Loyola of Los Angeles Law Review

Volume 44
Number 2 *Winter 2011 - Symposium: Rebooting California: Initiatives, Conventions & Government Reform*

Article 15

1-1-2011

Mining for Manny: Electronic Search and Seizure in the Aftermath of United States v. Comprehensive Drug Testing

Kimberly Nakamaru
Loyola Law School Los Angeles, kimberly.nakamaru@lls.edu

MINING FOR MANNY: ELECTRONIC SEARCH AND SEIZURE IN THE AFTERMATH OF *UNITED STATES V. COMPREHENSIVE DRUG TESTING*

*Kimberly Nakamaru**

As a part of a federal investigation of the Bay Area Lab Cooperative (BALCO) for allegedly providing illegal steroids to professional baseball players, the U.S. government received a warrant to search Comprehensive Drug Testing, Inc.'s computers that contained confidential test results of ten players who they had probable cause to believe received steroids from BALCO. In 2010, the Ninth Circuit majority in United States v. Comprehensive Drug Testing, Inc. *held that the government executed an unconstitutional "dragnet" search by examining the entire computer directory containing the test results of all professional athletes rather than just the records of those players for whom the government had probable cause. Furthermore, Chief Judge Alex Kozinski, in what previously appeared in the 2009 Ninth Circuit majority opinion but is now in the 2010 concurrence, provided guidelines regarding how to conduct a lawful electronic search and seizure. This Note suggests that even though Kozinski's guidelines cannot technically constitute an advisory opinion because they are no longer binding Ninth Circuit law, they will likely have the same effect because they will still "advise" future legal actors' actions. Additionally, this Note argues that new legislation is necessary to strike the best balance between the government's interest in law enforcement and the right of the individual to be free from unreasonable search and seizure in the digital realm.*

* J.D. Candidate, May 2011, Loyola Law School Los Angeles; B.A., Anthropology, June 2006, Princeton University. I would like to thank Loyola Law School Los Angeles Professor Christopher Hawthorne; the editors and staff of the *Loyola of Los Angeles Law Review*, especially Sean Daley, Emma D'Onofrio, and Elena DeCoste Grieco; and my husband, David Pidancet, for their valuable guidance, critiques, and encouragement.

TABLE OF CONTENTS

I. INTRODUCTION

Baseball players are lying. Cooperstown is crying. The government is prying? On September 13, 2010, in *United States v. Comprehensive Drug Testing, Inc.* (*Comprehensive Drug Testing IV*),[1] a Ninth Circuit Court of Appeals ruling sent shockwaves through Major League Baseball: the names of 104 players who tested positive for steroids in 2003 should never have been seized in the first place.

While most members of the American public are acutely aware of the ignominiously public downfall of Alex Rodriguez, David Ortiz, and Manny Ramirez, very few realize that these and hundreds of other professional baseball players were promised that their test results would remain confidential pursuant to an agreement between Major League Baseball (MLB) and the Major League Baseball Players Association ("Players Association"). According to the agreement, the tests were to only serve as a generalized gauge of the extent of the steroid problem in professional baseball.

Enter Barry Bonds. As part of a federal investigation of the Bay Area Lab Cooperative (BALCO) for allegedly providing illegal steroids to professional baseball players, the government received a warrant to search computers containing records of the confidential test results of ten players (Bonds being one) who they had probable cause to believe received steroids from BALCO. Fine. Legal. Where the government went wrong, according to the Ninth Circuit, however, was in searching and seizing the entire computer directory containing the test results of *all* professional athletes (baseball and non-baseball) rather than just the records of those players for whom the government had probable cause.

An unconstitutional "dragnet" seizure as the Ninth Circuit decried? Or a practical necessity? The problem hinges on the fact that the ten players' records were intermingled with hundreds of other athletes' records contained in a computer file called the "Tracey Directory." Indeed, data stored on electronic storage devices such as computer hard drives present a unique dilemma for the courts: how should digital data—specifically, intermingled digital data—be treated for Fourth Amendment purposes? The resolution of this issue affects everyone who has personal data stored on electronic

1. 621 F.3d 1162 (9th Cir. 2010).

devices. Can the government seize your private medical records if it has probable cause to seize another patient's records? What about financial information? Personal e-mails?

Case law is flush with concrete rules governing searches and seizures of tangible objects in the physical realm, but this Note contends that such rules are attenuated and outdated when applied to the digital world. Computers are not like file cabinets; rifling through physical files is not like digitally searching computer files. Part II of this Note examines the history of Fourth Amendment search and seizure doctrine and compares physical and digital[2] search and seizure law. Next, it addresses the problem of intermingled physical documents as resolved by *United States v. Tamura*,[3] and explores the various approaches that courts have taken with respect to intermingled digital documents. Part III provides an in-depth description of the *Comprehensive Drug Testing IV* opinion. Part IV critiques *Comprehensive Drug Testing IV* and suggests that Chief Judge Kozinski cleverly issued the equivalent of an unconstitutional advisory opinion in his concurrence by suggesting guidelines for magistrates to follow when dealing with intermingled digital documents on electronic storage devices. Finally, in Part V, this Note recommends that a legislative solution would enable Congress to genuinely federalize privacy expectations and maintain a balance between federal and state power that favors the individual.

II. STATEMENT OF EXISTING LAW

A. History of Fourth Amendment Search and Seizure Doctrine

In order to understand the rules governing computer search and seizure, it is necessary to first have a basic understanding of the relevant Fourth Amendment history. The Fourth Amendment's origin can be traced to eighteenth-century England and colonial America when general warrants were used to search private homes for evidence of any crime.[4]

2. This Note uses the term "digital search and seizure law" interchangeably with the terms "computer search and seizure law" and "electronic search and seizure law." Likewise, the term "digital search" is used interchangeably with the terms "computer search" and "electronic search."

3. 694 F.2d 591 (9th Cir. 1982).

4. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 536 (2005); *see generally* NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH

Specifically, the English government commonly used general warrants to ransack citizens' homes and seize political materials that could allegedly be used to undermine the government.[5] In addition to seizing the allegedly libelous material, the government also indiscriminately removed private papers from private homes.[6] Early courts were particularly troubled by the seizure of private papers, prompting Lord Camden, in *Entick v. Carrington*,[7] to famously explain that "[p]apers are the owner's goods and chattels: they are his dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection."[8] Accordingly, one of the Fourth Amendment's original aims was to keep the government's sticky fingers away from citizens' private materials—materials that innocent people would want to keep secret, materials that would embarrass the citizen but would not be illegal to possess.[9]

In reaction to these privacy breaches and dragnet searches, the Framers enacted the Fourth Amendment to ensure that the new federal government lacked the power to execute such sweeping searches.[10] Accordingly, the Framers prohibited general warrants, meaning that "every search or seizure had to be *reasonable*, and a warrant could issue under the Fourth Amendment only if it particularly described the place to be searched and the person or thing to be seized."[11] Based on this history and on the textual

AMENDMENT TO THE UNITED STATES CONSTITUTION 79–105 (1937) (discussing the development of the Fourth Amendment from the Virginia Bill of Rights of 1776 to the adoption of the Fourth Amendment).

5. *See* Entick v. Carrington, (1765) 95 Eng. Rep. 807 (K.B.); 19 How. St. Tr. 1030; Wilkes v. Wood, (1763) 98 Eng. Rep. 489 (K.B.); 19 How. St. Tr. 1153.

6. *Entick*, 95 Eng. Rep. at 818; 19 How. St. Tr. at 1066.

7. 95 Eng. Rep. 807 (K.B.); 19 How. St. Tr. 1030.

8. *Id.*

9. *See* William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393, 402 (1995) (discussing how in the *Entick* and *Wilkes* cases the emphasis was on the private nature of an individual's papers). The protection of private information that is embarrassing but not illegal is relevant in the computer data context as well. Take the BALCO steroid scandal, for example. What if the records that the government seized dated back to 1989, before the Anabolic Steroids Control Act criminalized steroid use? Anabolic Steroid Control Act of 1990, H.R. 4658, 101st Cong. (2d Sess. 1990). Or, what if a person took human growth hormone (HGH) within the confines of a doctor-patient relationship but in contravention of a professional sports league policy? Such private and potentially humiliating material fits within the Framers' rationale for enacting the Fourth Amendment just as much as incendiary pamphlets criticizing the Crown did in the eighteenth century.

10. LASSON, *supra* note 4, at 94–95; Kerr, *supra* note 4, at 536.

11. Kerr, *supra* note 4, at 536 (emphasis added); *see also* U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable

requirement that searches and seizures be "reasonable," the U.S. Supreme Court has created a set of rules that balances the needs of law enforcement with the individual's interest in deterring abusive law enforcement practices.[12]

B. Physical Search and Seizure

Since the Fourth Amendment's enactment, the search of a home has been the archetypal scenario in a search and seizure case.[13] The rules of such a search are well settled.[14] The police lawfully may enter a home if they have a warrant or an exception to the warrant requirement exists. Absent these circumstances, the police's entrance into the house constitutes an unlawful search[15] that violates the inhabitants' reasonable expectation of privacy.[16] Once the police have lawfully entered, they can walk around any open spaces.[17] However, opening drawers or moving items triggers a new search that requires a warrant or an exception to the warrant requirement.[18]

Additionally, the police can take away, or seize, any evidence described in the warrant.[19] According to the Supreme Court, an unlawful seizure occurs when the government meaningfully interferes with an individual's possessory interest in property.[20] However, the seizing of physical evidence is considered

searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the person or things to be seized.").

12. Kerr, *supra* note 4, at 536; *see* William J. Stuntz, *Implicit Bargains, Government Power, and the Fourth Amendment*, 44 STAN. L. REV. 553, 553, 561–62 (1992).

13. *See* United States v. U.S. District Court (*Keith*), 407 U.S. 297, 313 (1972) ("[P]hysical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed . . . .").

14. Kerr, *supra* note 4, at 536.

15. *Smith v. Maryland* created a two-pronged "reasonable expectation of privacy test" for whether an unlawful Fourth Amendment search has occurred: (1) whether the individual by his conduct has "exhibited an actual (subjective) expectation of privacy," and (2) whether the individual's subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable.'" 442 U.S. 735, 740 (1979).

