

No. 09-H20

IN THE SUPREME COURT OF THE UNITED STATES

UNITED STATES OF AMERICA,

Petitioner,

-against-

STARTESTS, INC. and the
COLONIAL FOOTBALL LEAGUE,

Respondent.

**ON WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE FOURTEENTH CIRCUIT**

BRIEF FOR THE PETITIONER

Competitor #17
Counsel for Petitioner

QUESTIONS PRESENTED

1. Whether the Respondent has standing to sue for the return of illegally seized property under Fed. R. Crim. P. 41(g).

2. Whether the government can rely on the “plain view” exception to the Fourth Amendment’s warrant requirement in digital searches.

3. Whether federal magistrates must adopt the guidelines of United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989 (9th Cir. 2009) (en banc), in issuing warrants in a digital evidence case.

TABLE OF CONTENTS

| | |
|---|----|
| Questions Presented | i |
| Table of Contents | ii |
| Table of Authorities | iv |
| Opinions Below | 1 |
| Constitutional Provisions and Statutes Involved | 2 |
| Statement of the Case..... | 3 |
| Summary of the Argument..... | 5 |
| Argument | 7 |
| I. The Collegiate Football League Does Not Have Standing..... | 7 |
| A. The Respondent Has Improperly Conflated Rule 41(g) and a Motion to Suppress..... | 7 |
| 1. The Motion to Suppress Cannot Simply Be Restyled as a Motion to Return Property | 9 |
| 2. The “Good Faith” Exception Entitles the Government to the Seized Property..... | 11 |
| B. The CFL Cannot Challenge the Search Under a “Targeting” Theory. | 12 |
| C. The CFL Fails the Pennell Test for Associational Standing..... | 12 |
| 1. The Individual Members Have No Standing to Sue..... | 13 |
| 2. The Litigation Is Not Germane to the CFL’s Purpose..... | 13 |
| 3. The CFL’s Membership Has a Profound Conflict of Interest. | 14 |
| II. The Plain View Doctrine Is Applicable to Digital Evidence Cases..... | 15 |
| A. The Fourth Amendment Does Not Distinguish Between Different Kinds of Containers. | 15 |
| B. Searching the Entire Hard Drive Is Consistent with Existing Fourth Amendment | |
| Doctrine. | 18 |
| C. The Plain View Doctrine Is Key to Law Enforcement Efforts. | 21 |
| III. The Guidelines Announced in <u>Comprehensive Drug Testing</u> Conflict with Precedent | |
| and Cause Significant Practical Harms. | 22 |
| A. The CDT Requirements Directly Conflict with Judicial Precedent..... | 22 |
| 1. The CDT Requirements Are Inconsistent with the Supreme Court’s Constitutional | |
| Judgment..... | 22 |
| 2. The CDT Requirements Have No Basis in the Constitution..... | 24 |
| 3. The CDT Requirements Bestow Enforcement Powers upon Magistrate Judges that | |
| Are Unconstitutional..... | 26 |

| | |
|---|-------|
| B. The CDT Requirements Are Unworkable in Practice..... | 27 |
| 1. Ex Ante Approval of Search Protocols Would Serve Little Purpose. | 28 |
| 2. The Use of Filter Teams Is Inefficient and Dangerous. | 29 |
| 3. Hiring Independent Third Parties Is Prohibitively Expensive and Risky..... | 30 |
| C. The CDT Requirements Unwisely Abandon the Common Law Method. | 31 |
| Conclusion | 34 |
| Appendix A..... | A - 1 |
| Appendix B..... | B - 1 |

TABLE OF AUTHORITIES

Cases

| | |
|--|------------|
| <u>Arkansas v. Sanders</u> , 442 U.S. 753 (1979) | 16 |
| <u>Bank of Nova Scotia v. United States</u> , 487 U.S. 250 (1988) | 23 |
| <u>California v. Carney</u> , 471 U.S. 386 (1985) | 16 |
| <u>Coolidge v. New Hampshire</u> , 403 U.S. 443 (1971) | 15 |
| <u>Dalia v. United States</u> , 441 U.S. 238 (1979) | 24, 25 |
| <u>Ex parte United States</u> , 287 U.S. 241 (1932) | 26 |
| <u>Grimes v. Comm’r</u> , 82 F.3d 286 (9th Cir. 1996) | 8, 9 |
| <u>Herring v. United States</u> , 129 S. Ct. 695 (2009) | 8 |
| <u>Horton v. California</u> , 496 U.S. 128 (1990) | 15, 19 |
| <u>Hudson v. Michigan</u> , 547 U.S. 586 (2006) | 8 |
| <u>Hunt v. Wash. State Apple Adver. Comm’n</u> , 432 U.S. 333 (1977) | 12 |
| <u>In re Worksite Inspection of Quality Products, Inc.</u> , | |
| 592 F.2d 611 (1st Cir. 1979) | 26 |
| <u>J. B. Manning Corp. v. United States</u> , 86 F.3d 926 (9th Cir. 1996) | 7, 11 |
| <u>Kitty’s East v. United States</u> , 905 F.2d 1367 (10th Cir. 1990) | 7, 11 |
| <u>Lo-Ji Sales, Inc. v. New York</u> , 442 U.S. 319 (1979) | 27 |
| <u>NAACP v. Patterson</u> , 357 U.S. 449 (1958) | 12, 14 |
| <u>New Jersey v. T.L.O.</u> , 469 U.S. 325 (1985) | 16 |
| <u>Pennell v. City of San Jose</u> , 485 U.S. 1 (1988) | 12 |
| <u>Rakas v. Illinois</u> , 439 U.S. 128 (1978) | 9, 12, 14 |
| <u>Ramsden v. United States</u> , 2 F.3d 322 (9th Cir. 1993) | 10 |
| <u>Retired Chicago Police Ass’n v. City of Chicago</u> , | |
| 76 F.3d 856 (7th Cir. 1996) | 14 |
| <u>Robbins v. California</u> , 453 U.S. 420 (1981) (plurality opinion) | 16 |
| <u>Shadwick v. City of Tampa</u> , 407 U.S. 345 (1972) | 27 |
| <u>Thomas v. Arn</u> , 474 U.S. 140 (1985) | 23 |
| <u>United States v. Barnes</u> , 909 F.2d 1059 (7th Cir. 1990) | 19 |
| <u>United States v. Bonfiglio</u> , 713 F.2d 932 (2d Cir. 1983) | 17 |
| <u>United States v. Brooks</u> , 427 F.3d 1246 (10th Cir. 2005) | 25, 29 |
| <u>United States v. Buckley</u> , 4 F.3d 552 (7th Cir. 1993) | 19 |
| <u>United States v. Calandra</u> , 414 U.S. 338 (1974) | 8 |
| <u>United States v. Carey</u> , 172 F.3d 1268 (10 th Cir. 1999) | 21, 32, 33 |
| <u>United States v. Cartier</u> , | |
| No. 2:06-cr-73, 2007 WL 319648 (D. N.D. Jan. 30, 2007) | 25 |
| <u>United States v. Chadwick</u> , 433 U.S. 1 (1977) | 15 |

