception in the context of digital evidence." *See* Kerr, *Searches and Seizures*, *supra* note 17, at 576–77 ("The dynamics of computer searches upset the basic assumptions underlying the plain view doctrine. More and more evidence comes into plain view, and the particularity requirement no longer functions effectively as a check on dragnet searches. In this new environment, a tightening of the plain view doctrine may be necessary to ensure that computer warrants that are narrow in theory do not become broad in practice.").

51 Moshirnia, *supra* note 41, at 613 ("Because the plain view doctrine is discordant with the digital domain, courts have struggled to apply their prior physical jurisprudence to new technologies. While some courts have become so frustrated that they have effectively abandoned plain view in the electronic context, other courts have adopted tortured and ultimately unsatisfactory frameworks for digital searches.").

52 *See infra* Part V.

prehensive Drug Testing, Inc. decision), the court often declined to suppress evidence relating to a second crime implicating the defendant when that evidence was found in plain view during an officer's warranted search of the defendant's computer.

In 2006, the Ninth Circuit in *U.S. v. Adjani* declined to restrict the government's e-mail search to specific search terms or e-mail addresses. Because file names can easily be altered or disguised, the government should "not be required to trust the suspect's self-labeling when executing a warrant."[53] The court further stated that "[t]here is no rule . . . that evidence turned up while officers are rightfully searching a location under a properly issued warrant must be excluded simply because the evidence found may support charges for a related crime (or against a suspect) not expressly contemplated in the warrant."[54] A warrant was issued to obtain evidence of an extortion plot of a co-defendant. The defendant in that case argued that the e-mails seized after a search of her computer were obtained illegally, since the e-mails fell outside the scope of the warrant. The court rejected the defendant's claim that the e-mails seized were outside the scope of the warrant "because they implicated her in the crime and supported a charge of conspiracy to commit extortion (a crime not specifically mentioned in the warrant)."[55]

In *U.S. v. Wong*, the Ninth Circuit allowed child pornography found on the defendant's computer to be admitted as evidence.[56] In that case, the search warrant specified that murder evidence could be found on the defendant's computer in "plain text, special text, and graphics files."[57] The court found that since the officers were lawfully searching the computer for "evidence of murder in the graphics files [] that they had legitimately accessed and where the incriminating child pornography was located, the evidence was properly admitted under the plain view doctrine."[58]

In *U.S v. Giberson*, the Ninth Circuit held that the district court properly denied the defendant's motion to suppress evidence of child pornography found on a copied computer hard drive by an officer during a search for evidence of the production of false identification (I.D.) cards, done pursuant to a valid warrant.[59] The court declined

53 United States v. Adjani, 452 F.3d 1140, 1150 (9th Cir. 2006).
54 *Id.* at 1151.
55 *Id.*
56 United States v. Wong, 334 F.3d 831, 839 (9th Cir. 2003).
57 *Id.* at 838.
58 *Id.*
59 United States v. Giberson, 527 F.3d 882, 889–90 (9th Cir. 2008).

to impose heightened protections in computer searches as a result of a computer's ability to store potentially intermingled information.[60] The court wrote that "[i]t would be unreasonable to require the government to limit its search to directories called, for example, 'Fake I.D. Documents.'"[61]

Finally, discussion of the Ninth Circuit's decisions on the plain view doctrine and computer searches mandates mention of *United States v. Tamura*, although that case dealt with intermingled *paper* documents.[62] In 1982, the court in *Tamura* broke with the closed container analysis and "objected to the 'wholesale seizure' of entire filing cabinets of records without any efforts to limit the seizure of unrelated material."[63] The government's warrant only authorized seizure of three types of records from the defendant's office.[64] Because those documents were so intermingled with other documents outside of those three categories and could not be separated without significant time and effort, the government seized all of the defendant's records in their entirety.[65] The court noted that as a general rule, only items specified in the warrant may be seized.[66] But, they recognized the plain view doctrine to the warrant requirement as it existed before *Horton v. California* and the abrogation of the inadvertence requirement as an exception.[67] The rule that only items specified in a search warrant may be seized "is subject to an exception which permits the seizure of contraband or other incriminating evidence found inadvertently during the execution of a search warrant."[68]

The court adopted the first prong of Winick's test in an effort to curb the "wholesale *seizure* for later detailed examination of records not described in a warrant."[69] The court found that in the rare instances where documents are so intermingled that they cannot be separated onsite, "the Government and law enforcement officials generally can avoid violating [F]ourth [A]mendment rights by sealing and holding the documents pending approval by a magistrate of a

60 *Id.* at 890.
61 *Id.*
62 United States v. Tamura, 694 F.2d 591, 594–95 (9th Cir. 1982).
63 Regensburger, *supra* note 21, at 1159.
64 *Tamura*, 694 F.2d at 594.
65 *Id.* at 595.
66 *Id.*
67 *See supra* Part I.
68 *Tamura*, 694 F.2d at 595 n.1.
69 *Id.* (emphasis in original).

further search."[70] In this case, the court sought to temper the possibility of wholesale removal of intermingled documents by requiring oversight of a "neutral, detached magistrate."[71] Accordingly, the court found that seizure of documents not covered by the search warrant was unreasonable.[72]

In sum, prior to the Ninth Circuit's decision in *Comprehensive Drug Testing, Inc.*, the court was willing to reject a special approach to computer searches by upholding the seizure of electronic evidence in plain view that was not covered by the government's initial search warrant. Despite this trend, cases dealing with intermingled paper documents, such as *Tamura*, suggested that there may be limits to what the government could seize.

III. THE NINTH CIRCUIT'S EN BANC DECISION IN *COMPREHENSIVE DRUG TESTING, INC.*

In August of 2009, *U.S. v. Comprehensive Drug Testing, Inc.*, (hereinafter *CDT*) eliminated the plain view doctrine and imposed a host of other burdensome requirements on investigators, while citing practically no precedent or reasoning for its decision.