16. *See* Kyllo v. United States, 533 U.S. 27, 32–33 (2001).

17. *Cf.* Maryland v. Macon, 472 U.S. 463, 469 (1985) (stating that the police officer's examination of items that were "intentionally exposed to all who frequent the place of business" did not trigger a search).

18. *See* Arizona v. Hicks, 480 U.S. 321, 325 (1987).

19. Kerr, *supra* note 4, at 537.

20. United States v. Jacobsen, 466 U.S. 109, 113 (1984).

"reasonable" if the property is listed in the warrant.[21] The police can also remove other evidence that they come across in "plain view,"[22] provided that the incriminating nature of the evidence is "immediately apparent."[23]

C. Plain View Doctrine

Unlike other exceptions to the warrant requirement, the plain view doctrine only permits a warrantless *seizure*—not a warrantless search.[24] The landmark case *Horton v. California*[25] exemplifies a typical plain view scenario. In *Horton*, the defendant used a gun to rob the victim of jewelry and cash.[26] Accordingly, a police officer obtained a warrant to search the defendant's home for the stolen jewelry and cash.[27] During the search, however, the officer saw weapons in plain view and seized them.[28] The Supreme Court found that, despite not being specified in the warrant, the trial court properly admitted the weapons into evidence.[29]

In so holding, the Supreme Court clarified that the requirements of a lawful plain view seizure are that (1) the officer did not violate the Fourth Amendment in arriving at the place from which the evidence could be plainly viewed;[30] (2) the officer had a "lawful right of access to the object itself";[31] and (3) the incriminating nature of the evidence was "immediately apparent."[32]

One major policy concern that the plain view doctrine addresses is the risk of evidence destruction.[33] Under the facts of *Horton*, this

21. *Id.* at 113–14.

22. The term "plain view" means "open and visible to the naked eye." People v. Nickles, 88 Cal. Rptr. 763, 767 (Ct. App. 1970).

23. Horton v. California, 496 U.S. 128, 136 (1990) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 446 (1971)).

24. *Id.* at 133–34.

25. 496 U.S. 128.

26. *Id.* at 130.

27. *Id.* at 130–31.

28. *Id.* at 131.

29. *Id.* at 142.

30. *Id.* at 141.

31. *Id.* at 137. In other words, the item allegedly in plain view was observed while the officer was confining her activities to the permissible scope of the intrusion itself.

32. *Id.* at 136.

33. *See, e.g.*, Illinois v. Andreas, 463 U.S. 765, 780 (1983) (Brennan, J., dissenting); Coolidge v. New Hampshire, 403 U.S. 443, 466–67 (1971).

issue could have arisen had the police officer been required to return to the magistrate for a new warrant that allowed him to seize guns. During "the delay inherent in obtaining a warrant," an accused can easily hide, destroy, or, as argued in digital evidence cases, encrypt or booby-trap the evidence.[34] Returning to the magistrate not only jeopardizes the integrity of the evidence but also is inefficient.[35] Whether these overall policy aims are as gravely at issue in a plain view seizure of computer files is the subject of a new and ongoing debate that is colored, in large part, by the differences between physical and digital data.

D. Digital Search and Seizure

Application of the plain view doctrine and Fourth Amendment search and seizure law is problematic when it involves data stored on computers. Because Fourth Amendment search and seizure law evolved vis-à-vis physical spaces, such as buildings and file cabinets, the extent to which this physical framework fits the digital arena is unsettled. This issue comes into sharper relief with regard to whether government officials may search and seize "intermingled" digital documents: "documents that are outside the scope of a search warrant, but so intermingled with materials specified in the warrant that on-site separation would be impractical."[36]

1. Differences Between Physical and Computer Searches

Physical search and seizure is quite similar to computer search and seizure: in both instances, government officials attempt to locate and retrieve germane information hidden inside a closed canister.[37] However, the physical search and seizure procedures, which focus on entering and taking tangible evidence, are considerably different from computer search and seizure procedures, which function by locating and copying data.[38]

34. *Andreas*, 463 U.S. at 780.

35. *See* Arizona v. Hicks, 480 U.S. 321, 327 (1987).

36. 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*, 6 CARDOZO PUB. L. POL'Y & ETHICS J. 101, 104 (2007).

37. Kerr, *supra* note 4, at 538.

38. *Id.* at 537.

In his well-known article *Searches and Seizures in a Digital World*, Professor Orin Kerr elucidates the key differences between physical and computer search and seizure methods.[39] To start, the method that government officials use to obtain information in these two scenarios is different. As previously mentioned, a physical space is traditionally searched by an official who enters a room or vehicle, opens drawers and containers, and looks around.[40] On the other hand, an agent cannot physically enter a computer to extract the desired data; he must type commands that signal the computer to access data[41] on the hard drive before the data becomes visible on an output device such as a monitor.[42] The difference is fundamental.

Second, where a physical search and seizure traditionally involves an agent entering a home and taking evidence, its digital corollary does not require any physical movement of evidence. Rather, in order to preserve the integrity of the original evidence, the agent or computer forensics expert makes an exact copy of the data and performs any analysis on the data copy on a government computer.[43] Whether copying data constitutes a Fourth Amendment seizure is undecided[44] and raises significant legal issues: Is this a

39. *See id.* at 538–47.

40. *See supra* Part II.B.

41. Furthermore, data on a computer storage device are intangible—every letter, number, or symbol is composed of a string of eight zeros and ones called a "byte" of information. *See* Kerr, *supra* note 4, at 538–39.

42. *See id.* at 539.

43. *Id.* at 540 (citing BILL NELSON ET AL., GUIDE TO COMPUTER FORENSICS AND INVESTIGATIONS 51 (2004)).

44. *Compare* Arizona v. Hicks, 480 U.S. 321, 323–24 (1987) (finding that a police officer writing down the serial number of a suspected stolen stereo did not constitute an illegal seizure of the serial number but also finding that the officer's movement of the stereo *did* constitute an illegal search), *and* Bills v. Aseltine, 958 F.2d 697, 707 (6th Cir. 1992) (holding that the recording of visual images of a scene by means of photography does not constitute an unlawful seizure), *with Comprehensive Drug Testing IV*, 621 F.3d 1162, 1168 (9th Cir. 2010) (assuming that copying digital data unlawfully seizes it by repeatedly characterizing the data as "seized data").

In his 2010 article, Kerr makes a critical distinction between copying serial numbers and taking photographs, and copying computer data: "Writing down information or taking a photograph merely preserves the human observation in fixed form[, whereas] electronic copying adds to the information in the government's possession by copying that which the government has not observed." Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 YALE L.J. 700, 714 (2010). Whether something constitutes an unlawful seizure, then, depends on whether the information has been first exposed to human observation..Accordingly, Kerr believes that copying serial numbers and taking photographs should not be considered a seizure while copying data for later observation should be. *Id.* As discussed in Part V, this distinction makes a plain view doctrine tailored to digital evidence cases (or even better, a statute codifying this distinction)

seizure of the original data? Can the government freely peruse its own copy? Is that a reasonable search?[45]

Third, the scope of computer searches is much greater than that of physical searches due to computers' vast storage space.[46] Whereas physical searches are limited by the confines of the room, vehicle, or file cabinet to be searched, a search of a hard drive of a typical one-hundred-gigabyte home computer can implicate the equivalent of fifty million typed pages.[47]

Accordingly, the sheer amount of data involved illustrates that electronic data seizure fits within the original policy aims of the plain view doctrine: to mitigate the risk of evidence destruction and to spare the government the "inconvenience . . . of going to obtain a warrant" every time it wishes to seize potentially incriminating material.[48] If the government is inconvenienced by returning to the magistrate for a warrant to search and seize one thousand pages, the government will certainly be aggravated by a digital search involving the equivalent of fifty million pages that could disappear in the stroke of a key. In other words, the risky and procedurally cumbersome process of returning to the magistrate is exacerbated by the volume of data in cases involving digital data.

Additionally, the intangible nature[49] of computer data in conjunction with the vast storage capacity of modern computers "creates a high risk of overbroad, wide-ranging searches and seizures."[50] Furthermore, a potentially overbroad search directly conflicts with the fundamental Fourth Amendment principle that government officials not conduct "general" searches and that

necessary because, otherwise, copying digital information will be deemed an unlawful seizure in jurisdictions that adopt Kerr's proposal.

45. Kerr, *supra* note 4, at 541; Lowenstein, *supra* note 36, at 104.

46. Lowenstein, *supra* note 36, at 105.

47. *Id.* (referring to Nathan Drew Larsen, *Evaluating the Proposed Changes to Rule 37: Spoliation, Routine Operation and the Rules Enabling Act*, 4 NW. J. TECH. & INTELL. PROP. 212, 216 (2006) ("One gigabyte of memory space can hold the equivalent of 500,000 typed pages.")).

48. *Hicks*, 480 U.S. at 327.

49. While the intangible nature of digital data makes it easier to execute an overbroad search in that typing commands into a computer is easier than physically seizing thousands of documents, the data's intangible nature does not affect the analysis because the Supreme Court has recognized that the Fourth Amendment protects "intangible as well as tangible evidence." Raphael Winick, *Searches and Seizures of Computer and Computer Data*, 8 HARV. J.L. & TECH. 75, 81 (1994) (citing Warden v. Hayden, 387 U.S. 294, 305 (1967)).

50. *Id.* at 78.

warrants specifically describe the places to be searched and the things to be seized.[51]

Finally, the technique for finding evidence and the degree of its invasiveness distinguish physical and computer searches and seizures.[52] When executing a physical search, a search team typically composed of trained police officers goes from room to room seeking the evidence described in the warrant; once the item is found, the search is over and the police leave.[53] Due to prohibitive costs, the police rarely conduct an extraordinarily extensive or thorough search unless the case is particularly important.[54] On the other hand, analysis of a single hard drive requires fewer people but can take a forensic analyst[55] months to complete, depending on the importance of the case or the nature of evidence sought.[56]

Contributing to their labor- and time-intensive nature, computer searches also require forensic analysts to conduct two different types of searches: a "logical," or "virtual," level search and a "physical" level search.[57] A logical search examines a hard drive's file system for certain file extensions, such as ".jpg."[58] Because it is easy to change the file extension, a "physical" level search is necessary to capture any data not gathered from the logical search. A physical search recovers data by searching for file headers—difficult-to-alter segments of data that tell the operating system information about the associated file type.[59]

Even with highly skilled forensic analysts performing comprehensive logical and physical searches, the targets of government investigations can attempt to thwart search efforts.[60] For example, computer owners can encrypt data, rendering it inaccessible

51. *See Hayden*, 387 U.S. at 301.