| | |
|---|--------|
| <u>United States v. Comprehensive Drug Testing</u> , 473 F.3d 915 (9th Cir. 2006)..... | 13 |
| <u>United States v. Comprehensive Drug Testing</u> , 579 F.3d 989 (9th Cir. 2009) (en banc)..... | passim |
| <u>United States v. DeBardeleben</u> , 823 F.2d 549, 1987 WL 36735 (4th Cir. 1987) (unpublished opinion) | 17 |
| <u>United States v. Falcon</u> , 766 F.2d 1469 (10th Cir. 1985) | 17 |
| <u>United States v. Farlow</u> , No. CR-09-38-B-W, 2009 U.S. Dist. LEXIS 112623 (D. Me. Dec. 3, 2009) | 21 |
| <u>United States v. Giberson</u> , 527 F.3d 882 (2008)..... | 16, 18 |
| <u>United States v. Gomez-Soto</u> , 723 F.2d 649 (9th Cir. 1984)..... | 17 |
| <u>United States v. Gray</u> , 78 F. Supp. 2d 524 (E.D. Va. 1999) | 16 |
| <u>United States v. Grubbs</u> , 547 U.S. 90 (2006)..... | 25 |
| <u>United States v. Grummer</u> , 08cr4402-DMS (S.D. Cal.) | 22 |
| <u>United States v. Hargus</u> , 128 F.3d 1358 (10th Cir. 1997) | 15 |
| <u>United States v. Havens</u> , 446 U.S. 620 (1980) | 8 |
| <u>United States v. Herndon</u> , 501 F.3d 683 (6th Cir. 2007) | 32 |
| <u>United States v. Horn</u> , 187 F.3d 781 (8th Cir. 1999)..... | 15 |
| <u>United States v. Kaechele</u> , 466 F.Supp.2d 868 (E.D. Mich. 2006) | 25 |
| <u>United States v. Kim</u> , --- F.Supp.2d ----, 2009 WL 5185389 (S.D. Tex. 2009)..... | 32 |
| <u>United States v. Leon</u> , 468 U.S. 897 (1984) | 11 |
| <u>United States v. Lloyd</u> , No. 98 Crim. 529, 1998 WL 846822 (E.D.N.Y. Oct. 5, 1998) | 25 |
| <u>United States v. Miranda</u> , 325 Fed. Appx. 858 (11th Cir. 2009)..... | 32 |
| <u>United States v. Payner</u> , 447 U.S. 727 (1980) | 8, 23 |
| <u>United States v. Pindell</u> , 336 F.3d 1049 (D.C. Cir. 2003) | 19 |
| <u>United States v. Raney</u> , 342 F.3d 551 (7th Cir. 2003)..... | 32 |
| <u>United States v. Reyes</u> , 798 F.2d 380 (10th Cir. 1986) | 17 |
| <u>United States v. Ross</u> , 456 U.S. 798 (1982)..... | 16, 19 |
| <u>United States v. Shinderman</u> , No. CRIM. 05-67-P-H, 2006 WL 522105 (D. Me. Mar. 2, 2006)..... | 25 |
| <u>United States v. Tamura</u> , 694 F.2d 591 (9th Cir. 1982)..... | 28 |
| <u>United States v. Turner</u> , 169 F.3d 84 (1st Cir. 2009)..... | 32 |
| <u>United States v. Upham</u> , 168 F.3d 532 (1st Cir. 1999)..... | 25 |
| <u>United States v. Walser</u> , 275 F.3d 981 (10th Cir. 2001)..... | 32 |
| <u>Zurcher v. Stanford Daily</u> , 436 U.S. 547 (1978) | 26 |

Statutes

| | |
|---------------------------|--------------|
| Fed. R. Crim. P. 41 | 7, 8, 10, 23 |
|---------------------------|--------------|

Miscellaneous Authorities

| | |
|---|--------|
| Abraham S. Goldstein, <u>The Search Warrant, the Magistrate, and Judicial Review</u> , 62 N.Y.U. L. Rev. 1173 (1987)..... | 27 |
| David J. S. Ziff, <u>Fourth Amendment Limitations on the Execution of Computer Searches Conducted Pursuant to a Warrant</u> , Note, 105 Colum. L. Rev. 841 (2005)..... | 20, 21 |
| Department of Justice Office of the Inspector General, <u>The Federal Bureau of Investigation's Efforts to Combat Crimes Against Children, Audit Report 09-08</u> (2009)..... | 30 |
| Orin S. Kerr, <u>Digital Evidence and the New Criminal Procedure</u> , 105 Colum. L. Rev. 279 (2005) | 21, 31 |
| Orin S. Kerr, <u>Searches and Seizures in a Digital World</u> , 119 Harv. L. Rev. 531 (2005) | 28, 29 |
| Raphael Winick, <u>Searches and Seizures of Computers and Computer Data</u> , 8 Harv. J. L. & Tech. 75 (1994) | 24 |
| Samantha Trepel, <u>Digital Searches, General Warrants, and the Case for the Courts</u> , 10 Yale J.L. & Tech. 120 (2007)..... | 15 |

OPINIONS BELOW

The opinion of the United States District Court for the District of Wythe is set out in the record. StarTests, Inc. and the Colonial Football League v. United States, No. 2010-W20 (R. at 1–6). The opinion of the United States Circuit Court of Appeals for the Fourteenth Circuit is set out in the record. StarTests, Inc. and the Colonial Football League v. United States, No. 2010-W23 (R. at 7–19).

CONSTITUTIONAL PROVISIONS AND STATUTES INVOLVED

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

U.S. Const. amend. IV.

STATEMENT OF THE CASE

Beginning in 2005, the Colonial Football League (“CFL”) began requiring its franchises to submit players for drug screening tests administered by StarTests, Inc. (“StarTests”). (R. at 8.) Both the CFL and StarTests represented to the players that the test results would remain confidential and stored in the StarTests facility. (R. at 1.) StarTests would release only the percentage of players who had tested positive for steroids, and only to the CFL. (R. at 8.)

In July 2008, the Federal Bureau of Investigation (“FBI”) began investigation into the distribution and usage of illegal steroids by five professional football players, all members of CFL franchises. (R. at 7–8.) Upon discovering that StarTests possessed a database of CFL players’ test results, the FBI requested a search warrant to seize “all computer records, files, and equipment” related to the StarTests-administered test. (R. at 8.) In the course of searching the StarTests databases for the test results related to the initial five players, FBI computer personnel came across the test results of many other players indicating widespread use of illegal substances. (R. at 9.) The FBI decided to expand the scope of their investigation to cover illegal substance abuse by professional athletes. They made copies of the StarTests databases and returned all the computer equipment and hard drives. (R. at 9.)

StarTests and the CFL filed a motion in the United States District Court for the District of Wythe for return of the copied records under Fed. R. Crim. P. 41(g). (R. at 9.) They claimed that the seized evidence was outside the scope of the warrant and was therefore an illegal search and seizure under the Fourth Amendment. (R. at 9.) The government responded with two arguments: first, that the CFL did not have standing to sue, and second, that the evidence was lawfully seized because it was in “plain view” when the government was searching for the five players’ information. (R. at 9.) The District Court accepted the government’s plain view

argument and ruled against StarTests and the CFL. (R. at 9.) On appeal, the Fourteenth Circuit Court of Appeals decided that the plain view doctrine would no longer have any application in digital evidence cases. (R. at 13.) Accordingly, it overturned the district court verdict, and announced the following set of requirements for magistrate judges to follow in digital evidence cases:

1. Magistrates should insist that the government waive reliance upon the plain view doctrine in digital evidence cases.
2. Segregation and redaction must be either done by specialized personnel or an independent third party. If done by government computer personnel, that personnel must agree not to disclose 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 courts.
4. The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by non-computer personnel agents.
5. The government must destroy or, if the recipient may lawfully possess it, return non-responsive data, at all times keeping the court informed of its progress.