This case has a long history and complicated factual record. Beginning in August, 2002, the federal government instituted an investigation into the Bay Area Lab Cooperative (BALCO), which was suspected of providing steroids to professional baseball players.[73] That same year, Comprehensive Drug Testing, Inc. (CDT) administered a suspicionless drug testing program at the behest of Major League Baseball.[74] The results of the tests were to remain "anonymous and confidential."[75] CDT kept a list of players and their respective results.[76] During the BALCO investigation, the federal government discovered ten players who had tested positive for steroid use in the CDT program.[77] As a result, the government obtained a search warrant in the Central District of California, "authorizing the search of

70 *Id.* at 595–96; *see also* Regensburger, *supra* note 21, at 1159 ("The first prong of Winick's test is essentially an adoption of the intermingled document doctrine, first espoused in *United States v. Tamura*.").

71 *Tamura*, 694 F.2d at 596.

72 *Id.*

73 United States v. Comprehensive Drug Testing, Inc., 513 F.3d 1085, 1089 (9th Cir. 2008).

74 United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 993 (9th Cir. 2009).

75 *Id.*

76 *Id.*

77 *Id.*

CDT's facilities in Long Beach."[78] The warrant was limited to those ten players.[79]

The magistrate judge who issued the search warrant granted the government broad authority to seize practically any computer, data storage device, log, or related material found at CDT's facility, and to examine all data contained in that equipment.[80] At the same time, the magistrate also placed limits on the government's authority, requiring the government to "examine the computer equipment and storage devices at CDT to determine whether information pertaining to the ten identified players c[ould] be searched on-site in a reasonable amount of time."[81] The warrant also contained "restrictions on how the seized data were to be handled," and required that the initial data review and segregation be conducted by computer personnel other than the investigating case agents.[82] These computer personnel were responsible for ensuring the integrity of the search and preventing over-seizure, outside the warrant's scope.[83]

Instead of following the magistrate's orders, the district court in the Central District of California found that "[o]nce the items were seized, the requirement of the Warrant that any seized items not covered by the warrant be first screened and segregated by computer personnel was completely ignored."[84] The government copied the entire "Tracey Directory" from CDT's directory, which contained "information and test results involving hundreds of other baseball players and athletes engaged in other professional sports."[85] The case agent reviewed the entire directory himself and used information gleaned from that directory to obtain subsequent search warrants in Northern and Southern California, as well as Nevada.[86]

The district court 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."[87] In August, 2009, the Ninth Circuit Court of Appeals, sitting en banc, found that the government

78 *Id.*
79 *Id.*
80 *Id.* at 995.
81 *Id.* (alteration in original) (internal quotation marks omitted).
82 *Id.* at 995–96.
83 *Id.* at 996.
84 *Id.* (alteration in original) (internal citations omitted).
85 *Id.* (internal quotation marks omitted).
86 *Id.* at 997.
87 *Id.* at 993–94.

failed to file a timely appeal and upheld the district court's ruling based on the preclusive effect of the order.[88]

Despite the conclusive nature of these findings, the en banc panel decided to dispose of the government's arguments and implement a framework of its own. The government argued that it was not required to return the data it found concerning players other than the ten mentioned in the warrant since that evidence was "in plain view" in the Tracey Directory.[89] Ninth Circuit Chief Judge Alex Kozinski, "in a withering opinion for the 9-2 majority, accused investigators of trampling the privacy rights and reputations of hundreds of people who had done nothing to alert the authorities' suspicion."[90] The court rejected the government's plain view argument as "too clever by half," stating that the danger of accepting it would be to turn a "limited search for particular information into a general search," and would be in direct contravention of Ninth Circuit precedent in *Tamura*.[91] Everything the government wanted to seize would, "under this theory, automatically come into plain view."[92] If the court accepted the government's plain view argument, it would be condoning the "fishing" expeditions expressly prohibited by *Tamura*.[93]

The Ninth Circuit did not end its discussion there. Instead, focusing on the supreme importance of preserving the privacy of intermingled electronic materials, it chose to establish firm guidelines, unsupported by any authority[94] that must be followed by magistrate judges when dealing with electronic data. Those guidelines, which

---

88 *Id.* at 997.

89 *Id.*

90 *See* Shane Harris, *Cuffing Digital Detectives*, NAT'L J., Dec. 19, 2009, at 52 ("Kozinski's opinion amounts to a concise and forceful description of the unique threats to Fourth Amendment prohibitions on unlawful searches and seizures in the Information Age."); *see also* Orin Kerr, *Cuffing Digital Detectives,* THE VOLOKH CONSPIRACY (Dec. 20, 2009, 1:08 AM), http://volokh.com/2009/12/20/cuffing-digital-detectives/ (acknowledging the National Journal Magazine article).

91 *Comprehensive Drug Testing, Inc.*, 579 F.3d at 998; *see also* United States v. Tamura, 694 F.2d 591, 597 (9th Cir. 1982) ("Under the circumstances of the present case, where the Government's wholesale seizures were motivated by considerations of practicality rather than by a desire to engage in indiscriminate 'fishing,' we cannot say, although we find it a close case, that the officers so abused the warrant's authority that the otherwise valid warrant was transformed into a general one, thereby requiring all fruits to be suppressed.").

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

93 *Tamura*, 694 F.2d at 597.

94 *See* Orin Kerr, *Ninth Circuit Considers Super-En-Banc for* Comprehensive Drug Testing, THE VOLOKH CONSPIRACY (Nov. 5, 2009, 5:39 PM), http://volokh.com/2009/11/05/ninth-circuit-considers-super-en-banc-for-comprehensive-drug-testing/ [hereinafter, Kerr, *Ninth Circuit Considers Super-En-Banc*] (noting that the guidelines were announced "without any apparent authority or even a case or controversy").

combined both Winick's and Kerr's approaches to computer searches, stated that:

> 1. Magistrates should insist that the government waive reliance upon the plain view doctrine in digital evidences 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, it must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant.
>
> 3. Warrants and subpoenas must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other judicial fora.
>
> 4. The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that 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.[95]

In response to this decision, the Department of Justice petitioned for "super en banc" rehearing.[96] On November 4, 2009, the Ninth Circuit entered an order requesting that the parties file briefs addressing whether this case should be reheard, yet again, by the court—this time by all thirty two judges on the Ninth Circuit.[97] The rationale for this decision can be summed up by the following: "in the unlikely event that six judges might command a majority of an eleven-judge en banc court and express a view inconsistent with the views of the other twenty one active judges on the court, the circuit rules provide for review by the full court upon the request of any

---

95 *Comprehensive Drug Testing, Inc.*, 579 F.3d at 1006 (internal citations omitted).