52. Kerr, *supra* note 4, at 543.

53. *Id.*

54. *See id.*

55. The forensic analyst makes the determination of how much time to spend on a computer search in conjunction with the warrant and the case agent. When conducting the search, the forensic analyst must keep in mind the warrant's specifications, as well as the amount of evidence the government needs to prove its case. *Id.* at 544.

56. *Id.*

57. *Id.*

58. *Id.* (citing JIM KEOGH, THE ESSENTIAL GUIDE TO COMPUTER HARDWARE 144–46 (2002)).

59. *Id.* at 545 (citing NELSON, *supra* note 43, at 493).

60. Lowenstein, *supra* note 36, at 106.

to anyone without a special password, or can even plant booby traps that destroy data if the analyst does not follow meticulous procedures.[61]

It has been argued that the justification for the plain view doctrine in physical searches—the risk of evidence being destroyed while government agents obtain another warrant—is not present in the context of digital searches because government agents remove a copy of the evidence from the owner's control during typical digital search and seizure procedures.[62] This argument assumes, however, that the copying itself is not an unlawful seizure. Kerr now believes that it is.[63] If copying digital data is an unlawful seizure, the government needs the plain view doctrine for the same reason it needs it in physical search and seizure proceedings: efficiency and protection of evidence. Even though a new warrant can be granted within one day, one day is more than adequate time for a technologically savvy suspect to destroy the data.

As has been illustrated, the analogy between physical and computer searches is attenuated, yet the plain view doctrine remains a necessity. This disharmony is further demonstrated by the central concern in *Comprehensive Drug Testing IV*: how to treat intermingled documents located on computer storage devices.

2. The Intermingled Documents Dilemma

The problem of intermingled documents arises when the government seizes documents not listed in a warrant when it seizes documents that are.[64] This happens in one of two ways: (1) it is not immediately apparent to the government official that the documents are outside the warrant's scope or (2) it would be too cumbersome or time-consuming to separate the relevant documents from the documents not listed in the warrant because they are so intertwined with each other.[65] Intermingled documents cases get litigated when the party aggrieved by the search and seizure of the intermingled

61. *Id.* (citing United States v. Hill, 322 F. Supp. 2d 1081, 1090–91 (C.D. Cal. 2004)).

62. Derek Regensburger, *Bytes, BALCO, and Barry Bonds: An Exploration of the Law Concerning Search and Seizure of Computer Files and an Analysis of the Ninth Circuit's Decision in* United States v. Comprehensive Drug Testing, Inc., 79 J. CRIM. L. & CRIMINOLOGY 1151, 1201 (2007).

63. *See* Kerr, *supra* note 44, at 714–15.

64. Lowenstein, *supra* note 36, at 106.

65. *Id.*

documents claims that the initial search unconstitutionally exceeded the warrant's scope, and that party accordingly moves to suppress.[66]

a. Physically intermingled documents: United States v. Tamura

In *Tamura*,[67] the Ninth Circuit held that intermingled documents seized during a search of Mr. Tamura's office for three specifically authorized categories of records constituted an "unreasonable"[68] seizure.[69] After Mr. Tamura's employees persistently refused to help the government agents locate the desired documents, the FBI seized eleven cardboard boxes of computer printouts, thirty-four file drawers of vouchers, and seventeen drawers of canceled checks and brought them off-site for sorting and extracting the relevant documents.[70]

Despite the court's disapproval of the broad seizure, it ultimately denied Mr. Tamura's motion to suppress because all of the documents introduced at trial were lawfully taken pursuant to the warrant and because the government was motivated by "practicality" and not by indiscriminate "fishing."[71] Even so, the Ninth Circuit emphasized that the "wholesale *seizure* for later detailed examination of records not described in a warrant is significantly more intrusive, and has been characterized as 'the kind of investigatory dragnet that the *fourth amendment* was designed to prevent.'"[72] In dicta, the court suggested that government officials can avoid running afoul of the Fourth Amendment by "sealing and holding the documents pending approval by a magistrate of a further search."[73]

Rather than standing for a specific legal precedent, *Tamura* is widely cited for its clear facts indicating what might constitute an overbroad seizure and for its suggestive dicta. Twenty federal court

66. *Id.* at 106–07.

67. United States v. Tamura, 694 F.2d 591 (9th Cir. 1982).

68. *Id.* at 594–96. The Ninth Circuit did not use the word "unreasonable" synonymously with "legally unreasonable." Rather, "unreasonable" meant that the court disagreed with, or did not "sanction" the government's action, but did not intend for the action to carry the weight of illegality. *See id.* at 596–97.

69. *Id.* at 596.

70. *Id.* at 595.

71. *Id.* at 597.

72. *Id.* at 595 (second emphasis added) (quoting United States v. Abrams, 615 F.2d 541, 543 (1st Cir. 1980)).

73. *Id.* at 595–96.

opinions and two state court opinions have cited the *Tamura* guidelines.[74] This widespread reliance on the *Tamura* guidelines illustrates the power of nonbinding statements of the court. This is important to note at this juncture because it foreshadows the effect that Chief Judge Kozinski's concurring "guidelines" will likely have in the wake of *Comprehensive Drug Testing IV*. As discussed in Part IV below, when the court lays down guidelines, even nonbinding guidelines, it alerts attorneys, judges, and the FBI as to how the court plans to evaluate searches and seizures of intermingled documents. As a result, U.S. Attorneys hoping to use seized evidence, district judges hoping not to get reversed, and FBI agents hoping that their searches will stand up in court will quickly realize that they had better adhere to the guidelines—especially those written by the chief judge of the Ninth Circuit.

b. Digitally intermingled documents: The new frontier

The intermingled documents problem is even more pronounced in the computer context because separating irrelevant files from those within a warrant's scope is necessarily time-consuming and almost always requires that a computer forensics expert analyze the data off-site.[75]

Courts have had mixed reactions to digitally intermingled documents. On one hand, some courts have granted government agents broad authority to conduct sweeping computer searches, seemingly in reaction to the ostensible ease with which computer owners can hinder government searches.[76] Conversely, other courts have expressed concern that broad computer searches are particularly

74. *See Westlaw KeyCite Result*, WESTLAW, http://www.westlaw.com (search for citation "694 F.2d 591," click "KeyCite Citing References for this Headnote" for Headnote "[3]", check the box next to "Cases [22]," and click "Go"). A Westlaw KeyCite search for *Tamura*'s Headnote Three, *349k141*k, on October 10, 2010, provided the cited statistical information. Headnote Three reads: "In instances where documents are so intermingled that they cannot feasibly be sorted on sight, government and law enforcement officials generally can avoid violating Fourth Amendment rights by sealing and holding documents pending approval by magistrate of further search." *See id.*

75. Lowenstein, *supra* note 36, at 108.

76. *See* United States v. Hill, 322 F. Supp. 2d 1081, 1090 (C.D. Cal. 2004) ("[Computer i]mages 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."); United States v. Gray, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999) ("[H]ackers often intentionally mislabel files, or attempt to bury incriminating files within innocuously named directories.").

invasive because they grant the government access to a much greater quantity and many more types of information about people's private lives than do physical searches.[77] Most courts, however, have tried to strike a balance between these two extremes and have accordingly applied a number of different doctrines.

Some courts have looked at the state of mind of the agent conducting the search.[78] In *United States v. Carey*,[79] for example, the Tenth Circuit held that a government detective exceeded a warrant's scope when he admitted that after he opened one image file containing child pornography, he continued to look for child pornography rather than for the drug-related evidence listed in the warrant.[80] Accordingly, because the officer "knew" he was not going to find evidence related to drug activity yet continued to search outside the warrant's scope, the court found that the officer conducted an unconstitutional general search.[81]

On the other hand, in *United States v. Gray*,[82] the court found that an FBI agent's discovery of child pornography during a search for evidence of computer hacking did not exceed the warrant's scope because the discovery was "inadvertent."[83]

Courts are also divided in their application of the plain view doctrine to intermingled computer files. While some courts have held that a piece of evidence is not in plain view when a government agent must type commands in order to access a particular file,[84]

77. Lowenstein, *supra* note 36, at 108–09 (citing United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001) ("Because computers can hold so much information touching on many different areas of a person's life, there is a greater potential for the 'intermingling' of documents and a consequent invasion of privacy when police execute a search for evidence on a computer.")); Winick, *supra* note 49, at 105 ("[The] quantity and variety of information [on a computer] increases the likelihood that highly personal information, irrelevant to the subject of the lawful investigation, will also be searched or seized.")).

78. Lowenstein, *supra* note 36, at 109.

79. 172 F.3d 1268 (10th Cir. 1999).

80. *Id.* at 1271.

81. *Id.* at 1274, 1276.

82. 78 F. Supp. 2d 524 (E.D. Va. 1999).

83. *Id.* at 529.

84. *See, e.g.*, United States v. Comprehensive Drug Testing, Inc. (*Comprehensive Drug Testing I*), 473 F.3d 915, 966–67 (9th Cir. 2006) (Thomas, J., dissenting) (stating that computer evidence was not in plain view because locating such evidence "required analysis and thorough examination off-site"); United States v. Lemmons, 282 F.3d 920, 925 n.5 (7th Cir. 2002) (finding that officer's testimony illustrated that images of child pornography were not in plain view because he "had to access them by opening a program and looking on the hard drive for pornographic images").

others deem such evidence in plain view despite the intermediary step.[85]

Still another response to the problems presented by intermingled digital data is to require warrants to dictate *ex ante* the steps that a government agent must follow when searching a computer.[86] In *Dalia v. United States*,[87] however, the Supreme Court rejected the defendant's argument that warrants must include "a specification of the precise manner in which they are to be executed."[88] Because it is difficult to know what type of search is required until the agent actually sees the data,[89] the Court emphasized that "it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant," subject to a reasonableness standard.[90]

Finally, as will be explored shortly in the discussion about *Comprehensive Drug Testing IV*, some courts have adopted the *Tamura* court's dicta and have found that the best way to avoid violating the Fourth Amendment is to seal the evidence pending magistrate review and to seek an additional warrant by specifying to the magistrate what types of files are sought.[91] While electronic search and seizure law presents more questions than answers, the Ninth Circuit's *Comprehensive Drug Testing IV* decision is a compelling, though arguably flawed, attempt to create a new body of law that has profound ramifications for the government and for individual privacy.