(R. at 17.) These requirements (“CDT requirements”) were directly drawn from United States v. Comprehensive Drug Testing, 579 F.3d 989, 1001 (9th Cir. 2009) (en banc), a Ninth Circuit en banc decision on remarkably similar facts. (R. at 17.)

SUMMARY OF THE ARGUMENT

Treating digital files differently from all other forms of evidence has no basis in the Fourth Amendment and imposes significant harms on society. The ruling of the Fourteenth Circuit should be reversed for five reasons.

First, the CFL lacks standing to pursue the Rule 41(g) motion. By seeking the return and destruction of the test results, they conflate Rule 41(g) and a motion to suppress evidence. In fact, the CFL is not “aggrieved” by the absence of the test results at all, but is instead concerned with their potential use in future investigations. Indeed, the government is explicitly allowed to retain the originals or copies of the evidence in anticipation of future use in criminal proceedings. The Fourteenth Circuit’s order, cloaked in the guise of a motion to return property, is really a categorical motion to suppress with none of its limitations. As such, even if such a motion is granted, the government is still entitled to the seized property under the “good faith” exception.

Nor does the CFL have standing simply because its databases were the ones targeted by the FBI. Lastly, the CFL fails the Pennell test for associational standing, because its individual members have no standing to sue, the litigation is not germane to the CFL’s purpose, and the CFL membership faces a profound conflict of interest in this case.

Second, the plain view doctrine should apply to searches of computers and electronic media. Fourth Amendment jurisprudence has repeatedly held that all types of containers are subject to the same expectation of privacy. Singling out computers for special treatment has no basis in the Fourth Amendment and would lead to absurd results. Far from establishing a “limitless” search, the plain view doctrine is already curtailed in electronic searches by the

requirement that the illegality of the evidence be “immediately apparent”. Creating a special exception for computers would also severely damage law enforcement efforts.

Third, the CDT requirements directly conflict with judicial precedent. They are mutually exclusive with this Court’s recent amendments to the Federal Rules of Criminal Procedure regarding digital searches. Moreover, they have no basis in the Constitution and unconstitutionally delegate power to magistrate judges.

Fourth, the CDT requirements present an unworkable framework for effective law enforcement. In the context of unpredictable electronic searches, an ex ante approach that requires a magistrate judge to have both perfect foresight of eventual problems and mastery of cutting-edge technology is futile. The use of a filter team to segregate case agents from the search would be extremely expensive, grossly inefficient, and significantly hinder the ability of law enforcement to effectively locate critical evidence.

Finally, the CDT requirements unwisely abandon the common law approach to adjudication. Adopting inflexible ex ante rules now would derail the evolving jurisprudence of digital evidence, a field subject to extremely rapid change.

ARGUMENT

I. THE COLLEGIATE FOOTBALL LEAGUE DOES NOT HAVE STANDING.

A. The Respondent Has Improperly Conflated Rule 41(g) and a Motion to Suppress.

Rule 41(g) provides for the return of property unlawfully seized by the government. Fed. R. Crim. P. 41. Prior to 1989, the Rule also provided for suppression of evidence if it was returned to the aggrieved party. That language, however, was eliminated as both confusing and contrary to the evolution of the exclusionary doctrine. See id., Advisory Committee Notes to 1989 Amendments. Today, Rule 41(g) is used solely for the return of property, and not for the suppression of evidence. See Kitty's East v. United States, 905 F.2d 1367, 1372 (10th Cir. 1990) (“Under the rule as it now exists, suppression and return of property are separate and distinct inquiries”).

As such, the Respondent does not have standing under Rule 41 because the Fourteenth Circuit’s order is a motion to suppress rather than a return of property. Rule 41(g) may not be used as a pre-emptive method of suppressing evidence. Indeed, it is common practice for the government to make copies of property before returning it in anticipation of future criminal charges. See J. B. Manning Corp. v. United States, 86 F.3d 926, 928 (9th Cir. 1996) (noting that the “current Rule 41(e) specifically allows the government to impose ‘reasonable conditions’ on the return of property to protect access and use of the property in subsequent proceedings”). As the Advisory Committee notes explain, “[if] the United States has a need for the property in an

investigation or prosecution, its retention of the property generally is reasonable.” Fed. R. Crim. P. 41, Advisory Committee Notes to 1989 Amendments.

Instead, the Respondents are attempting to create for themselves a remedy functionally equivalent to a motion to suppress evidence, but with none of the limitations of the exclusionary rule. This Court has repeatedly held that a court’s authority to suppress evidence must be restricted by the exclusionary rule. See United States v. Payner, 447 U.S. 727, 735-36 (1980) (holding that a federal court could not exercise its equitable supervisory powers to suppress evidence in circumstances where the exclusionary rule did not allow such suppression); United States v. Calandra, 414 U.S. 338, 348 n.6 (1974) (holding that a motion for the return of property “does not constitute a statutory expansion of the exclusionary rule”). See also Grimes v. Comm’r, 82 F.3d 286, 290 (9th Cir. 1996) (holding that Rule 41 does not provide movants “any protection beyond that provided by the exclusionary rule”). “Accordingly, courts must follow the Supreme Court’s exclusionary rule jurisprudence when fashioning suppression remedies under Rule 41(g) or its equitable counterpart.” United States v. Comprehensive Drug Testing, 579 F.3d 989, 1021 (9th Cir. 2009) (en banc) (Ikuta, J., dissenting).

This is important because this Court’s development of the exclusionary rule has made clear that suppression is an extreme remedy, a “last resort, not . . . [a] first impulse.” Hudson v. Michigan, 547 U.S. 586, 591 (2006). See also Herring v. United States, 129 S. Ct. 695, 700 (2009) (“We have repeatedly rejected the argument that exclusion is a necessary consequence of a Fourth Amendment violation.” (citing cases)). This Court has adopted numerous exceptions to the exclusionary rule, including many permissible uses of illegal evidence. See Calandra, 414 U.S. at 351–52 (holding that the exclusionary rule does not apply to grand jury proceedings); United States v. Havens, 446 U.S. 620, 627-28 (1980) (holding that evidence obtained in

violation of the Fourth Amendment can be used to impeach a defendant's testimony at trial); Rakas v. Illinois, 439 U.S. 128, 148-49 (1978) (holding that evidence obtained in violation of one person's Fourth Amendment rights can be used against another person whose Fourth Amendment rights were not violated by the search or seizure). As such, when courts fashion remedies for Fourth Amendment violations, they must be carefully fitted to both the underlying violation and the government's legitimate competing interests in using the illegally seized evidence. See Grimes, 82 F.3d at 291 (“Because the government may now use illegally obtained evidence in a variety of situations, it should be permitted to retain copies of such evidence absent extreme circumstances not apparent from this record.”).