96 *See* Orin Kerr, *Ninth Circuit Considers Super-En-Banc, supra* note 94 ("[T]he Ninth Circuit entered an order [on November 4th, 2009] addressed to the parties in the case asking them to brief whether the case should be reheard by the full en banc court . . . ."). As of August 16, 2010, the Ninth Circuit had not ruled on whether to conduct an en banc rehearing. Orin Kerr, *Whatever Happened to the Request for Super-En-Banc Rehearing in* CDT*?*, THE VOLOKH CONSPIRACY (Aug. 16, 2010, 6:15 PM), http://volokh.com/2010/08/16/whatever-happened-to-the-request-for-super-en-banc-rehearing-in-cdt/ [hereinafter Kerr, *Whatever Happened*].

97 Order No. 05-10067, United States v. Comprehensive Drug Testing, 579 F.3d 989 (9th Cir. 2009) (D.C. No. MISC-04-234-SI) (Nov. 4, 2009); *see also* Orin Kerr, *Ninth Circuit Considers Super En Banc* ("The Ninth Circuit has so many active judges that its *en banc* panels consist of only about a third of its active judges."). Thus, the first en banc hearing consisted of only 11 judges.

judge."[98] Notably, this has never occurred since the limited en banc rule was adopted by the court in 1980.[99]

On November 23, 2009, the Department of Justice, led by then Solicitor General Elena Kagan, filed its Brief in Support of Rehearing en banc by the full court.[100] The Justice Department primarily took issue with the new guidelines promulgated by the Ninth Circuit, stating that "computer searches have ground to a complete halt" in many jurisdictions as a result of the court's decision.[101] The brief further argued that "[t]he en banc panel stepped outside the proper role of an Article III court when it set forth detailed protocols that purport to bind, and that are being understood as binding, magistrate and district judges in future cases."[102] The Justice Department argued that the seminal issues should be resolved in actual cases involving computer searches, not through "guidance" that "magistrate judges must be vigilant in observing."[103]

The Justice Department warned of the potentially damaging effects *CDT*'s strict protocols could have on the furtherance of effective investigations of electronic data. The burden of following the procedures outlined in that decision would largely fall on the federal authorities who are responsible for conducting criminal investigations and could lead to drastically increased investigatory costs.[104] The effects might be passed on to state authorities, who would be forced to effectuate what federal authorities could not, since the state police would be unconstrained by the holding in *CDT* and thus more easily able to conduct computer searches.[105] Further, one commentator ob-

98 Statement of Circuit Judge Alex Kozinski to the House Judiciary Subcommittee on Courts Regarding H.R. 2723 (Oct. 21, 2003).

99 *Id.*

100 Brief for the United States in Support of Rehearing En Banc by the Full Court at 1, United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989 (9th Cir. 2009) (Nos. 05-10067, 05-15006, 05-55354).

101 *Id.*

102 *Id.* at 2.

103 *Id.*

104 *See id.* at 16.; Rob Lee, *Sweeping 9th Circuit Decision Regarding Law Enforcement Officer Computer Forensics*, SANS COMPUTER FORENSICS AND E-DISCOVERY WITH ROB LEE (Aug. 27, 2009, 3:10 AM), http://blogs.sans.org/computer-forensics/2009/08/27/sweeping-9th-circuit-decision-regarding-law-enforcement-officer-computer-forensics/ (arguing that increased costs could come in the form of governmental agencies being forced to expand their personnel to include computer specialists, or to hire independent third parties at a substantial cost); *see also* United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1013 (9th Cir. 2009) (Callahan, J., dissenting) (noting that these cost implications could also have a large effect on the ability of smaller police departments to do their jobs).

105 Brief for the United States in Support of Rehearing En Banc by the Full Court at 6, United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989 (9th Cir. 2009) (Nos. 05-10067, 05-15006, 05-55354).

served that "[i]f law enforcement officials had to stop their investigation and seek judicial oversight every time they seized a computer, law enforcement would grind to a halt in the United States . . . . [This would be like requiring] . . . law enforcement officials to impound the contents of a desk or a car before being allowed to search it."[106]

The government also noted that an FBI forensic analyst in the District of Arizona had expressed concern that he would "need many months to learn a complex national security case before attempting to segregate responsive and non-responsive data on a seized computer," as required by the procedures in *CDT*.[107] That decision's protocols could also lead to missed opportunities to discover evidence. In the same rehearing brief, the Justice Department cited a case in the Western District of Washington where federal agents who were investigating a potential child rape case did not obtain a warrant to search the defendant's computer, despite evidence of incriminating images, "because of concerns that any evidence discovered about other potential victims could not be disclosed by the filter team."[108]

IV. NINTH CIRCUIT'S AMENDED *COMPREHENSIVE DRUG TESTING, INC. PER CURIAM* OPINION

On September 13, 2010, almost a year after the Department of Justice petitioned for rehearing, the Ninth Circuit issued a new opinion denying an en banc rehearing, but amending its original opinion to remove the challenged guidelines from the majority opinion.[109] The amended decision did not change the outcome of the case: the court found, once again, that the government had ignored the dictates of the warrant and *Tamura*, and the decision to force them to return the test results for the baseball players not covered by

106 Regensburger, *supra* note 21, at 1204.

107 Brief for the United States in Support of Rehearing En Banc by the Full Court at 6, United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989 (9th Cir. 2009) (Nos. 05-10067, 05-15006, 05-55354).

108 *Id.* at 6–7.