85. *See, e.g.*, United States v. Wong, 334 F.3d 831, 838 (9th Cir. 2003) (finding that computer forensic expert's discovery of child pornography was in plain view despite the warrant's scope only covering evidence of murder because the warrant was valid and because the incriminating nature of the child pornography was "immediately apparent" under *Horton v. California*); Frasier v. State, 794 N.E.2d 449, 465–66 (Ind. Ct. App. 2003) (holding that the plain view exception still applied even though the government opened the digital file to see its contents because the file was ambiguously labeled, hence rendering the discovery of child pornography "inadvertent" under *United States v. Carey*).

86. Kerr, *supra* note 4, at 571.

87. 441 U.S. 238 (1979).

88. *Id.* at 257–59.

89. Kerr feels that the ex ante approach is deeply flawed because the forensics process is too "contingent and unpredictable" for judges to make effective rules. Kerr, *supra* note 4, at 572.

90. *Dalia*, 441 U.S. at 257.

91. United States v. Campos, 221 F.3d 1143, 1148 (10th Cir. 2000); United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999); United States v. Stierhoff, 477 F. Supp. 2d 423, 443 (D. R.I. 2007).

III. *UNITED STATES V. COMPREHENSIVE DRUG TESTING, INC.*

In *Comprehensive Drug Testing IV*, the Ninth Circuit considered many of the issues discussed above. Perhaps infamously, *Comprehensive Drug Testing IV* is about a federal investigation into professional baseball players' steroid use.[92] As it pertains to this Note, however, *Comprehensive Drug Testing IV* is about the procedures that federal courts must follow when issuing and administering search warrants for electronically stored information.[93]

A. Facts and Procedural History

The present case came before the Ninth Circuit as a consolidation of three cases arising from the federal investigation of BALCO on suspicion that it had provided steroids to professional baseball players.[94] The government began the investigation in August 2002 and eventually developed probable cause that at least ten major league baseball players had received steroids from BALCO.[95] The same year, the Players Association entered into a collective bargaining agreement with MLB whereby players would be anonymously tested for steroid use in 2003.[96] According to the agreement, the purpose of the tests was only to determine the extent of the steroid problem in baseball; if more than 5 percent of players tested positive, further testing would be ordered in subsequent seasons.[97] The players were also promised confidentiality pursuant to the agreement.[98]

An independent business, Comprehensive Drug Testing, Inc. (CDT), administered the program from its Long Beach, California, facility and collected players' urine samples.[99] However, a laboratory named Quest Diagnostics, Inc. ("Quest") in Las Vegas, Nevada,

92. *Comprehensive Drug Testing IV*, 621 F.3d 1162, 1165 (9th Cir. 2010).

93. *Id.* at 1165–66.

94. *Id.* (citing United States v. Comprehensive Drug Testing, Inc. (*Comprehensive Drug Testing II*), 513 F.3d 1085 (9th Cir. 2008)).

95. *Id.* (citing *Comprehensive Drug Testing II*, 513 F.3d at 1089).

96. *Id.* at 1166.

97. *Id.*

98. *Id.*

99. *Id.*

performed the actual tests.[100] While Quest kept the urine samples, CDT kept the list of players and their test results.[101]

1. Central District of California and the Cooper Order

On April 7, 2004, the Central District of California granted the government a warrant authorizing the search of CDT's facilities.[102] The warrant's scope was limited to the records of the ten players as to whom the government had established probable cause.[103] Nonetheless, on April 8, 2004, twelve federal agents,[104] led by Special Agent Jeff Novitzky, seized and reviewed the drug testing records[105] of hundreds of MLB and other professional athletes.[106] Although the warrant granted broad authority to seize and remove nearly all computer equipment from CDT's Long Beach, California, facility, it required that specially trained computer personnel—not the investigating agents—conduct the initial review and segregation of the data.[107] This requirement was meant to ensure that the investigating agents would not see data beyond the warrant's scope.[108] Nonetheless, government agents went ahead and copied the Tracey Directory—which contained the names of hundreds of other athletes in addition to the ten baseball players that the warrant named—from the computers properly seized from CDT.[109] Accordingly, Judge Florence-Marie Cooper found that the government "completely ignored" the warrant's requirements.[110]

100. *Id.*

101. *Id.*

102. *Id.* (citing *Comprehensive Drug Testing II*, 513 F.3d 1085, 1091 (9th Cir. 2008)).

103. *Id.*

104. The twelve agents included a Computer Investigative Specialist Agent, Joseph Abboud. *Comprehensive Drug Testing II*, 513 F.3d at 1092.

105. CDT officials did not initially help Agent Novitzky find the evidence that the government was authorized to seize. *Id.* But, later that day, a CDT director identified a computer directory—the Tracey Directory—containing all of the computer files for all of CDT's sports drug testing programs. *Id.* This directory contained hundreds of files and many subdirectories. *Id.* Pursuant to the warrant's language, the agents copied the directory and removed the copy for review at government offices. *Id.* at 1093. Ultimately, the government seized a "25-page master list of all MLB players tested during the 2003 season and a 34-page list of positive drug test results for eight of the ten named BALCO players, intermingled with positive results from 26 other players." *Id.*

106. *Id.* at 1092.

107. *Comprehensive Drug Testing IV*, 621 F.3d at 1168.

108. *Id.*

109. *Id.* at 1169.

110. *Id.* at 1171.

In addition to ignoring the warrant's requirements, the government also used the information it found during its impermissible review of the seized computer data to obtain the subsequent warrants issued in the Northern and Central Districts of California, as well as in Nevada.[111] Accordingly, Judge Cooper found that the government's behavior demonstrated a "callous disregard for the rights of those persons whose records were seized and searched outside the warrant."[112] Therefore, Judge Cooper concluded that the government's failure to segregate responsive from nonresponsive data did not comply with the *Tamura* guidelines. She thereby issued an order (the "Cooper Order") demanding the return to CDT of any evidence not connected with the ten players named in the warrant.[113]

2. District of Nevada and the Mahan Order

On the same day that federal agents searched CDT in the Central District of California, another group of federal agents seized specimens from Quest's laboratory in the District of Nevada.[114] Judge James Mahan issued an order (the "Mahan Order") similar to the Cooper Order that the government had to return all specimens, as well as all notes and memoranda created by agents who reviewed the evidence except for that information pertaining to the ten BALCO players named in the original warrant.[115]

3. Northern District of California and the Illston Quashal

On May 6, 2004, the government secured grand jury subpoenas in the Northern District of California seeking from CDT the same records it had just seized pursuant to a warrant in the Central District, and which had just been ordered returned to CDT by Judge Cooper.[116] In December 2004, Judge Susan Yvonne Illston issued a

111. *Id.* at 1169.

112. *Id.* at 1169–70.

113. *Id.* at 1166 (referring to Order Granting Return of Property, United States v. Comprehensive Drug Testing, No. CV-04-02887-FMC (C.D. Cal. Oct. 1, 2004)).

114. *Id.* at 1170; *Comprehensive Drug Testing II*, 513 F.3d 1085, 1093 (9th Cir. 2008).

115. *Comprehensive Drug Testing IV*, 621 F.3d at 1166–67; *see also Comprehensive Drug Testing II*, 513 F.3d at 1094 (referring to Order Granting Return of Property, United States v. Comprehensive Drug Testing, No. CV-04-00707-JCM (D. Nev. Aug. 19, 2004)).

116. *Comprehensive Drug Testing IV*, 621 F.3d at 1167; *see also Comprehensive Drug Testing II*, 513 F.3d at 1095 (listing the date that the government secured the grand jury subpoenas).

quashal of the subpoenas (the "Illston Quashal"), holding that the government's conduct was unreasonable and constituted harassment. [117]

B. The 2010 Ninth Circuit Decision

The government subsequently appealed the three district court decisions to the Ninth Circuit. The three decisions were heard as one case by the same three-judge panel in 2006 and 2008, followed by an en banc panel in 2009. [118]

In the 2009 decision, Chief Judge Alex Kozinski, writing for the en banc majority, relied on issue preclusion [119] to affirm the Cooper Order, the Mahan Order and the Illston Quashal. He then interestingly—and controversially—concluded his opinion by issuing guidelines for magistrate judges to follow when the government wishes to obtain a warrant to examine an electronic storage medium or when a search for evidence could result in seizing a computer. [120]

Following the 2009 decision, then–Solicitor General Elena Kagan sought, for the first time in history, a rehearing by the full Ninth Circuit. [121] Kagan, on behalf of the Department of Justice,

117. *Comprehensive Drug Testing IV*, 621 F.3d at 1167 (referring to Order Quashing Subpoenas Seeking CDT Records, United States v. Comprehensive Drug Testing, No. MISC-04-234-SI (N.D. Cal. Dec. 2004)); *see also Comprehensive Drug Testing II*, 513 F.3d at 1095 (listing the date that the Illston Quashal was issued).

118. In the Ninth Circuit, the term "en banc" refers to a panel of eleven judges consisting of the chief judge of the Ninth Circuit and ten additional judges to be drawn by lot from the active judges of the Ninth Circuit. 9TH CIR. R. 35-3. There are twenty-nine active judges on the Ninth Circuit. *See History of the Federal Judiciary: U.S. Court of Appeals for the Ninth Circuit*, FED. JUDICIAL CTR., http://www.fjc.gov/history/home.nsf/page/courts_coa_circuit_09.html (last visited Nov. 20, 2010).

119. Issue preclusion prevents a court from reconsidering an issue when "the first and second action involve application of the same principles of law to an [sic] historic fact setting that was complete by the time of the first adjudication." Steen v. John Hancock Mut. Life Ins. Co., 106 F.3d 904, 913 n.5 (9th Cir. 1997) (quoting 18 CHARLES A. WRIGHT ET AL., FEDERAL PRACTICE & PROCEDURE § 4425 (Supp. 1996)). In other words, where, as here, the later-decided actions (the Mahan Order and Illston Quashal) involve the same facts and legal principles as the earlier-decided action (the Cooper Order), the later-decided actions are bound by the factual and legal determinations of the earlier-decided action.