1. The Motion to Suppress Cannot Simply Be Restyled as a Motion to Return Property

The Ninth Circuit claims Payner and Calandra do not apply to these Rule 41 motions because there is no formal “motion to suppress . . . before [the court].” Comprehensive Drug Testing, 579 F.3d at 1001. But this argument is too clever by half. Regardless of how the motion is styled, the substance of the order is the same: barring the government from using information about the players, not to return their property. A true motion for return of property would be a remedy for a party “aggrieved by a deprivation of its property.” Here, rather than being “aggrieved by the deprivation of its property,” the CFL is only “aggrieved by the government’s possession of inculpatory evidence.” Comprehensive Drug Testing, 579 F.3d at 1023 (Ikuta, J., dissenting). In fact, the CFL is not “aggrieved” by the deprivation of the test

results at all, but only by the information's potential publication. Certainly, the storage of the player samples and test results at StarTests have not unduly aggrieved the CFL, and it is hard to imagine any immediate need for their return now other than to frustrate the government's ability to continue its investigation into drug use in professional sports.

In addition, if this were truly a motion for return of property, the government would not necessarily be prohibited from continuing to use information from the property as evidence. Fed. R. Crim. P. 41(g) (if a court grants a motion for return of property, it may "impose reasonable conditions to protect access to the property and its use in later proceedings"). As the dissent in Comprehensive Drug Testing points out, this is a liberal standard: in Ramsden v. United States, 2 F.3d 322 (9th Cir. 1993), the government made a warrantless search and seizure of a briefcase, but was still permitted to preserve copies of the documents in the briefcase. Ramsden, 2 F.3d at 325–27. See also Comprehensive Drug Testing, 579 F.3d at 1023 (Callahan, J., dissenting). Surely in this case, when the government received a valid search warrant, "Ramsden counsels a compromise solution as contemplated by Rule 41(g)." Comprehensive Drug Testing, 579 F.3d at 1023 (Callahan, J., dissenting).

Instead, the effect of the Fourteenth Circuit's order is simply to fashion a broader suppression remedy, which categorically prevents the government from using the seized evidence for any purpose (R. at 16), despite this Court's clear instruction that suppression must be tailored to a specific purpose. Simply labeling it as a motion for "return of property" cannot change its fundamental essence as a categorical suppression remedy.¹

¹ An additional harm of this "alternative categorical suppression remedy" is that it would likely only be brought by wealthy defendants. Most searches occur before the right to counsel attaches, and so such pre-indictment challenges would likely only be exploited by defendants with counsel already.

2. The “Good Faith” Exception Entitles the Government to the Seized Property

Courts have long acknowledged a “good faith” exception to the exclusionary rule. United States v. Leon, 468 U.S. 897 (1984). Though originally applicable to Rule 41(g), the decoupling of a motion for the return of property and suppression of the evidence itself has led several courts to find Leon inapplicable to Rule 41(g). See J. B. Manning Corp. v. United States, 86 F.3d 926, 928 (9th Cir. 1996); Kitty’s East v. United States, 905 F.2d 1367, 1372 (10th Cir. 1990). In holding that the good faith exception was unsuitable for Rule 41(g), the courts noted that the Court’s primary concern in Leon was weighing the benefits of discouraging overbroad warrants against the potential cost of freeing a guilty defendant. See J.B. Manning Corp., 86 F.3d at 928. Recognizing that the recently amended Rule 41(g) provided for no suppression of the evidence, the balancing test was found no longer necessary, and Leon was inapplicable.

The reimagining of Rule 41(g) proposed by the Respondents, however, reintroduces the risk of allowing the guilty to go free. The incorporation of suppression back into Rule 41(g) suggests that Leon is again applicable. See Kitty’s East at 1372 (Leon applies only to “motions to suppress *and their equivalent*”) (emphasis added). Turning to the facts of this case, the alleged illegality of Judge Leon’s “broad warrant” is therefore not dispositive. If suppression is again part of Rule 41(g), then the “good faith” exception shields the law enforcement personnel working under a presumptively valid warrant.

B. The CFL Cannot Challenge the Search Under a “Targeting” Theory.

Additionally, the CFL may not pursue the case as “one against whom the search was directed.” (R. at 10.) While the warrant did explicitly direct the federal agents to seek the “CFL” database, the mere fact that the CFL was “targeted” by the search does not impart standing. See Rakas v. Illinois, 439 U.S. 128, 135 (1978). As this Court has repeatedly explained, Fourth Amendment rights may not be exercised vicariously. See id. at 138 (“A person who is aggrieved by an illegal search and seizure through the introduction of damaging evidence secured by a search of a third person’s premises or property has not had any of his Fourth Amendment rights infringed.”).

C. The CFL Fails the Pennell Test for Associational Standing.

In the absence of individual standing, the CFL is forced to rely upon a theory of associational standing. This Court has recognized that sometimes associations may litigate on behalf of their membership. See NAACP v. Patterson, 357 U.S. 449, 459 (1958) (noting that associations are often a “medium through which its individual members seek to make more effective the expression of their own views”). However, the organization must show the members would have standing in their own rights, that the litigation is germane to the organization’s purpose and that the claim or relief requested does not require the participation of individual members. See Pennell v. City of San Jose, 485 U.S. 1 (1988); Hunt v. Wash. State Apple Adver. Comm’n, 432 U.S. 333 (1977).

1. The Individual Members Have No Standing to Sue.

The CFL fails the first prong of the Pennell test because it cannot demonstrate that its players have standing to sue in an individual capacity. Specifically, the players cannot demonstrate an ownership interest in the test results. The players have voluntarily relinquished their samples to a third party, retaining no possessory interest in the results of the testing. No court has found that the individuals have an ownership interest in the bodily fluids donated for testing, Comprehensive Drug Testing, 579 F.3d at 1022 n.2 (Ikuta, J., dissenting), and it stands to reason that the players therefore cannot demonstrate an ownership interest in the accompanying test results either.

2. The Litigation Is Not Germane to the CFL's Purpose.

The CFL, like other sports organizations, exists primarily as a tool for the franchise owners. Unlike the Player's Association in Comprehensive Drug Testing, which has the sole purpose of "represent[ing] the best interests of MLB players," United States v. Comprehensive Drug Testing, 473 F.3d 915, 926 (9th Cir. 2006), the CFL must juggle several interests along with the player's concerns, including preserving the league's public image and ensuring the continuing profitability of the sport. (R. at 1.) Concealing the positive drug tests of some of its players cannot be said to be "germane" to the purpose of the CFL.

3. The CFL's Membership Has a Profound Conflict of Interest.

An association may also fail to achieve standing if its membership is split over the outcome of the case. See Retired Chicago Police Ass'n v. City of Chicago, 76 F.3d 856, 864-870 (7th Cir. 1996) (noting that such a profound conflict arises when there is a “direct, detrimental effect to some members’ interests”). This requirement serves two purposes. First, it ensures that the association has such a “personal stake or interest in the outcome of the controversy as to assure the concrete adverseness which Art. III requires.” Rakas, 439 U.S. at 131 n.2. An association pulled in two directions by its membership is unlikely to satisfy Article III requirements. Secondly, the requirement relates back to the second Pennell factor, as the litigation is unlikely to be germane to the association’s interests if its membership is in fact split over the case.