109 *See* United States v. Comprehensive Drug Testing, Inc., Nos. 05-11067, 05-15006, 05-55354, 2010 WL 352947 (9th Cir. Sept. 13, 2010) (Kozinski, J., concurring) (providing future guidance on how to deal with electronically stored data searches); Orin Kerr, *Ninth Circuit Balks in BALCO Case: Denying Super En banc in* United States v. Comprehensive Drug Testing *but Amending Opinion to Remove Challenged Section*, THE VOLOKH CONSPIRACY (Sept. 13, 2010, 2:04 PM), http://volokh.com/2010/09/13/ninth-circuit-balks-in-balco-case-denying-super-en-banc-in-united-states-v-comprehensive-drug-testing-but-amending-opinion-to-remove-challenged-section/ [hereinafter Kerr, *Ninth Circuit Balks in BALCO Case*] ("[I]t seems that the weird mandatory rules part of Judge Kozinski's initial en banc majority opinion in *CDT* is now just part of a Kozinski concurrence to what has been relabeled a *per curiam* majority opinion.").

the warrant was upheld.[110] The court acknowledged that the government likely attempted to comply with *Tamura* by seeking "advance authorization for sorting and segregating the seized materials off-site" but "[o]nce the items were seized, the requirement of the Warrant that any seized items not covered by the warrant be first screened and segregated by computer personnel was completely ignored."[111] The court reiterated the challenges faced by modern law enforcement in the wake of advancing technology.[112] "This pressing need of law enforcement for broad authorization to examine electronic records," the court noted, "creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant."[113] In cases involving intermingled electronic data, the court made it clear that the approach in *Tamura* is to govern.[114] Finally, the court closed the door to any future petitions in this case, stating that "[t]he revised opinion filed concurrently herewith shall constitute the final action of the court."[115]

Judge Kozinski's guidance, including the court's insistence "that the government waive reliance upon the plain view doctrine in digital evidence cases,"[116] largely remained unchanged, but that guidance lost the support of a majority of the Ninth Circuit and was relegated to the concurrence in this new opinion.[117] Consequently, the suggested guidelines are no longer Ninth Circuit law. Kozinski's concurrence now acknowledges the non-binding nature of these guidelines, but still stresses their importance and relevance, noting that "the guidance . . . offers the government a safe harbor . . . . District and magistrate judges must exercise their independent judgment in every case, but heeding this guidance will significantly increase the likelih-

---

110 *Comprehensive Drug Testing, Inc.*, 2010 WL 3529247, at *6 ("We can and do uphold these findings based on the preclusive effect of the Cooper and Illston Orders.").

111 *Id.* at *5 (alteration in original).

112 *Id.* at *12 ("Law enforcement today thus has a far more difficult, exacting and sensitive task in pursuing evidence of criminal activities than even in the relatively recent past.").

113 *Id.*

114 *Id.* at *13 ("*Tamura* has provided a workable framework for almost three decades, and might well have sufficed in this case had its teachings been followed. We have updated *Tamura* to apply to the daunting realities of electronic searches.").

115 *Id.* at *1.

116 *Id.* at *16.

117 Kozinski's concurrence is joined by four other judges—Judges Andrew Kleinfeld, William Fletcher, Richard Paez, and Milan Smith, Jr. His guidelines lost the support of Judges Marsha Berzon, Susan Graber, and Kim McLane Wardlaw. *See* Ginny LaRoe, *Steroids in Baseball: 9th Circuit Backtracks on Electronic Search Rules*, LAW.COM (Sept. 14, 2010), http://www.law.com/jsp/law/LawArticleFriendly.jsp?id=1202472007634 (explaining that the Ninth Circuit backtracked from the privacy guidelines issued in the original en banc opinion).

ood that the searches and seizures of electronic storage . . . will be . . . lawful."[118] There can be no doubt that the government's actions, particularly in the Ninth Circuit, will continue to be shaped and influenced by Kozinski's guidelines, especially with the assurance that complying with them will provide the government with a "safe harbor."

A. Problems with Judge Kozinski's Electronic Search Guidelines

A lengthy portion of this Comment in an earlier draft form was dedicated to how and why Judge Kozinski's guidelines should be removed from the majority's decision. Though these guidelines are no longer Ninth Circuit law, they remain problematic and, more importantly, unconstitutional. While the court did not give any explanation for its decision to remove the guidelines from the *per curiam* opinion, the decision was nevertheless correct. The guidelines were both beyond the scope of Article III and in direct contravention to Supreme Court precedent applying the plain view doctrine to warranted searches.

i. Guidelines Were Beyond the Scope of Article III

Article III of the U.S. Constitution vests the federal courts with "judicial [p]ower" and grants the courts jurisdiction to exercise it in various "cases" and "controversies."[119] As the Justice Department points out in its brief for rehearing, the controversial procedures set forth by Judge Kozinski go far beyond the resolution of any "case" or "controversy."[120] The detailed guidance set forth by the Ninth Circuit was unnecessary to the resolution of the case at hand. In the en banc *CDT* opinion, the court noted the "preclusive effect" of the lower court orders, but went on with its procedural recommendations because "the matter is important, and to avoid any quibble about the proper scope of preclusion."[121] Nevertheless, "[i]n issuing this wide-ranging and detailed 'guidance' about subjects that were unnecessary

---

118 *Comprehensive Drug Testing, Inc.*, 2010 WL 3529247, at *14.

119 U.S. CONST. art. III ("The judicial Power of the United States, shall be vested in one supreme Court, and in such inferior Courts as the Congress may from time to time ordain and establish.").

120 Brief for the United States in Support of Rehearing En Banc by the Full Court at 4, United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989 (9th Cir. 2009) (Nos. 05-10067, 05-15006, 05-55354). ("[T]he en banc panel reached well beyond the issues before it and purported to establish binding new procedures . . . .").