120. United States v. Comprehensive Drug Testing, Inc. (*Comprehensive Drug Testing III*), 579 F.3d 989, 1006–07 (9th Cir. 2009).

121. Brief of United States, Petitioner-Appellant, in Support of Rehearing En Banc by the Full Court at 2, *Comprehensive Drug Testing IV*, 621 F.3d 1162 (Nos. 05-10067, 05-15006, 05-55354) [hereinafter Brief]. The Ninth Circuit may order a rehearing by the all of the judges on the Ninth Circuit following a hearing or rehearing en banc. 9TH CIR. R. 35-3.

argued that the en banc panel's guidelines exceeded an Article III court's proper role.[122]

On September 13, 2010, rather than granting a rehearing by the full court, the same eleven-judge en banc panel reheard *Comprehensive Drug Testing IV* and issued a per curiam opinion that was identical to the 2009 opinion but with the guidelines relegated to a concurrence by Chief Judge Kozinski.

1. The Per Curiam Majority Affirms the Cooper Order and the Mahan Order

Although the majority used issue preclusion to affirm the Mahan Order because it covered the same issues[123] as the previously decided Cooper Order and Illston Quashal, the majority also addressed the government's contrary arguments.[124] In doing so, the majority acknowledged that its decision could rest on issue preclusion, but it felt that the "matter [was] important" and necessary to discuss further in order to "avoid any quibble about the proper scope of preclusion."[125] The majority discussed the government's arguments regarding (1) *Tamura* and (2) the initial review by computer personnel.[126] The following sections discuss each in turn.

a. The government's invocation of the plain view doctrine does not comply with the spirit of the Tamura *procedures*

The government's primary argument was that "it *did* comply with the procedures in *Tamura*," but it was not obligated to return the data showing steroid use by non-BALCO players because the evidence was in "plain view" once the government agents searched

122. Brief, *supra* note 121, at 2.

123. The common issues were that the government "callously disregarded" the non-BALCO players' constitutional rights, and that it "unreasonably refuse[d]" to follow the procedures set forth in *Tamura* upon learning that the ten BALCO players' records were intermingled with the records of players not named in the warrants. *Comprehensive Drug Testing IV*, 621 F.3d at 1185.

124. *Id.* at 1170.

125. *Id.*

126. *Id.* at 1170–75. The majority also discussed CDT and the Players Association's motions in the Central District of California and the District of Nevada for the return of property under Federal Rule of Criminal Procedure 41(g). *Id.* The government argues that plaintiffs improperly brought a Rule 41(g) motion as a motion to suppress. *Id.* at 1172. However, it is clear that plaintiffs did not intend their motion as a suppression motion because suppression motions only implicate criminal defendants. *Id.* Additionally, Rule 41(g) plainly authorizes a motion to return property on behalf of any "'person aggrieved by an unlawful search and seizure of property *or by the deprivation of property*.'" *Id.* at 1173 (quoting FED. R. CRIM. P. 41(g)).

the Tracey Directory.[127] The government argued that *Tamura* did not apply because the seizure was then allegedly lawful.[128]

The majority, however, contended that while the government sought advance authorization for off-site sorting and seizure under *Tamura*, it violated the spirit of *Tamura*.[129] In particular, the majority noted that the point of the *Tamura* procedures was "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 of office file systems and computer databases."[130] The majority feared that allowing the government to look at every piece of seized electronic data will bring everything into "plain view," thus expanding the scope of the search far beyond what was originally permitted by the warrant.[131] In other words, there would be no discernable limit to what the government could search and seize, rendering the procedural safeguards in *Tamura* worthless.[132]

b. Initial review by computer personnel

The majority found that the government ignored one of the main processes designed to prevent government access to intermingled materials beyond the scope of the warrant: initial review by "computer personnel."[133] Despite the presence of an agent specially trained in computer forensics at the scene, the government agent assumed control over the Tracey Directory as soon as it was extracted from the CDT computers.[134]

The government adhered to the warrant specifications to the extent that the computer specialist determined that the data contained on the CDT computers could not be searched and segregated on-site and that it was safe to copy the Tracey Directory rather than seize the entire computer.[135] However, once the copy was made, the computer specialist did not take further steps to segregate the data contained in

127. *Id.* at 1170.
128. *Id.*
129. *Id.* at 1168–71.
130. *Id.* at 1170.
131. *Id.* at 1170–71.
132. *Id.* at 1171.
133. *Id.*
134. *Id.*
135. *Id.* at 1171–72.

the Tracey Directory.[136] Instead, the government proceeded, as it admitted at a hearing before Judge Mahan, "to take [the Tracey Directory] and later on briefly peruse it to see if there was anything above and beyond that which was authorized for seizure in the initial warrant."[137]

Accordingly, the majority concluded that this admission "obvious[ly]" illustrated that the government agents intended the search to bring constitutionally protected data into the government agents' plain view.[138] Furthermore, the majority dismissed as "sophistry" the government's argument that the warrant did not specifically state that *only* computer personnel could view the seized files.[139]

2. The Per Curiam Majority Affirms the Illston Quashal

Judge Illston quashed the government's subpoenas because the government served the subpoenas after it had learned from the Cooper Order that the same evidence had already been illegally seized.[140] Thus, Judge Illston found the subpoenas to be an "unreasonable 'insurance policy'"[141] because it appeared that the government subpoenaed the same materials "in an attempt to moot any future proceedings for the return of property."[142]

While the majority noted that it is not necessarily "unreasonable" to perform an investigation using both subpoenas and search warrants,[143] it held that when using investigatory tools such as warrants and subpoenas, the government must "fully disclose to each judicial officer prior efforts in other judicial fora to obtain same or related information, and what those efforts have achieved."[144] The majority's finding reflected its concern that the government's

136. *Id.* at 1172.

137. *Id.* at 1171.

138. *Id.*

139. *Id.* at 1172. To prevent overreaching and the attendant accusations of pretext, Chief Judge Kozinski proposed, in what was the majority opinion in 2009 but is now a concurrence, a detailed protocol that will be discussed below in Part III.B.4. *Id.* at 1178–80.

140. *Id.* at 1175.

141. *Id.* (quoting United States v. Comprehensive Drug Testing, MISC-04-234-SI (N.D. Cal. Dec. 2004) (quashing subpoenas seeking CDT records) (filed under seal)).

142. *Id.* (comparing J.B. Manning Corp. v. United States, 86 F.3d 926 (9th Cir. 1996)).

143. *Id.* (referring to *In re* Grand Jury Subpoenas Dated Dec. 10, 1987, 926 F.2d 847, 851–55 (9th Cir. 1991)).

144. *Id.*

strategy of moving from district to district in pursuit of the same information intentionally misled the court. [145]

3. The Per Curiam Majority Concludes by Updating *Tamura* and Suggesting Balance

The majority ended its opinion by abruptly stating that it has "updated *Tamura* to apply to the daunting realities of electronic searches." [146] However, the majority did not discuss the technicalities of how the government and judicial officers should handle this "update."

Furthermore, recognizing that over-seizing is inherent in the electronic, or digital, search process, the majority implored judicial officers to exercise "greater vigilance . . . in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable search and seizures." [147] The majority again, however, did not suggest how this balance should be struck.

4. Chief Judge Kozinski's Concurrence Provides Guidelines Designed to Ensure Lawful Electronic Search and Seizure

Even though the majority did not delineate how judicial officers should balance the government's and individuals' interests, Chief Judge Kozinski offers guidelines to the public, the government, and the courts regarding how to conduct a lawful electronic search and seizure. [148] Kozinski emphasized that while judges must exercise their independent judgment, "heeding this guidance will significantly increase the likelihood that the searches and seizures of electronic storage that they authorize will be deemed reasonable and lawful." [149]

Accordingly, in what was originally part of the 2009 majority opinion, Kozinski recommended that: (1) "magistrate judges should insist that the government waive reliance upon the plain view doctrine in digital evidence cases"; (2) "segregation and redaction must be done by specialized personnel[, and] if by government

145. *Id.*

146. *Id.* at 1177.

147. *Id.*

148. *Id.* at 1178–80 (Kozinski, J., concurring). Judges Andrew Kleinfeld, W. Fletcher, Richard Paez, and Milan Smith joined Kozinski's concurrence.

149. *Id.* at 1178.

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) "[t]he 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"; and (5) "[t]he 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." [150]

V. CRITIQUE OF EXISTING LAW

The only difference between the 2009 en banc panel opinion and the 2010 per curiam rehearing is that the Ninth Circuit moved Kozinski's guidelines from his majority opinion in 2009 to his concurrence in 2010. This curious maneuver is likely the Ninth Circuit's peace offering to the Department of Justice and then–Solicitor General Kagan. [151] Rather than grant the requested full court rehearing, the Ninth Circuit removed the Kozinski guidelines, which the Department of Justice argued were unconstitutionally advisory in violation of Article III, [152] and issued the 2010 opinion per curiam with Kozinski's guidelines relegated to a concurrence. [153]

150. *Id.* at 1179–80 (quoting Judge Kozinski's majority opinion in *Comprehensive Drug Testing III*, 579 F.3d 989, 1006 (9th Cir. 2009)).

151. *See* Steven Kalar, *Case o' the Week: One Shy—Search Guidelines Fall in* C.D.T., NINTH CIRCUIT BLOG (Sept. 19, 2010, 8:52 PM), http://circuit9.blogspot.com/search?q=comprehensive+drug+testing.

152. 16 AM. JUR. 2D *Constitutional Law* § 131 (2010) ("Absent constitutional or statutory authorization, a court has no power to render an advisory opinion. Thus, in most states, the courts will not give advisory opinions on constitutional or on any other kinds of issues not before the court as 'cases' or 'controversies.' Under the United States Constitution, the judicial power of the federal courts is restricted to 'cases' and 'controversies.' Thus, federal courts are not authorized to issue advisory opinions under any circumstances."). The 2009 guidelines were arguably an advisory opinion because the issues in the case were already decided pursuant to issue preclusion. Yet, the 2009 majority still issued its guidelines to govern future behavior.