In the instant case, the CFL’s player membership will likely be divided. While privacy concerns may trouble some players, others may find the use of controlled substances within the sport objectionable and welcome government intervention. Football, after all, is a professional competitive sport where player salaries often depend upon performance. Thus, certain players may advocate for increased enforcement to level the playing field. Compare NAACP v. Patterson, 357 U.S. 449, 459 (1958) (noting that the association’s members were “in every practical sense identical”). The players and franchises of the CFL therefore cannot be said to have a unified opinion on this case.

II. THE PLAIN VIEW DOCTRINE IS APPLICABLE TO DIGITAL EVIDENCE CASES.

The plain view doctrine permits law enforcement personnel to seize incriminating evidence that they come upon during an otherwise legal search. Coolidge v. New Hampshire, 403 U.S. 443, 465 (1971). It has been applied to every form of evidence. See, e.g., United States v. Horn, 187 F.3d 781, 789 (8th Cir. 1999) (video recordings); United States v. Hargus, 128 F.3d 1358, 1363 (10th Cir. 1997) (file cabinets); Horton v. California, 496 U.S. 128 (1990) (home); Coolidge, 403 U.S. at 465 (car). By requiring the government to waive reliance on the plain view doctrine in cases of digital evidence, the CDT requirements therefore “offer far greater protection to digital files than Fourth Amendment doctrine provides to any category of physical evidence.” Samantha Trepel, Digital Searches, General Warrants, and the Case for the Courts, 10 Yale J.L. & Tech. 120, 138 (2007).

A. The Fourth Amendment Does Not Distinguish Between Different Kinds of Containers.

Nothing in the text of the Fourth Amendment suggests that different types of containers are subject to different constitutional standards. (Certainly the Framers could never have contemplated that computers would receive “Fourth-Amendment-plus” protection.) At one point, this Court attempted to rank different types of containers in terms of their expectations of privacy. Luggage, for example, had high expectations of privacy. See, e.g., United States v. Chadwick, 433 U.S. 1, 12-13 (1977) (“[A] person's expectations of privacy in personal luggage

are substantially greater than in an automobile.”) Other containers, on the other hand, “did not deserve the full protection of the Fourth Amendment.” Arkansas v. Sanders, 442 U.S. 753, 765 n.13 (1979) (“[F]or example, a kit of burglar tools . . . cannot support any reasonable expectation of privacy . . .”).

Soon, though, a plurality of this Court recognized the bankruptcy of such an analytical hierarchy: it had absolutely no basis in the language of the Fourth Amendment, which “protects people and their effects . . . whether they are ‘personal’ or ‘impersonal.’” Robbins v. California, 453 U.S. 420, 426 (1981) (plurality opinion). By 1982, a full majority of this Court rejected the distinctions between containers, finding that “the central purpose of the Fourth Amendment forecloses such a distinction [T]he most frail cottage in the kingdom is absolutely entitled to the same guarantees of privacy as the most majestic mansion.” United States v. Ross, 456 U.S. 798, 822 (1982). See also California v. Carney, 471 U.S. 386, 394 (1985) (rejecting distinction between worthy and unworthy motor vehicles); New Jersey v. T.L.O., 469 U.S. 325, 337-39 (1985) (student’s purse has no less of a protected privacy interest).

The Ninth Circuit has applied this principle approvingly to digital evidence, observing that “Fourth Amendment exceptions and distinctions based solely on a type of technology are ‘unwise[] and inconsistent with the Fourth Amendment.’” United States v. Giberson, 527 F.3d 882, 887 (2008) (quoting Kyllo v. United States, 533 U.S. 27, 41 (2001) (Stevens, J., dissenting)). See also United States v. Gray, 78 F. Supp. 2d 524, 529 (E.D. Va. 1999) (“[S]earches of computer records are no less constitutional than searches of physical records.”).

Accordingly, if this Court were to declare computers worthy of special protection under the Fourth Amendment, it would be going against established judicial doctrine and reading a

nonexistent distinction into the Fourth Amendment. It would also lead to bizarre results. To take a real example, if a law enforcement officer searched a criminal's house for illegal firearms and came across a suspiciously labeled cassette tape, the plain view doctrine permits its seizure and examination. United States v. Bonfiglio, 713 F.2d 932, 936 (2d Cir. 1983). And if the tape turned out to contain evidence of arson, such evidence could not be suppressed at trial. Id. Cases like this have been upheld in many different circuits. See, e.g., United States v. Reyes, 798 F.2d 380 (10th Cir. 1986); United States v. Falcon, 766 F.2d 1469 (10th Cir. 1985); United States v. Gomez-Soto, 723 F.2d 649, 655 (9th Cir. 1984); United States v. DeBardeleben, 823 F.2d 549, 1987 WL 36735 (4th Cir. 1987) (unpublished opinion).

But suppose that same criminal had converted his cassette tape into an MP3 audio file, stored on his hard drive. According to the CDT requirements, this simple act would prevent law enforcement officials from seizing the evidence under a plain view theory. See Comprehensive Drug Testing, 579 F.3d at 1000–01. Indeed, the government may never even find out about its existence if an independent third party has already redacted the hard drive. The arsonist has effectively protected himself from prosecution simply by converting his incriminating evidence to a digital format. Surely the Fourth Amendment cannot tolerate such absurd distinctions.

Attempting to distinguish computer searches also leads to line-drawing issues. The ubiquity of electronics in our everyday lives makes it difficult to decide where this arbitrary line should be drawn. Suppose an agent seizes an iPhone to search for evidence of drug deals, only to find recent phone calls to known terrorist groups. Does that qualify for the plain view exception? What about the contents of a digital camera? Would a DVD be treated any differently from a vinyl record, which essentially operates on the same principle, albeit on a different scale? Moreover, if computers are entitled to special protections, why shouldn't every

other kind of container receive its own set of Fourth Amendment rules? See, e.g., United States v. Giberson, 527 F.3d 882, 888 (2008).

B. Searching the Entire Hard Drive Is Consistent with Existing Fourth Amendment Doctrine.

The chief concern expressed by both the Ninth Circuit and the court below is that the plain view doctrine is too powerful when computer searches involve searching the entire hard drive (R. at 11). See Comprehensive Drug Testing, 579 F.3d at 1005 (“Authorization to search *some* computer files therefore automatically becomes authorization to search all files”) (emphasis in original). But such a concern is no different from prior, non-digital applications of the plain view doctrine. This Court has made clear that a warrant to search a place for specific evidence permits the search of anything in that place where the described evidence could be located:

A lawful search of fixed premises generally extends to the entire area in which the object of the search may be found, and is not limited by the possibility that separate acts of entry or opening may be required to complete the search. Thus, a warrant that authorizes an officer to search a home for illegal weapons also provides authority to open closets, chests, drawers, and containers in which the weapon might be found. A warrant to open a footlocker to search for marihuana would also authorize the opening of packages found inside. A warrant to search a vehicle would support a search of every part of the vehicle that might contain the object of the search. When a legitimate search is under way, and when its purpose and its limits have been precisely defined, nice distinctions between closets, drawers, and containers, in the case of a home, or between glove compartments, upholstered seats, trunks, and wrapped packages, in the case of a vehicle, must give way to the interest in the prompt and efficient completion of the task at hand. *This rule applies equally to all containers, as indeed we believe it must.*

United States v. Ross, 456 U.S. 798, 821–22 (1982) (emphasis added). As a result, officers searching for small items within a person’s home are permitted to go “through the residence with a fine tooth comb.” United States v. Buckley, 4 F.3d 552, 557 (7th Cir. 1993).