121 United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 997 (9th Cir. 2009).

to resolve the particular cases before it, the en banc panel departed from the proper role of an Article III court."[122]

Rather than resolving a particular "case" or "controversy," as required by Article III, the Ninth Circuit in its original en banc opinion issued an advisory opinion. The Supreme Court "has used the term 'advisory opinion' to embrace . . . '[a]ny opinion, or portion thereof, not truly necessary to the disposition of the case at bar (that is, dicta)'."[123] The prohibition against advisory opinions has been deemed "the oldest and most consistent thread in the federal law of justiciability."[124] According to *Preiser v. Newkirk*, "a federal court has neither the power to render advisory opinions nor to decide questions that cannot affect the rights of litigants in the case before them," yet, by issuing the detailed guidelines for all future computer searches, this is precisely what the Ninth Circuit had done.[125] To be sure, the guidelines proposed by the Ninth Circuit "would ordinarily be handled through the legislative process, rather than through a heavy-handed judicial edict," such as this one.[126]

ii. Guidelines Departed From Precedent Allowing Warrantless Searches of Objects in Plain View

The five guidelines place a heavy burden on officers, police departments, and the federal government that go far beyond the textual requirements of the Fourth Amendment. The plain view exception to the warrant requirement, as described by the Supreme Court, applies when officers "have a warrant to search a given area for specified objects, and in the course of the search come across some other article of incriminating character."[127] While there are valid concerns regarding the dangers of the plain view doctrine's applicability to computer searches[128] and turning particularized search warrants into

---

122 Brief for the United States in Support of Rehearing En Banc by the Full Court at 4–5, United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989 (9th Cir. 2009) (Nos. 05-10067, 05-15006, 05-55354).

123 Richard H. Fallon, Jr. et al, THE FEDERAL COURTS AND THE FEDERAL SYSTEM 56 (6th ed. 2009) (quoting Even Tsen Lee, *Deconstitutionalizing Justiciability: The Example of Mootness*, 105 HARV. L. REV. 603, 644–45 (1992)).

124 Charles Alan Wright & Mary Kay Kane, LAW OF FEDERAL COURTS 65 (6th ed. 2002).

125 Brief for the United States in Support of Rehearing En Banc by the Full Court at 5, United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989 (9th Cir. 2009) (Nos. 05-10067, 05-15006, 05-55354).

126 Thomas R. Eddlem, *Fourth Amendment Under Siege Again*, NEW AMERICAN, Nov. 28, 2009, at 2.

127 Horton v. California, 496 U.S. 128, 135 (1990).

128 *See supra* Part I.

general search warrants, the wholesale elimination of the plain view doctrine has no basis in the law and is in direct contradiction to Supreme Court precedent allowing the use of the plain view doctrine in the context of warranted searches.

The Ninth Circuit effected a wholesale elimination of the doctrine with respect to computer searches without providing any manner of legal support for its ruling. The dissent in the *per curiam* opinion noted "the suggested protocols essentially jettison the plain view doctrine in digital evidence cases . . . . This is put forth without explaining why the Supreme Court's case law or our case law dictates or even suggests that the plain view doctrine should be entirely abandoned in digital evidence cases."[129]

Moreover, not only is the elimination of the plain view doctrine in contradiction to Supreme Court precedent, it also sidesteps Ninth Circuit precedent. As previously noted, the Ninth Circuit in *United States v. Adjani*, *United States v. Giberson* and *United States v. Wong*, refused to suppress evidence found in plain view during the course of a valid computer search.[130]

V. ALTERNATIVES TO ELIMINATING THE PLAIN VIEW DOCTRINE

Judge Kozinski calls for the total elimination of the plain view doctrine during computer searches. This approach is far too drastic and far-reaching—and, more importantly, flies in the face of important constitutional principles. The Ninth Circuit undoubtedly acknowledged this by amending its opinion in *CDT*. While Judge Kozinski's approach remained part of the majority opinion in *CDT*, several other circuits, including the Fourth and the Seventh, expressly failed to follow it.[131] Those circuits—as well as the Tenth Circuit—demonstrate that the plain view doctrine can and should be applied to computer searches.

---

129 United States v. Comprehensive Drug Testing, Inc., Nos. 05-10067, 05-15006, 05-55354, 2010 WL 352947 (9th Cir. Sept. 13, 2010), at *20.

130 *See* United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1011 (9th Cir. 2009); United States v. Giberson, 527 F.3d 882, 884 (9th Cir. 2008) (refusing to suppress evidence of child pornography found in a search for false identification card); United States v. Adjani, 452 F.3d 1140, 1150 (9th Cir. 2006) (rejecting the defendant's claim that emails seized were outside the scope of the warrant because they implicated her in another crime not covered by the search warrant); United States v. Wong, 334 F.3d 831, 833 (9th Cir. 2003) (applying the plain view doctrine to murder investigation case in the context of a computer search and the discovery of child pornography).

131 *See infra* Part V.A-B.

A. The Fourth Circuit's Approach

In the wake of the original en banc decision in *CDT*, several circuit courts had already expressed their reluctance to prohibit the use of the plain view doctrine. For example, the Fourth Circuit in *United States v. Williams* used the closed container approach to computer searches to find that the seizure of images portraying child pornography was justified by the plain view exception to the warrant requirement.[132] The warrant authorized a search of the defendant's computers for evidence relating to the state law crimes of making threats and computer harassment.[133] During the course of the search of the defendant's computer and accompanying electronic media, one of the officers encountered over one thousand images in "thumbnail view," some of which were sexually explicit.[134] The defendant challenged the authority of the officers to seize these images under the warrant.[135] The court reasoned that in order to properly conduct the search, the warrant implicitly "authorized officers to open each file on the computer and view its contents, at least cursorily, to determine whether the file fell within the scope of the warrant's authorization."[136] The court expressed concerns about the difficulties of computer searches—namely, that an effective computer search cannot be limited to reviewing files based on labeling, file name, or extension, which can be easily changed or hidden.[137] According to the Fourth Circuit, "[o]nce it [was] accepted that a computer search must, by implication, authorize at least a cursory review of each file on the computer, then the criteria for applying the plain-view exception [were] readily satisfied."[138]

The conception of the plain view doctrine as articulated by the Fourth Circuit is equally as radical as the Ninth Circuit's "safe harbor"

---

132 United States v. Williams, 592 F.3d 511, 522 (4th Cir. 2010) ("And so, in this case, any child pornography viewed on the computer or electronic media may be seized under the plain-view exception.").

133 *Id.* at 521.

134 *Id.* at 516.

135 *Id.* at 516, n.2.

136 *Id.* at 521.