153. *See* Kalar, *supra* note 151. Additionally, the Ninth Circuit may have avoided Supreme Court review by moving the controversial "guidelines" into a concurrence. Lee Tien, *Revised Opinion in Privacy Case Blurs Clear Limits to Digital Search and Seizure*, ELECTRONIC FRONTIER FOUND. (Sept. 14, 2010), https://www.eff.org/deeplinks/2010/09/revised-opinion-privacy-case-blurs-clear-limits.

A. While Avoiding the Advisory Opinion Label, the 2010 Guidelines Will Still "Advise" Future Legal Actors

Even though Kozinski's guidelines are no longer binding Ninth Circuit law, and the opinion is thus no longer susceptible to being a true advisory opinion, the guidelines will likely have the same *effect* because they will still "advise" future legal actors' actions. Particularly because the 2010 per curiam opinion did not explain *how* judicial officers should apply the updated *Tamura* procedures to electronic searches and seizures or *how* they should strike the "right balance" between the government's and individuals' interests, it is likely that judicial officers and the government will look to Kozinski's concurrence for guidance.[154] Without clear rules in the per curiam opinion and with the assurance that "heeding [Kozinski's guidelines] will significantly increase the likelihood that searches and seizures of electronic storage . . . will be lawful," the government and judicial officers will be tempted to follow Kozinski's guidelines.[155] And, as illustrated by the twenty times that the non-binding *Tamura* procedures have been cited by federal courts, the government and judicial officers would be foolish not to.[156]

B. The 2010 Guidelines Do All the Damage of an Advisory Opinion with None of the Liability

Even though Kozinski's guidelines cannot technically constitute an advisory opinion because they are no longer binding on the court, they do all the damage of an advisory opinion with none of the liability. The danger of an advisory opinion is that it will be afforded the force of a holding despite being unrelated to a case or controversy before the court.[157]

For example, an unfortunate byproduct of Kozinski's 2009 guidelines was that magistrates were "treating the en banc panel's 'guidance' as binding."[158] Indeed, after the 2009 opinion, the "Chief

154. Kalar, *supra* note 151.

155. *Comprehensive Drug Testing IV*, 621 F.3d at 1178 (Kozinski, J., concurring).

156. *See Westlaw KeyCite Result*, WESTLAW, http://www.westlaw.com (search for citation "694 F.2d 591," click "KeyCite Citing References for this Headnote" for Headnote "[3]", check the box next to "Cases [22]," and click "Go").

157. *See* United States v. Alaska S.S. Co., 253 U.S. 113, 116 (1920) (explaining that a court is not empowered to decide moot questions or abstract propositions that are not germane to the issues of the case).

158. Brief, *supra* note 121, at 5.

Magistrate Judge for the Western District of Washington . . . sent the United States Attorney's Office for that district a letter stating that 'we are all required to follow the requirements set forth in the [2009 en banc majority]'s decision.'" [159]

Additionally, the treatment of the 2009 guidelines as binding created hardships for U.S. Attorney's Offices because federal agents had difficulty executing warrants, and forensic examiners trying to adhere to the guidelines spent much more time learning complex cases before sorting intermingled documents. [160] Put differently, the 2009 guidelines chilled magistrates from deviating from the guidelines and chilled the government from seeking new warrants.

The 2009 guidelines also caused the federal government to transfer its investigations to state authorities who were not constrained by the guidelines. [161] For example, when federal agents in the Western District of Washington heard from their colleagues in San Diego that two people had filmed themselves raping a four-year-old girl and sent the images over the Internet, the agents did not apply for a warrant to search the suspects' computers because the 2009 guidelines insisted that the government "waive reliance on the plain view doctrine in digital evidence cases." [162] The agents were thus afraid that any evidence that the forensic experts found on the suspects' computers pertaining to other potential victims could not be revealed because the 2009 guidelines prohibited forensic experts from revealing anything to the FBI beyond the warrant's scope. [163] Rather than risk discovering other potential victims and not being able to use the evidence, the federal agents opted to transfer the case to state officials. [164]

Legal actors' troublesome reliance on the 2009 advisory guidelines will not dissipate now that Kozinski's concurrence contains the guidelines. While magistrates and the government need not follow Kozinski's 2010 guidelines, they will likely continue to

159. *Id.*

160. *Id.* at 6.

161. *Id.*

162. *Comprehensive Drug Testing III*, 579 F.3d 989, 1006 (9th Cir. 2009); Brief, *supra* note 121, at 6–7.

163. Brief, *supra* note 121, at 6–7.

164. This shifting between federal and state jurisdictions raises an interesting federalism issue that will be discussed in Part V.

follow his advice in the absence of clear rules in the 2010 majority opinion. When the chief judge speaks, even if in a concurrence, people listen. In other words, by putting his guidelines in a nonbinding concurrence that cannot be considered an advisory opinion with a capital "A," Kozinski had his cake and ate it too.

C. Alternatives to Moving the Guidelines into a Concurrence

Other than transferring Kozinski's guidelines to a concurrence—an arguable end run around the advisory opinion problem—what else could the Ninth Circuit have done? In many ways, *Comprehensive Drug Testing IV* was not a good test case to formulate a coherent set of rules governing intermingled documents stored on computers.

To start, jurisdictions are already split as to the applicability of the plain view doctrine, the agent's state of mind as an indicator of an unconstitutionally broad search, and the application of the *Tamura* procedures in the digital realm.[165] While the plain view doctrine works well as traditionally understood in the confined physical spaces of homes, cars, and file cabinets, it raises more privacy concerns in the vast digital storage spaces of hard drives, floppy disks, and thumb drives.

Similarly, sorting intermingled physical documents under *Tamura* does not require the same degree of technical skill that sorting intermingled digital data entails. Indeed, the danger of digital booby traps and the reality of encryption are dilemmas unique to searching and sorting digital information. Therefore, the attenuated analogy between physical and digital information renders Kozinski's attempt to create new plain view rules and the majority's attempt to apply *Tamura* to computer searches and seizures fragmented at best, and an end run at worst.

Second, the issues in *Comprehensive Drug Testing IV* were not a good foundation on which to build new digital search and seizure law because they were primarily procedural.[166] It was not until *after*

165. *See supra* Part II.D.1–2.

166. The Ninth Circuit ruled on the following issues: (1) whether the appeal of the Cooper Order was timely filed; (2) whether the appeal of the Mahan Order was controlled by the preclusive effect of the Cooper and Illston Orders; (3) whether the government complied with the terms of certain warrants; (4) whether the District Court for the District of Nevada abused its discretion in ordering property returned to the appellees pursuant to Rule 41(g); and (5) whether the District Court for the Northern District of California abused its discretion in concluding that compliance with a particular subpoena would be "unreasonable or oppressive." *Comprehensive*

ruling for CDT and the Players Association on the merits of these issues that Kozinski issued the digital search and seizure guidelines that "should prove a useful tool for the future." [167]

In *Comprehensive Drug Testing IV*, the resolution of the dispositive issues was judicially sound, and the Ninth Circuit issued an order decreeing that it would not consider any further petitions for rehearing. [168] Thus, the Ninth Circuit will likely have to wait for a case that has the guidelines as its central issue until it can create a new body of digital search and seizure law.

D. The 2010 Guidelines Could Still Become Binding Precedent If They Become an Issue Before a Different Set of Ninth Circuit Judges

In fact, even though the guidelines are in a concurrence, a different Ninth Circuit panel of judges or a case that features the guidelines as the dispositive issue could result in the guidelines becoming controlling precedent yet again. [169] It is noteworthy that the technologically savvy Judge Sidney Thomas was not involved in either the 2009 or 2010 *Comprehensive Drug Testing IV* opinions. [170] Judge Thomas's dissent in the 2006 panel decision sparked the ensuing Ninth Circuit debate because he suggested that the computer evidence had not been in plain view. [171] Had Judge Thomas been one of the eleven judges on the 2010 panel, or had one of Judges Wardlaw, Berzon, or Graber remained loyal to Kozinski's guidelines, the guidelines might still be in the majority opinion. [172]

V. PROPOSAL

When framing a solution to digital searches and seizures—or any issue for that matter—one of the first steps is to determine what is and whose interests are at stake. In *Comprehensive Drug Testing IV*, the government, magistrates, and athletes whose drug-testing information was seized in the Tracey Directory clearly had a strong

Drug Testing IV, 621 F.3d 1162, 1167, 1170–72, 1174–75 (9th Cir. 2010); Brief, *supra* note 121, at 3–4.

167. *Comprehensive Drug Testing IV*, 621 F.3d at 1180 (Kozinski, J., concurring).

168. *Id.* at 1165 (majority opinion).

169. Kalar, *supra* note 151.

170. *Id.*

171. *Comprehensive Drug Testing I*, 473 F.3d 915, 966–67 (9th Cir. 2006) (Thomas, J., dissenting).

172. Kalar, *supra* note 151.

interest in the outcome of the case. Beyond *Comprehensive Drug Testing IV*, however, millions of ordinary individuals whose personal information might be intermingled with data targeted by a warrant are left without a reasonable expectation of privacy. It is this concern for innocent third-party privacy that frames this Note's proposal.

A. A Legislative Solution Federalizes Privacy Expectation and Best Accounts for the Fundamental Differences Between Physical and Digital Data

Courts are traditionally viewed as the guardians of individual privacy: they "can expose constitutional, statutory, and common law privacy gaps and identify the constitutional standards to which legislation must conform." [173] A judicial solution, then, seems logical. However, because *Comprehensive Drug Testing IV* has left more questions than answers, and because jurisdictions are split over the proper application of search and seizure doctrine to intermingled digital data, the permanent solution is legislative.