Of course, there are limits to this doctrine. The “reasonableness” requirement of the Fourth Amendment prevents the government from tearing down the walls of a house simply because a bullet might be hidden within. U.S. Const. amend. IV. Likewise, it is probably unreasonable for police to search a suspect’s floppy disks for terrorist training videos, or his iPod for evidence of insider trading. But the Fourth Amendment does not require incomplete searches. When a warrant describes items that are small and easily hidden, courts have repeatedly allowed meticulous searches, even of someone’s home. For example, in a case in the Seventh Circuit, an officer was permitted to examine a notebook while ostensibly searching for cocaine because cocaine “is commonly distributed . . . in small vials and envelopes, and thus, is easily concealable in confined areas, such as notebooks,” even though the agent testified he intended to look for things other than cocaine. United States v. Barnes, 909 F.2d 1059, 1069–70 & n.12 (7th Cir. 1990). See also United States v. Pindell, 336 F.3d 1049, 1056 (D.C. Cir. 2003); Buckley, 4 F.3d at 557. If these searches are not overbroad even within the sanctity of a personal residence, surely the sanctity of a hard drive does not warrant a higher level of protection.

In addition, privacy interests are protected by existing limitations within the plain view doctrine itself. The plain view test imposes three requirements to allow warrantlessly seized evidence: first, the officer must have had lawful access to the place where the evidence can be plainly viewed; second, the incriminating nature of the evidence must be “immediately apparent”; third, the officer must have a “lawful right of access” to the object. Horton v. California, 496 U.S. 128, 136–37 (1990).

Applying these requirements provides a strong safeguard for privacy interests. Suppose an officer has a warrant to search the contents of a computer for child pornography. The “immediately apparent” standard of the plain view doctrine requires that the officer can view a file titled “letter to grandma.doc” only to the extent necessary to verify it is not a mislabeled file containing child pornography. David J. S. Ziff, Fourth Amendment Limitations on the Execution of Computer Searches Conducted Pursuant to a Warrant, Note, 105 Colum. L. Rev. 841, 869 (2005). The officer is prohibited from actually reading the letter—if it actually contained, for example, fraudulent tax returns, it cannot be seized under plain view because it cannot plausibly be said to have an “immediately apparent” criminal nature. Id. at 869–70. “Even if an individual file ‘appears suspicious to an officer but further investigation [beyond what is necessary to determine that the file is outside the scope of the warrant] is required to establish probable cause as to its association with criminal activity, the item is not immediately incriminating’ and cannot be seized pursuant to the plain view doctrine.” Id. at 869 (footnote omitted) (quoting *United States v. Byrd*, 2000 WL 491511, at *3 (6th Cir. 2000)).

Indeed, as Judge Bea’s dissent in Comprehensive Drug Testing points out, applying this standard would have defeated the government’s claim in that case without needing to abolish the plain view doctrine altogether. See Comprehensive Drug Testing, 579 F.3d at 1016–17 & n.2 (Bea, J., dissenting) (demonstrating why the evidence could not have been “immediately apparent,” and suggesting an alternative methodology). The Fourteenth Circuit’s fears are therefore unfounded. (R. at 12 (“[The ‘immediately apparent’ prong] of the plain view doctrine . . . fails as a procedural safeguard [because] [w]e have only been able to discover one case in which the court ruled that the criminal character of the documents was not apparent.”).)

It is true that computers can hold significantly more information than any other traditional storage device, causing some courts to consider a “special approach” for computer searches. United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999). See also Orin S. Kerr, Digital Evidence and the New Criminal Procedure, 105 Colum. L. Rev. 279, 303 (2005). But the plain view doctrine provides a file-by-file protection of privacy. Fourth Amendment doctrine applies to individual files rather than to aggregate amounts of information. Each individual file is accorded the same constitutional protections regardless of whether it is in a stack of ten documents or in a computer with ten thousand documents. If we approve of the protection individual documents receive when they are in a stack of ten, then there is no reason to apply a different test simply because the stack has grown. See Ziff, supra, at 869.

C. The Plain View Doctrine Is Key to Law Enforcement Efforts.

“The judicial directive to forswear in advance the plain view doctrine, placed in a different context, is equivalent to demanding that a DEA investigative team engaged in the search of a residence for drugs promise to ignore screams from a closet or a victim tied to a chair.” United States v. Farlow, No. CR-09-38-B-W, 2009 U.S. Dist. LEXIS 112623 at *19 n.3 (D. Me. Dec. 3, 2009). Computers play an increasingly important role in modern life, and therefore also an increasingly important role in modern crime. Eliminating reliance on the plain view doctrine would not only conceal evidence of serious but unrelated imminent criminal activity, but also result in the loss of probative evidence even directly related to the case at hand. For example, in the course of executing a warrant containing a date restriction, agents may discover time-critical evidence indicating the criminal activity has continued well after

investigators previously believed it had ended. By definition, all such evidence uncovered in plain is the fruit of constitutional activity. Accordingly, concealing such evidence surrenders society's compelling interest in prosecuting crime without serving a countervailing privacy interest.

These are not hypothetical concerns. In one recent case, an agent searching a computer pursuant to a warrant to search for evidence of the sale of DDT discovered that the defendant possessed large quantities of child pornography (including videos of his 13-year-old stepdaughter naked) as well as file-sharing software making his child pornography available to others. United States v. Grummer, 08cr4402-DMS (S.D. Cal.). Had the government been required to waive the plain view doctrine as a condition of obtaining that initial warrant, the defendant may very well have been immunized from prosecution.

III. THE GUIDELINES ANNOUNCED IN COMPREHENSIVE DRUG TESTING CONFLICT WITH PRECEDENT AND CAUSE SIGNIFICANT PRACTICAL HARMS.

A. The CDT Requirements Directly Conflict with Judicial Precedent.

1. The CDT Requirements Are Inconsistent with the Supreme Court's Constitutional Judgment.

The CDT requirements contradict this Court's recent amendments to Rule 41 of the Federal Rules of Criminal Procedure. Rule 41 authorizes the government to retain a copy of

“electronically stored information that was seized or copied”. Fed. R. Crim. P. 41(f)(1)(B). Yet both the Ninth Circuit, Comprehensive Drug Testing, 579 F.3d at 1000–01, and the Fourteenth Circuit (R. at 14–16) announced the opposite rule, ordering the government to destroy all its copies of returned data in the absence of specific judicial authorization. (R. at 14–16.). Similarly, the CDT guidelines require the government to “provide the issuing officer with a return disclosing precisely what data it has obtained as a consequence of the search,” Comprehensive Drug Testing, 579 F.3d at 1000, even though the new Rule 41 requires only that the return “describ[es] the physical storage media that were seized or copied.” Fed. R. Crim. P. 41(f)(1)(B).