137 *Id.* at 522 ("To be effective, such a search could not be limited to reviewing only the files' designation or labeling, because the designation or labeling of files on a computer can easily be manipulated to hide their substance.").

138 *Id.* The *Williams* court rejected the defendant's argument that the images must have been found by the officers inadvertently in order to satisfy the plain view doctrine. *Id.* at 522–23 ("This argument, however, cannot stand against the principle. . . that the scope of a search conducted pursuant to a warrant is defined *objectively* by the terms of the warrant and the evidence sought, not by the *subjective* motivations of an officer."); *see also infra* Part V.B.

elimination of the plain view doctrine, though at the opposite end of the spectrum.[139] The Fourth Circuit, like the Ninth, offers a bright line rule: "a warrant for one file is a warrant for all files on a device."[140] Courts should be hesitant to accept this approach to computer searches. Treating a hard drive, floppy disk, or computer as a "container," as the Fourth Circuit did, is problematic for its broad-reaching implications. Essentially, this standard is analogous to treating a house as a "container," by turning a warrant to obtain evidence for a particular crime into a blanket license to ransack an entire house in a search for that evidence. Following this method, a warrant to search a computer for a specific crime is likely to become a general warrant—precisely what the Fourth Amendment was written to prohibit. This approach fails to protect a suspect's privacy, or the privacy of others with intermingled data.[141]

B. A Better Approach in the Tenth and Seventh Circuits: Restoring the Inadvertence Requirement to the Plain View Doctrine

The Tenth and Seventh Circuits have developed an approach to computer searches that allows for the use of the plain view doctrine in limited circumstances. The "virtual file" approach has been adopted by these two circuits.[142] According to this approach:

> the relevant unit of search . . . is an individual file. If you analogize a computer hard drive to a suitcase, each file is . . . its own zippered pocket in the suitcase. A computer is like a container that stores thousands of individual containers in the form of discrete files.[143]

In assessing the reasonableness of a seizure, it is first asked whether or not that individual file is outside the scope of the warrant. If yes, it is then asked whether that file was discovered inadvertently.

---

139 United States v. Comprehensive Drug Testing, Inc., Nos. 05-11067, 05-15006, 05-55354, 2010 WL 352947 (9th Cir. Sept. 13, 2010), at *14 ("The guidance below offers the government a safe harbor, while protecting the people's right to privacy and property in their papers and effects.").

140 Moshirnia, *supra* note 41, at 622.

141 *Id.* at 622–23 ("[T]his approach could prove disastrous in the medical or corporate contexts because it is likely [to] allow searches of individuals' private information that is only tenuously related to the criminal investigation.").

142 Kerr, *Searches and Seizures*, *supra* note 17, at 554 (describing three basic options for defining the zone of a computer search: "the zone could be defined by the contents of a virtual file, the physical storage device, or the exposed data. If the zone is a device, then opening it searches all of its contents. If the zone is a file, then that file is searched but the rest of the computer is unsearched. Finally, if the zone is the exposed data itself, then exposure of data leaves all unexposed information unsearched").

143 *Id.* at 555.

Rather than effecting a wholesale elimination of the plain view doctrine, the case law in the Tenth and Seventh Circuits provides a viable and less drastic alternative where "deliberate overreaching" by the police through the use of the plain view doctrine is prevented.[144] Evidence can be seized "outside the warrant only if it was uncovered pursuant to a good faith search for evidence described in the warrant."[145] In effect, these circuits created a more workable standard that ensures against morphing computer searches into grants of general warrants by giving force to the historic "inadvertence requirement" of the plain view doctrine.[146]

The Tenth Circuit first tackled the issue of what plain view means in the context of computer searches in 1999.[147] In *United States v. Carey*, the Tenth Circuit found that a warrantless search of picture files on the defendant's computer was not justified under the plain view doctrine.[148] In that case, a police officer was searching a computer for evidence of drug trafficking, and "after noting several files with a sexually suggestive name and with a 'jpg' file name extension, suggesting an image file, the officer began looking through the 'jpg' files."[149] In rejecting the plain view doctrine in this case, the court reasoned that "[t]he government's argument [that] the files were in plain view [was] unavailing" because after opening one image file and finding evidence of child pornography, the officer continued to open subsequent image files, thereby obviating the inadvertence requirement.[150]

The detective was aware that he was acting without judicial authority (and outside of the scope of the warrant) when he abandoned his search for evidence of drug dealing and began looking through "jpg" files with "sexually suggestive titles."[151] Thus, the court suppressed the evidence since the detective could not have "inadvertently discov-

144 *See* Kerr, *Digital Evidence, supra* note 17, at 316–17 (citing *United States v. Carey* as an example of a case that has narrowed the potential reach of the plain view doctrine in computer searches by "focusing on the investigator's subjective intent").

145 *Id.* at 317.

146 *See* discussion *supra* Part I. The Tenth Circuit has acknowledged that the "inadvertence requirement" has not been mandated by the Fourth Amendment since *Horton v. California*. Nevertheless, the Supreme Court continues to recognize the supreme importance and relevance of "inadvertence" in plain view searches. *See* United States v. Carey, 172 F.3d 1268, 1276–77 (10th Cir. 1999) (Baldock, J., concurring) (finding that child pornography discovered inadvertently while opening a defendant's individual computer files could not be admitted into evidence as the result of a plain view search).

147 *See Carey*, 172 F.3d at 1273.

148 *Id.*

149 *Plain View Doctrine*, 84 A.L.R. 58, § 13a (5th ed. 2000).

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

151 *Id.* at 1270–71.

ered" the contents of the image files.[152] In *U.S. v. Walser*, the Tenth Circuit distinguished the facts of *Carey* and reaffirmed the inadvertence requirement.[153]

Most recently, the Seventh Circuit in *United States v. Mann* explicitly refused to extend the protocols outlined in the en banc majority opinion in *CDT* to the facts of that case and adopted the *Carey* inadvertence requirement.[154] The *Mann* court took a similar approach to the Tenth Circuit and asked "whether the agent knew or should have known that the file opened was outside the scope of the warrant."[155] In that case, the government executed a warrant to search the defendant's computer for evidence of "voyeurism" and in the process of searching the files, the government encountered evidence of child pornography.[156] The defendant moved to suppress the evidence of child pornography alleging that the evidence exceeded the scope of the warrant.[157] The court noted that "[o]nce the [child pornography] files had been flagged" by the filtering software, the detective "knew (or should have known) that files in a database of known child pornography images would be outside the scope of the warrant."[158] The defendant urged the Seventh Circuit to adopt the Ninth Circuit's approach in *CDT* in refusing to recognize that the child pornography images were found in plain view during the officer's search of the

152 *Id.* at 1273.