As Professor Patricia Bellia states in her recent law review article *Federalization in Information Privacy Law*, "some of our most significant federal information privacy statutes attempt to implement or recalibrate the balance that courts have arrived at in applying the Fourth Amendment to the conduct of government agents." [174] Congress does this under its Commerce Clause power. [175] Specifically, where, as in *Comprehensive Drug Testing IV*, a court has applied the Fourth Amendment to government conduct affecting information privacy, the Supreme Court has broadly interpreted the Commerce Clause [176] "[to] give[] Congress considerable leeway to

173. Patricia Bellia, *Federalization in Information Privacy Law*, 118 YALE L.J. 868, 878 (2009).

174. *Id.*

175. *Id.*

176. *See, e.g.*, Gonzales v. Raich, 545 U.S. 1, 17 (2005) (explaining that the Supreme Court has firmly established Congress's power to regulate local, non-commercial activities if, in the aggregate, the activities have a substantial effect on interstate commerce); Wickard v. Filburn, 317 U.S. 111, 128–29 (1942) (finding that a farmer's growth of wheat for personal consumption in excess of the quota imposed by the Agricultural Act can be regulated under the Act because of its potentially substantial impact in the aggregate). Furthermore, the scope of certain privacy statutes has been explicitly linked to interstate commerce. *See, e.g.*, 18 U.S.C. § 2510(1) (2006) (defining "wire communication" as a transmission in interstate commerce or one that affects interstate commerce); 18 U.S.C. § 2710(a)(4) (2006) (defining "video tape service provider" as any person engaged in business in or affecting interstate commerce); 42 U.S.C. § 2000aa(a), (b) (2006) (regulating government officials' search and seizure of work product and other documents

respond by implementing or ratcheting up the judicial standard."[177] Under this interpretation, the Commerce Clause gives Congress the power to create statutes that reinforce or overcome judicial opinions to conform to Congress's ideal balance of individual privacy and law enforcement capability.[178] Because the legislature creates laws that represent the culmination of judicial wrestling with constitutional issues, Bellia calls this nexus a "quasi-constitutional form of criminal procedure."[179]

An example of this quasi-constitutional machinery at work is exemplified by the enactment of the Federal Wiretap Act[180] in response to the Supreme Court's 1967 decisions in *Katz v. United States*[181] and *Berger v. New York*.[182] In *Berger*, the Court struck down a New York statute that permitted eavesdropping on private citizens by local law enforcement officials.[183] Similarly, in *Katz*, the Court found that FBI agents' use of an electronic listening and recording device to overhear a suspect's conversation in a public telephone booth constituted a Fourth Amendment "search"[184] and thus required a warrant.[185]

Both *Berger* and *Katz* forbade eavesdropping by government officials unless the officials complied with the Fourth Amendment requirements that the Court identified.[186] In 1968, the year following the *Berger* and *Katz* decisions, Congress enacted the Federal Wiretap Act, codifying the steps government officials must take to obtain a warrant authorizing electronic surveillance.[187]

relating to material possessed by a person reasonably believed to intend to disseminate the materials "in or affecting interstate . . . commerce").

177. Bellia, *supra* note 173, at 878.

178. *Id.* at 878–79.

179. *Id.* at 879.

180. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 197, 211 (codified as amended at 18 U.S.C. §§ 2510–22 (2006)).

181. 389 U.S. 347 (1967).

182. 388 U.S. 41 (1967); Bellia, *supra* note 173, at 879.

183. *Berger*, 388 U.S. at 41–42, 63–64.

184. *Katz*, 389 U.S. at 359.

185. *Id.* at 347.

186. Bellia, *supra* note 173, at 879.

187. 18 U.S.C. § 2518 (2006); *see* United States v. Cox, 449 F.2d 679, 687 (10th Cir. 1971) (explaining that Congress made "[e]very effort" to comply with the requirements of *Berger* and *Katz* in enacting the Federal Wiretap Act and that Congress was "seeking to deal realistically with highly complex problems in accordance with the demands of the Constitution"); Bellia, *supra* note 173, at 879.

Whether or not *Comprehensive Drug Testing IV* stays on the books, a legislative solution would enable Congress to federalize digital privacy expectations. Legislation protecting privacy in the digital arena is particularly necessary because it is difficult to place a value on the damaging societal effects of the release of personal data.[188] For example, the names of MLB players whose records were intermingled with the ten players' records that the government had a warrant to seize have begun to publically leak.[189] One player whose name has leaked, David Ortiz of the Boston Red Sox, has admitted that the "scandal has affected his recent performance on the field."[190] The shame, public condemnation, and loss of goodwill that the revelation has had on Ortiz are difficult to translate into monetary terms.

While it might be difficult to sympathize with the plight of a multi-millionaire professional athlete, it is important to remember that the athletes whose records were seized in the Tracey Directory were promised anonymity by the government as a precondition of submitting to the drug tests. The athletes' expectation of privacy, therefore, is no different than that of the ordinary citizen who expects his or her sensitive medical or bank records to remain confidential. Legislating in this area will enable Congress to articulate its stance on an individual's reasonable expectation of privacy should private information become intermingled with the target of a valid digital search and seizure.

Congress also has a strong interest in safeguarding the economic well-being of the innocent third parties whose data is intermingled with the targeted information. In *Comprehensive Drug Testing IV*, the majority explained that the government has to return the property to "protect[] the privacy and economic well-being of [the players], which could easily be impaired if the government were to release the test results swept up in the dragnet."[191]

188. *See* James Nehf, *Recognizing the Social Value in Information Privacy*, 78 WASH. L. REV. 1, 62–64 (2003).

189. Eric Polsky, *Every Thorn Has Its Rose*, BASEBALL DAILY DIG. (Aug. 12, 2009, 12:12 AM), http://www.baseballdailydigest.com/2009/08/12/every-thorn-has-its-rose/.

190. *Id.*

191. *Comprehensive Drug Testing IV*, 621 F.3d 1162, 1172 (9th Cir. 2010).

A legislative solution also has many precedents; Congress has historically acted in reaction to highly publicized privacy breaches.[192] For example, in 1988, Congress passed the Video Privacy Protection Act (VPPA)[193] in response to the publication of Judge Robert Bork's video rental history during his failed Supreme Court nomination hearing. The Senate report accompanying the proposed legislation linked the media coverage of Judge Bork's video rental history to the need for VPPA.[194]

Likewise, Congress should both explicate its position on the reasonable expectation of privacy and act in response to the highly publicized leak of the names of MLB players who have tested positive for steroids. As was the case with VPPA, the prior publication of a major investigative report would bolster any new legislation in light of *Comprehensive Drug Testing IV*. After the results of the anonymous drug testing referenced in *Comprehensive Drug Testing IV* revealed the prevalence of steroid use in major league baseball, former Senator George Mitchell undertook a twenty-month-long investigation. That investigation culminated in the publication of the 409-page Mitchell Report that listed the names of eighty-nine players who allegedly used steroids and made recommendations on how to resolve baseball's steroid problem.[195] The explosive publicity that accompanied the leak of the innocent players' names along with the existence of a major investigative report gives Congress additional compelling reasons to create laws governing intermingled digital information.

B. The Composition of a New Digital Statute

The composition of any statute Congress might enact in response to the publicity, the Mitchell Report, and *Comprehensive Drug Testing IV* will depend in part on whether the U.S. Supreme Court rehears *Comprehensive Drug Testing IV*. Even if the Court rehears *Comprehensive Drug Testing IV*, however, the law still will

192. Bellia, *supra* note 173, at 884.

193. Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (codified at 18 U.S.C. § 2710 (2006)).

194. S. REP. NO. 100-599, at 4–5 (1988), *reprinted in* 1988 U.S.C.C.A.N. 4342-1, 4342-5.

195. Barry M. Bloom, *Mitchell Report Proposes Solutions*, MLB.COM (Dec. 13, 2007, 11:02 PM), http://mlb.mlb.com/news/article.jsp?ymd=20071213&content_id=2324860&vkey=news_mlb&fext=.jsp&c_id=mlb.

not sufficiently address the fact that digital evidence is fundamentally different from physical evidence because judicial decisions are bound by stare decisis. It will then force the Supreme Court to create law based on the existing plain view rules, rather than create new law from scratch like Congress can. While a Supreme Court opinion could provide a temporary solution to the digital evidence problem, the permanent solution is legislative. In the meantime, I have an advisory opinion of my own.

First, any new statute (or any common law development, for that matter) must be framed by the policy that law enforcement abuse is the exception rather than the norm. While case law is littered with examples of government agents, such as those in *Carey* and *Comprehensive Drug Testing IV*, who "callously disregarded" individual rights or "indiscriminately fished" for information beyond a warrant's scope, "there is no evidence that police disobedience of search warrant limitations is so widespread to compel such onerous pre-issuance procedures."[196] This is but one reason why the new statute should purge Kozinski's suggestion that the government waive reliance on the plain view doctrine.

Second, the legislature must provide law enforcement with a seizure device—similar to the plain view doctrine—that accounts for the major differences between physical and digital searches. Not only does the exponential difference in storage capacity between physical and digital storage media exacerbate the already "inconvenient" process of returning to the magistrate for a new warrant, but seeing contraband in plain view on a bedside table is inherently different from opening file folders on a hard drive and seeing a JPEG of child pornography.[197] Therefore, even though trying to judicially reconfigure the plain view doctrine to fit digital evidence cases could be an adequate temporary fix, a legislative solution will best be able to account, anew, for the vast differences between digital and physical searches.

196. United States v. Farlow, No. CR-09-38-B-W, 2009 WL 4728690, at *6 n.3 (D. Me. Dec. 3, 2009). That a judge from the U.S. District Court of the District of Maine would drop a footnote expressing displeasure with the 2009 *Comprehensive Drug Testing III* guidelines is telling of the shockwaves that the guidelines have sent throughout the United States. This issue is not confined to the Ninth Circuit.

197. *See* Arizona v. Hicks, 480 U.S. 321, 327 (1987) (discussing the practical justifications of permitting a police officer to seize contraband viewed in the course of a lawful arrest); *supra* Part II.D.1.

As mentioned in Part II.D.1, Kerr draws a distinction between seizing evidence subject and not subject to human observation (e.g., an officer's handwritten notes versus an officer's copy of an entire computer directory created without actually seeing the directory's contents) by suggesting that the former is not an unlawful seizure while the latter is.[198] But most electronic copies are created without the copier actually observing the entire file—the sheer size of digital files making such a practice inefficient and unwieldy.[199] Therefore, a statutory provision similar to the plain view doctrine will be necessary to avoid unlawfully seizing copied electronic data.