Neither the Ninth Circuit nor the court below identified the source of their newly announced rules. To the extent that the courts saw the rules as required by the Fourth Amendment, the decisions directly contradict this Court’s own constitutional judgment. But if the rules were intended as part of the federal supervisory power, they are overruled by the new Rule 41 amendments. “[E]ven a sensible and efficient use of the supervisory power . . . is invalid if it conflicts with constitutional or statutory provisions,” Thomas v. Arn, 474 U.S. 140, 148 (1985), and “federal courts have no more discretion to disregard [a] Rule’s mandate than they do to disregard constitutional or statutory provisions,” Bank of Nova Scotia v. United States, 487 U.S. 250, 255 (1988). Nor can the supervisory power be used as a supplement to the Fourth Amendment. In United States v. Payner, 447 U.S. 727 (1980), the Sixth Circuit used the supervisory power to exclude evidence that the Fourth Amendment did not, as a supplement to Fourth Amendment protection. This court reversed, rejecting the use of the supervisory power “as a substitute for established Fourth Amendment doctrine.” Id. at 736 n.8.

2. The CDT Requirements Have No Basis in the Constitution.

The CDT requirements include specification of an ex ante search protocol in the warrant. See Comprehensive Drug Testing, 579 F.3d at 1006 (“The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents.”). See also Raphael Winick, Searches and Seizures of Computers and Computer Data, 8 Harv. J. L. & Tech. 75, 108 (1994) (recommending that law enforcement officials be required to specify a search protocol using “key word searches” ex ante).

But there is no basis in the Fourth Amendment for such warrant requirements. As this Court emphasized in Dalia v. United States, 441 U.S. 238 (1979), the Warrant Clause contains exactly three requirements for a search warrant to issue: an oath or affirmation; probable cause to search; and a particular description of the place to be searched. Id. at 255. Accordingly, this Court rejected ex ante regulations on how warrants are to be executed:

Nothing in the language of the Constitution or in this Court's decisions interpreting that language suggests that . . . warrants also must include a specification of the precise manner in which they are to be executed. On the contrary, 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 of course to the general Fourth Amendment protection “against unreasonable searches and seizures.”

. . . .

It would extend the Warrant Clause to the extreme to require that, whenever it is reasonably likely that Fourth Amendment rights may be affected in more than one way, the court must set forth precisely the procedures to be followed by the executing officers. Such an interpretation is unnecessary, as we have held . . . the manner in which a warrant is executed is subject to later judicial review as to its reasonableness.

Dalia v. United States, 441 U.S. 238, 255–258 (1979) (footnotes omitted). The “general Fourth Amendment protection” described by the court is usually measured ex post in motions to suppress, not ex ante in the form of procedures to be followed to execute the warrant. See, e.g., United States v. Grubbs, 547 U.S. 90 (2006) (overturning ex ante Ninth Circuit rules on the execution of anticipatory warrants). This principle has been repeatedly applied to the digital realm. See, e.g., United States v. Brooks, 427 F.3d 1246, 1251 (10th Cir. 2005) (“At the outset, we disagree with [defendant] that the government was required to describe its specific search methodology.”); United States v. Upham, 168 F.3d 532, 537 (1st Cir. 1999) (“The . . . warrant did not prescribe methods of recovery or tests to be performed, but warrants rarely do so. The warrant process is primarily concerned with identifying what may be searched or seized-not how-and whether there is sufficient cause for the invasion of privacy thus entailed.”); United States v. Cartier, No. 2:06-cr-73, 2007 WL 319648, at *3 (D. N.D. Jan. 30, 2007) (“[T]he warrant is not defective because it did not include a computer search methodology.”); United States v. Kaechele, 466 F.Supp.2d 868, 889 (E.D. Mich. 2006) (rejecting claim that warrant was overbroad because it lacked a search protocol); United States v. Shinderman, No. CRIM. 05-67-P-H, 2006 WL 522105, at *19 (D. Me. Mar. 2, 2006) (“[T]here is no Fourth Amendment requirement that search warrants spell out the parameters of computer searches where the warrant provides particularity as to what is being searched for.”); United States v. Lloyd, No. 98 Crim. 529, 1998 WL 846822, at *3 (E.D.N.Y. Oct. 5, 1998) (rejecting claim that warrant should have described computer search method).

In addition, the Ninth and Fourteenth Circuits also announced that henceforth, a third party or “specialized personnel” would be required to segregate and redact non-responsive data. This approach is problematic because this Court has already rejected the idea that different rules

are necessary for “‘third party’ search[es]” because “[t]he Fourth Amendment itself has struck the balance between privacy and public need.” Zurcher v. Stanford Daily, 436 U.S. 547, 553, 559 (1978).

3. The CDT Requirements Bestow Enforcement Powers upon Magistrate Judges that Are Unconstitutional.

To enforce these new requirements, the Ninth and Fourteenth Circuits awarded magistrate judges powers that are simply unconstitutional. For example, if the government doesn’t consent to a waiver of plain view, the magistrate judge can “deny the warrant altogether.” Comprehensive Drug Testing, 579 F.3d at 998. But the Warrant Clause of the Fourth Amendment provides no justification for according magistrate judges this power. As noted above, the only requirements for facial validity of a warrant are an oath or affirmation, probable cause, and particularity. If the magistrate can refuse to sign warrants unless the government makes additional promises as to how the warrant will be executed, then magistrate judges can shape the Fourth Amendment in each case as they see fit. See In re Worksite Inspection of Quality Products, Inc., 592 F.2d 611, 613 (1st Cir. 1979) (noting the limited role of magistrate judges in issuing search warrants); Ex parte United States, 287 U.S. 241, 250 (1932) (holding that a magistrate judge did not have discretion to refuse to issue an arrest warrant after the grand jury returned an indictment, and noting that “the refusal of the trial court to issue a warrant . . . is, in reality and effect, a refusal to permit the case to come to a hearing upon either questions of law or fact, and falls little short of a refusal to permit the enforcement of the law”);

Abraham S. Goldstein, The Search Warrant, the Magistrate, and Judicial Review, 62 N.Y.U. L. Rev. 1173, 1196 (1987) (“The few cases on [whether a magistrate judge can refuse to issue a warrant on the ground that the search may be executed unconstitutionally] hold that a judge has a 'ministerial' duty to issue a warrant after 'probable cause' has been established.”).

Moreover, the mere act of asking magistrate judges to supervise the execution of these warrants raises serious constitutional issues. The Fourth Amendment requires that search warrants be issued by “neutral and detached” judicial officers; “[w]hatever else neutrality and detachment might entail, it is clear that they require severance and disengagement from activities of law enforcement.” Shadwick v. City of Tampa, 407 U.S. 345, 350 (1972). Accordingly, this Court has historically been wary of judicial supervision of the execution of a search warrant. In Lo-Ji Sales, Inc. v. New York, 442 U.S. 319 (1979), a Town Justice accompanied law enforcement in their execution of a search warrant upon an adult bookstore. Though the state argued that his presence served to ensure that only evidence within the scope of the warrant would be seized, this Court held that the Town Justice’s personal determinations and supervision manifested “an erosion” of neutrality and detachment. Id. at 326–27. This is exactly the kind of hands-on supervision envisioned by the CDT guidelines yet repeatedly rejected by this Court.