153 United States v. Walser, 275 F.3d 981, 987 (10th Cir. 2001) ("In *Carey*, the officer was engaged in a similar search for electronic records of drug dealing. As in this case, the officer in *Carey* inadvertently discovered the first image of child pornography while searching for documents relating to drug activity. In *Carey*, however, after opening the first file, the officer's conduct was the opposite of that which occurred in the present case. . . . Had Agent McFarland conducted a more extensive search than he did here by rummaging in folders and files beyond those he searched, he might well have exceeded the bounds of the warrant and the requirements of *Casey* [sic]. The fact of the matter, however, is that no such wholesale searching occurred here. Agent McFarland showed restraint by returning to the magistrate for a new warrant before commencing a new search for evidence of child pornography.") (citations omitted).

154 United States v. Mann, 592 F.3d 779 (7th Cir. 2010) (finding that evidence of child pornography inadvertently discovered during a computer file search should not be suppressed when the search was conducted within the scope of an existing warrant, and the search was not abandoned following discovery of the material in question).

155 *See* Orin Kerr, *Plain View for Computer Searches Generates Two Circuit Splits in Two Days*: United States v. Williams *and* United States v. Mann THE VOLOKH CONSPIRACY (Jan. 21, 2010, 11:41 PM) http://volokh.com/2010/01/21/plain-view-for-computer-searches-generates-two-circuit-splits-in-two-days-united-states-v-williams-and-united-states-v-mann/.

156 *Mann*, 592 F.3d at 781 (noting that the case agents used software employing a filter to view the files tagged by an "Alert," which flags "those files identifiable from a library of known files previously submitted by law enforcement—most of which are images of child pornography").

157 *Id.*

158 *Id.* at 784.

computer files for voyeurism. In declining to accept the Ninth Circuit's approach, the court stated that "[a]lthough the Ninth Circuit's rules provide some guidance in a murky area, we are inclined to find more common ground with the dissent's position that jettisoning the plain view doctrine entirely in digital evidence cases is an 'efficient but overbroad approach.'"[159]

Courts should adopt the approach of the Tenth and Seventh Circuits when determining whether seizure of electronic data is reasonable under the Fourth Amendment. This approach is the only one that has successfully treaded the line between completely eliminating the plain view doctrine and turning a warrant to search a computer into a wholesale license to search and potentially seize a computer's entire contents.

Indeed, an approach which treats a file as a container and applies the inadvertence requirement could have addressed the general concerns of the Ninth Circuit inherent to computer searches that general warrants will result when officers are allowed to seize and search computers unchecked through the use of the plain view doctrine. General warrants are not a possibility since the computer is not the "container." Instead, each file on a computer's hard drive is the "container" for purposes of the warrant. Thus, a warrant to search a computer is not treated like a warrant to search the entire contents of a suitcase. A court, following this approach, must ask whether each file was opened in an attempt to comply with the warrant, not just whether the computer was seized pursuant to the warrant. Then, if an officer wishes to seize a file on a computer through the plain view doctrine, he must show that he came across the evidence in that file inadvertently, i.e., in good faith, and not in an attempt to uncover evidence outside the scope of the warrant.

Further, treating each file as a separate container will preserve a defendant's (and any third party's) privacy interest in the documents being searched that are not subject to the warrant by guaranteeing that an officer's search of a computer is narrowly tailored. An officer must reasonably believe that a file is related to the target of a search before he can open it. If an officer does so and still comes across information not covered by the warrant, that information may only be seized if it is discovered inadvertently. These extra protections will narrow the scope of electronic data that can reasonably be seized with

159 *Id.* at 785 (citation omitted). The Seventh Circuit went on to say, "[a]s the dissent recognizes, 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." *Id.*

a warrant, which, in turn, will help to preserve the privacy interests of those involved.

Critics of this approach note that courts are generally reluctant to engage in an analysis of an officer's subjective intent.[160] Courts would necessarily have to do so in assessing whether an officer came across electronic data inadvertently. This is undoubtedly difficult, yet not impossible. Certainly, the court in *Carey* did just that. As the complexity of technology and the sophistication of criminals increase, so too does the likelihood that an officer will need to search all, or mostly all, of the files on a computer to be certain that he has completed his search. In light of this, the intent of the officer becomes much more important in assessing the reasonableness of a seizure of electronic information and whether it comports with the Fourth Amendment and the plain view doctrine. It may be the only way to both preserve the integrity of the plain view exception to the warrant requirement and prevent general warrants. Any difficulties in conducting an analysis of an officer's subjective intent are far outweighed by these benefits.

VI. THE PLAIN VIEW DOCTRINE AND COMPUTER SEARCHES AFTER THE *COMPREHENSIVE DRUG TESTING, INC.* AMENDED *PER CURIAM* OPINION

In the wake of the Ninth Circuit's recent *per curiam* opinion, the plain view doctrine's place in the realm of intermingled data remains uncertain. While this new opinion has most likely eliminated the possibility of certiorari to the Supreme Court, Judge Kozinski is undoubtedly correct when he notes that this issue is "important and likely often to arise again."[161] The Ninth Circuit no longer mandates that the government waive reliance on this doctrine in computer searches, yet it is unclear how and to what extent the government may use it. The *per curiam* opinion does not expressly disavow use of the plain view doctrine, though it does reject the government's attempts in this instance as "too clever by half."[162] The case agent in

160 *See Recent Cases*, *Fourth Amendment—Plain View Doctrine—En Banc Ninth Circuit Holds that the Government Should Waive Reliance on Plain View Doctrine in Digital Contexts*—United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989 (9th Cir. 2009) (en banc), 123 HARV. L. REV. 1003, 1009 (2010) ("While the virtual file approach is preferable to eliminating the plain view doctrine altogether, there is at least one significant drawback: admissibility of evidence outside the scope of the warrant hinges primarily on the investigating agent's subjective intent, which may be impossible to discern with certainty.").