Furthermore, a statute similar to the plain view doctrine but tailored to digital evidence cases fits within the original policy aim of preventing data destruction. Prior to Kerr's suggestion that the "power to seize is the power to freeze,"[200] the strongest argument against a digital plain view doctrine was that copying data eliminates the risk of data destruction. However, if courts adopt Kerr's distinction, the government will not copy digital data for fear of violating the Fourth Amendment. Rather, the government will likely revert to *Tamura*'s and Kozinski's suggestion to return to the magistrate for a new warrant. What once seemed like a good idea to Kozinski could ultimately provide a window for suspects to encrypt and destroy digital data.

1. Digital Plain View

Whether the final arbiter of the digital plain view doctrine debate is the courts or the legislature, it is clear that such a doctrine must be clearly distinguished from *Tamura* and the file-cabinet analogue. The differences in file types, file sizes, and infrastructure between computers and physical spaces are fundamental. Digital plain view should build on the requirements of *Horton* and adjust those requirements to the information stored on computers.

198. Kerr, *supra* note 44, at 714.

199. *See id*. at 715.

200. This clever phrase means that copying data is an unlawful seizure because copying data is like "freezing" data for the government's later use without the government having first observed the data at the scene. Copying as freezing is distinguishable from copying in the form of photographs or written notes because photographs and written notes are first observed before the copy is made, implying that their use is more akin to refreshing one's memory than adding to evidence that one might not have obtained otherwise. *See id.* at 711–12.

Specifically, digital plain view should keep the requirement that the officer must not have violated the Fourth Amendment in arriving at the place from which the evidence can be plainly viewed. While in *Horton* this meant that the officer had a valid warrant to enter the home, in the digital context this should be amended to mean both that the officer received a valid warrant to search the computer and that a forensics expert does the actual searching. If encryption and data destruction are as onerous of problems as the government maintains, it makes sense that an expert do the digging.

In addition, Kozinski's suggestion that the expert not reveal to the FBI any evidence found outside the warrant's scope should not be incorporated into the legislation. Forensic experts are computer experts, not trained law enforcement officers. As such, they are not in the best position to know whether a piece of evidence is validly within plain view. What they do know, however, is how to navigate though the different types of files and how to efficiently and safely locate the desired information.

Additionally, in order to comply with adding the forensics expert to the digital search, the *Horton* requirement that the *officer* must have a lawful right to seize the object itself should be amended so that the *forensics expert* is the one who needs to confine his or her search to the warrant's confines. With the advent of digital plain view in the wake of *Comprehensive Drug Testing IV*, what constitutes the warrant's confines must also be determined.

At this juncture, case law is not developed enough to speculate on how specific a warrant must be to comply with the Fourth Amendment in the digital realm. In fact, the notes accompanying the December 2009 amendment to Federal Rule of Criminal Procedure § 41(e) specify that while the amended rule includes new provisions tailored to electronic searches and seizures, the decision as to the warrant's specificity must be left to "ongoing case law development."[201] When the time comes, the Supreme Court should consider carving out an exception for intermingled documents because of the ease with which documents outside a warrant's scope can get swept up with documents within its scope.

Finally, the *Horton* requirement that the evidence's incriminating nature must be "immediately apparent" must be further

201. FED. R. CRIM. P. 41(e) advisory committee's note.

explicated to cover information stored on computers. As Supreme Court precedent currently stands, the term "immediately apparent" does not imply an "unduly high degree of certainty as to the incriminatory character of the evidence . . . ." [202] Instead, many courts have held that satisfying the "immediately apparent" prong requires only that the government agents have probable cause [203] to believe that the object they are viewing is evidence of a crime. [204] Still, neither the Supreme Court nor any of the Courts of Appeals have issued opinions explaining how or whether digitally stored information alters the meaning of "immediately apparent." [205]

Because digitally and physically stored information differ in irreconcilable ways, I propose that "immediately apparent" digital information include information discovered during a two-tiered logical and physical search by a forensic expert. If there is probable cause that a computer contains child pornography and an expert discovers such files during his two-tiered search, such data should be considered "immediately apparent."

Unlike opening a drawer or physical file, performing logical and physical searches exposes more of a suspect's information to the searcher. However, the amount and complexity of digital information, as well as a suspect's ability to hide, encrypt, or booby-

202. Texas v. Brown, 460 U.S. 730, 741 (1983).

203. The Supreme Court has frequently explained that "probable cause is a flexible, common-sense standard [that] merely requires that the facts available to the officer would 'warrant a man of reasonable caution in the belief that certain items may be contraband or stolen property or useful as evidence of a crime; it does not demand any showing that such a belief be correct or more likely true than false." *Id.* at 742.

204. *Id.* at 741–42; *see also* Arizona v. Hicks, 480 U.S. 321, 326 (1987) (holding that probable cause is required to invoke the plain view doctrine but not specifically stating that probable cause is required to satisfy the "immediately apparent" prong); United States v. Smith, 459 F.3d 1276, 1290–91 (11th Cir. 2006) (stating that meeting the "immediately apparent" prong requires probable cause to believe that the objects the agents are viewing is evidence of a crime but not specifying whether that is the only requirement).

205. A search of district court opinions revealed one case that offered guidance as to what constitutes "immediately apparent" digital evidence. In *United States v. Mitchell*, the U.S. District Court for the Southern District of Georgia held that images of child pornography on the suspect's hard drive were immediately apparent because the suspect answered, "Yes, probably" to a question as to whether his computer contained child pornography. CR407-126, 2007 U.S. Dist. LEXIS 74349, at *16 (S.D. Ga. Oct. 3, 2007). The unequivocal language of the suspect, combined with the FBI's prior knowledge that the suspect had purchased something from an illegal website "clearly furnished probable cause" that the suspect's computer contained images of child pornography. *Id.* at *16–17. While this case was factually about data on electronic storage devices, the court nonetheless defined "immediately apparent" as that which meets probable cause.

trap data, necessitates the depth and breadth of a logical and physical search. What might be found during such a search, then, must properly be considered "immediately apparent" under the new digital plain view doctrine.

Because I propose that the statute not include Kozinski's suggestion that the forensic expert not reveal information outside the warrant's scope to the FBI, the risk of the forensic expert missing evidence validly within plain view is mitigated. For example, in *Comprehensive Drug Testing IV*, the government might not have seized the entire Tracey Directory if a rule existed that permitted the forensic expert to reveal potentially incriminating evidence to the government for the government to then decide whether to apply for a new warrant or to seize the evidence as "immediately apparent" under plain view.

For all of this to work, however, mechanisms must be put in place to enforce the one-way investigative wall between the forensic expert and the government. While the expert is permitted to reveal potentially incriminating evidence to the government under the proposed law, nothing legally prevents the government from looking over the expert's shoulder—from silently yet effectively usurping the process. This is a perceived weakness of the new statute but an issue for another paper. A piece of legislation encompassing the aforementioned provisions and addressing the practical necessity of an investigative wall strikes the best balance "between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures." [206]

2. A Uniform Federal Law Is Consistent with Federalism

Furthermore, creating a uniform federal law will best serve the interests of federalism by preventing law enforcement duties from being transferred from federal to state governments. As previously discussed, federal agents operating under the 2009 guidelines handed their duties to the states rather than ignore potentially incriminating information due to the forensic experts' inability to divulge information outside a warrant's scope. Without clear rules in the 2010 majority opinion, and with Kozinski's conspicuous notification that following his 2010 guidelines will "significantly increase the

206. *Comprehensive Drug Testing IV*, 621 F.3d 1162, 1177 (9th Cir. 2010).

likelihood" that searches and seizures "will be deemed reasonable and lawful," federal agents will likely turn to Kozinski's concurrence for the same guidance that caused them to transfer cases to state governments prior to the 2010 decision.[207] The lack of clear federal law will thus place a greater law enforcement burden on state governments.

The creation of clear federal law also may lead to new state law in this area. Bellia points out, "As in the case of quasi-constitutional statutes, when Congress fills a perceived information privacy gap before states do and Congress does not preempt state legislation, states can adopt their own laws regulating similar conduct."[208] This situation is significant due to a phenomenon called "competitive federalism."[209] Competitive federalism occurs when states enact laws—digital search and seizure laws, for example—and people or businesses move to the state they perceive to have the most favorable laws.[210] The states essentially compete for residents and businesses. Because states have an incentive to attract residents and businesses, they will theoretically create laws that favor individual privacy over government law enforcement. Therefore, not only will creating a clear federal law prevent cases from being transferred to the states, it will also prompt the states to enact laws favorable to the people.

VI. CONCLUSION

The *Comprehensive Drug Testing IV* opinion, while particularly interesting to baseball aficionados, is universally compelling because it implicates several pressing issues at the forefront of digital search and seizure doctrine. Specifically, whether in the 2009 majority opinion or the 2010 concurring opinion, the suggestion that the plain view doctrine should not apply to digital evidence cases overlooks the fundamental differences in file size, time needed to search, and possibility of data destruction inherent in digital evidence as compared to the physical evidence discussed in *Tamura*. Rather than leaving the government and judicial officers to figure out how the plain view doctrine explicated in the 1982 *Tamura* case applies to the

207. *Id.* at 1178 (Kozinski, J., concurring).

208. Bellia, *supra* note 173, at 883–85 (calling the phenomenon the "Federal-First" regulatory response).

209. *Id.* at 876–77.

210. *Id.*

computer realm, as suggested by the 2010 majority, the legislature should decide how the plain view doctrine—or a similar exception to the warrant requirement—applies to intermingled digital documents.

The legislature's best shot at a workable digital plain view doctrine is to reconfigure *Horton* to incorporate Kozinski's suggestion that a forensic expert perform the search. However, the legislation should not include Kozinski's guideline suggesting that the expert not reveal anything outside the warrant's scope to the government officials. This configuration protects individual privacy by removing the government agents from the searcher role, yet assures the government that it will not miss any new victims or evidence solely because the expert cannot reveal information outside the warrant's scope.

In addition to its ability to reconfigure the plain view doctrine without the confines of stare decisis, the legislature can also honor the principles of federalism by creating a uniform federal law. The fact that federal agents are transferring cases to state agencies for fear of running afoul of Kozinski's guidelines in *Comprehensive Drug Testing IV* is troubling—troubling for underfunded government agencies and troubling for the principles of federalism. Ultimately, the legislature should act because it will best serve the interests of the citizenry by catalyzing competitive federalism. Not only will the American people have a clearly defined federal digital search and seizure law but also the choice to move to states with laws that favor individual privacy.