161 United States v. Comprehensive Drug Testing, Inc., Nos. 05-10067, 05-15006, 05-55354, 2010 WL 3529247 (9th Cir. Sept. 13, 2010), at *14 (*per curiam*) (Kozinski, J., concurring).

162 *Id.* at *6.

CDT expressly disregarded the instructions in the search warrant when he did not allow computer forensic personnel to examine and segregate the data but instead did it himself.[163]

Still, the question remains: when dealing with intermingled electronic data, when a search warrant provides no guidance, is the plain view exception to the warrant requirement compatible with the procedures dictated by *Tamura*?[164] Undoubtedly, yes—at least under certain circumstances. The interaction between the two doctrines is complicated and made even more so by the abrogation of the inadvertence requirement in *Horton* in 1990. *Tamura* dictates that evidence outside the scope of a warrant generally may not be seized. Thus, when an officer determines that data is so intermingled it cannot feasibly be sorted onsite, that data should be sealed and held until a magistrate can determine how to proceed.[165] When *Tamura* was originally decided in 1982, the Ninth Circuit contemplated a situation in which an officer executing a search warrant inadvertently identified evidence outside the scope of the warrant. In that case, according to *Tamura*, it was possible for a reasonable seizure of evidence to include that inadvertently discovered evidence.[166]

In *CDT*, the government knew prior to the execution of the search warrant that electronic documents were so intermingled that they would need to be seized in full and sorted off site. In situations like this, *Tamura* dictates that the government should apply to the magistrate ahead of time for permission to seize the data in full. But, when *Tamura* was decided in 1982, none of the intermingled documents that fell outside of the warrant's scope could be seized and used as evidence in another crime under the plain view exception because their discovery was not inadvertent.

Since *Horton* and the abrogation of the inadvertence requirement, theoretically everything outside the scope of the warrant found while searching through intermingled data on a computer could come into plain view. This is true even if the officer knows with a high degree of certainty, as he did in *CDT*, that he will find inculpatory evidence not covered by the warrant. This was the fear of the court in the *per curiam CDT* opinion:

---

163 *Id.* at *5.

164 *See id.* at *13 ("We have updated *Tamura* to apply to the daunting realities of electronic searches.").

165 United States v. Tamura, 694 F.2d 591, 594–96 (9th Cir. 1982).

166 *Id.* at 595, n.1 ("This rule is subject to an exception which permits the seizure of contraband or other incriminating evidence found inadvertently during the execution of a search warrant.").

> The point of the *Tamura* procedures is to maintain the privacy of materials that are intermingled with seizable materials, and to avoid turning a limited search for particular information into a general search . . . . If the government can't be sure whether data may be concealed . . . without carefully examining the contents of every file . . . then everything the government chooses to seize will . . . automatically come into plain view. . . . Let's take everything back to the lab, have a good look around and see what we might stumble upon.[167]

When officers are aware that they will encounter intermingled electronic data prior to the execution of the search warrant, reinstating the inadvertence requirement as part of the plain view doctrine presents a solution that is consistent with *Tamura*. This approach will also serve to protect and preserve privacy rights, without completely eliminating the plain view doctrine.

Applying the inadvertence requirement to the facts of *CDT*, it is obvious that the officer's seizure of over one hundred names in the Tracey Directory cannot be justified by the plain view doctrine. There is strong evidence that the officer who searched the Directory knew that he would encounter test results for players other than the ten mentioned in the warrant. Not only did the seizing officer in *CDT* remark that his rationale for taking the entire Directory was to give him an opportunity to "briefly peruse it to see if there was anything above and beyond that which was authorized for seizure in the initial warrant,"[168] but the government applied to the magistrate judge before execution of the search warrant for advanced authorization to sort the intermingled data offsite.[169] It is likely that the officer seized the entire Directory in an attempt to ascertain which other baseball players had tested positive for steroid use. Applying the inadvertence requirement, it follows that the evidence pertaining to individuals other than the ten specifically mentioned in the search warrant could not have properly been admitted as evidence in court under the plain view doctrine. Thus, eliminating the plain view doctrine in its entirety is an unnecessary and overbroad solution to cases such as this.

VII. CONCLUSION

While the guidelines that were a controversial component of the decision in *CDT* have since been relegated to the concurrence of the Ninth Circuit's recently amended *per curiam* opinion, they are still key to understanding the complexities of searches and seizures of elec-

167 *Comprehensive Drug Testing, Inc.*, 2010 WL 3529247, at *6.

168 *Id.* at *23 (Kozinski, J., dissenting) (internal quotation marks omitted).

169 *Id.* at *5.

tronic data. Importantly, the total elimination of the plain view exception to the warrant requirement has been rejected by multiple circuits—the Fourth, Seventh, and Tenth circuits have all approved of its use. But, given the inherent differences between physical and computer searches and seizures, allowing officers to justify seizures beyond the scope of a search warrant by blindly relying on the plain view doctrine could easily result in massive over-seizing of data, as well as the possibility that specific warrants will become general ones. A preferable approach is to follow the Seventh and Tenth Circuits in adopting the "virtual file" approach and reinstating the inadvertence requirement. This approach should also be applied in cases like *CDT*, dealing with intermingled electronic data.

Since the amended opinion, it is unclear precisely how government officials in the Ninth Circuit will proceed while conducting searches of electronic data. Will they conform to the guidelines completely and abandon the use of the plain view doctrine in an effort to get a "safe harbor" in court? Or will they continue to rely on that doctrine and force the courts to address this question, yet again? Indeed, one thing is certain: though Judge Kozinski's controversial guidelines in the en banc decision in *U.S. v. Comprehensive Drug Testing, Inc.* were ultimately consigned to a non-binding concurrence, echoes of their impact will surely reverberate ad infinitum.