B. The CDT Requirements Are Unworkable in Practice.

The CDT requirements impose tremendous costs upon law enforcement. It requires ex ante approval of search protocols when ex post review is a much more realistic approach. In addition, the requirement that “specialized personnel or an independent third party” must be

involved in every case of digital evidence is dangerous, inefficient, and a “crushing expense” for police departments. Comprehensive Drug Testing, 579 F.3d at 1013 (Callahan, J., dissenting).

1. Ex Ante Approval of Search Protocols Would Serve Little Purpose.

As previously noted, courts have never found that the Fourth Amendment requires specification of how the warrant is to be executed. This principle is especially relevant in the context of computer searches, which are “contingent, fact-bound, and quite unpredictable.” Orin S. Kerr, Searches and Seizures in a Digital World, 119 Harv. L. Rev. 531, 574 (2005). Before beginning a computer search, agents often know next to nothing about the nature of the computer. What operating system does the computer use? What other software is in place? What precautions should be taken? And under these circumstances, which forensic tool would be best for the job? All of these questions cannot be answered without at least looking at the hard drive—”[i]n a sense, the forensic process is a bit like surgery: the doctor may not know how best to proceed until he opens up the patient and takes a look.” Id. at 575.

Accordingly, even a skilled forensic expert cannot predict exactly what techniques will be necessary to find the information sought by the warrant. Asking magistrate judges (who cannot be expected to have extensive expertise in computer forensics) to review and approve search strategies in advance would therefore be a largely futile exercise.

This case can be distinguished from cases like United States v. Tamura, 694 F.2d 591 (9th Cir. 1982), where the Ninth Circuit required judges to approve offsite searches, so as to prevent overbroad seizures before they occurred. Such seizures can be reviewed ex ante because

they only occur once. But judges cannot exercise the same ex ante control over a computer search—they would literally have to stand alongside the forensics expert approving every step along the way. The decision tree the agent employs in these searches is generally “too long and complex” for judges to approve ex ante. Kerr, Searches and Seizures, *supra* at 576.

2. The Use of Filter Teams Is Inefficient and Dangerous.

Requiring a filter team presupposes that conducting computer searches involves little more than seizing discrete and easily identified files, and therefore any filter team with sufficient technological expertise can substitute for a case agent.

In reality, substituting a filter team for an experienced case agent would be akin to substituting a dictionary for a literary translator. Computer searches are “as much an art as a science.” United States v. Brooks, 427 F.3d 1246, 1252 (10th Cir. 2005). Case agents must identify what information is relevant and falls within the scope of a warrant in a hard drive containing millions of files. This demands much more than just technological expertise; it requires a meticulous knowledge of every detail in the case, an intuitive familiarity with the law, and years of experience with the practices and customs of the criminals targeted. In cases of national security, agents must deal with terrorists and foreign spies who have received extensive training in how to cover their tracks. Moreover, agents on these cases frequently also must be fluent in multiple languages and have access to highly classified information.

As such, the CDT requirements significantly and needlessly delay the process of obtaining time-sensitive evidence. Case agents will need to spend weeks or months educating

filter teams in the details of the case and the underlying law. But the case agent's other skills—her years of experience and intuition—cannot be taught; this means that filter teams may very well miss critical evidence that a case agent would not.

Moreover, the government's computer forensics labs are already overburdened. The Digital Evidence Section of the FBI processed 2.57 petabytes in 2007,² but faces both funding cuts and a backlog of hundreds of cases still awaiting digital evidence analysis. Department of Justice Office of the Inspector General, The Federal Bureau of Investigation's Efforts to Combat Crimes Against Children, Audit Report 09-08, at 53 (2009). Requests for forensic analysis can take up to nine months to be fulfilled. Id. at 55. Learning entire cases and meticulously documenting compliance with the filter team requirement would impose a massive burden on an already strained cybercrime lab.

3. Hiring Independent Third Parties Is Prohibitively Expensive and Risky.

These problems are only magnified if the government employs an independent third party. Hiring these third parties is prohibitively expensive: previous cases in which the government had to employ special masters to separate legally privileged electronic materials have cost hundreds of thousands of dollars.

Third party searchers also risk the integrity and security of evidence. The government may lose admissible evidence if a third-party searcher fails to protect against security breaches, employee misconduct, or evidence contamination. In many instances, a computer searcher must

² One petabyte is equivalent to 1,024 terabytes, and one terabyte is equivalent to 1,024 gigabytes. As printed text, each petabyte is roughly equivalent to 250 billion double-sided pages, a stack of paper 10,000 miles high.

have access to highly sensitive information, such as the name of an informant or classified materials, in order to comprehend what he is seeing. The United States cannot afford to entrust the security of sensitive information or the viability of its cases to private contractors whose employees the government cannot hire, fire, or supervise.

Nor will the use of an outside filter team provide an additional protection to legitimate privacy interests. Finding relevant evidence on a computer subject to a lawful search means *someone* is going to have to see the contents of the hard drive. Using an outside filter team would only protect criminals by placing incriminating information beyond the reach of law enforcement officers with legitimate investigatory reasons to examine a computer.

Lastly, neither the Ninth nor the Fourteenth Circuit explains how third parties are liable for contraband. As Judge Bea points out in dissent, could a third party computer technician “who comes across child pornography yet refuses to report it immediately, or returns it as part of data seized and searched,” be held liable for possession of child pornography? Comprehensive Drug Testing, 579 F.3d at 1019 (Bea, J, dissenting). This is the cost of “issuing bright line rules at the expense of developing the law through the common law method.” Id.

C. The CDT Requirements Unwisely Abandon the Common Law Method.

It is undisputed that plain view doctrine in the context of digital evidence represents an area where Fourth Amendment doctrine has yet to mature. See, e.g., Kerr, Digital Evidence, supra at 280 (noting that courts have just begun to interpret the Fourth Amendment differently in computer cases). Accordingly, courts should “allow the contours of the plain view doctrine to

develop incrementally through the normal course of fact-based adjudication.” Comprehensive Drug Testing, 579 F.3d at 1013 (Callahan, J., dissenting). This is especially important in a field where technology improves exponentially every month. Through gradual ex post review, the jurisprudence can develop sensibly alongside the technologies that arise. In addition, courts can look to Congress for guidance, as legislative bodies have competitive advantages in setting out bright-line rules through deliberation and expert testimony. See Comprehensive Drug Testing, 579 F.3d at 1018 (Bea, J., dissenting).

Virtually every circuit currently takes this approach. See, e.g., United States v. Turner, 169 F.3d 84, 88 (1st Cir. 2009); United States v. Miranda, 325 Fed. Appx. 858, 860 (11th Cir. 2009); United States v. Herndon, 501 F.3d 683, 693 (6th Cir. 2007); United States v. Raney, 342 F.3d 551, 559 (7th Cir. 2003); United States v. Walser, 275 F.3d 981, 987 (10th Cir. 2001), cert. denied, 535 U.S. 1069, 122 S.Ct. 1943, 152 L.Ed.2d 847 (2002); Carey, 172 F.3d at 1274 (implicitly recognizing the plain view exception but not delineating its precise scope); United States v. Kim, --- F.Supp.2d ----, 2009 WL 5185389, at *12 (S.D. Tex. 2009). See also Comprehensive Drug Testing, 579 F.3d at 1018 n.3 (Bea, J., dissenting).

By contrast, issuing “bright-line diktats” in a field evolving exponentially would short-circuit the common law process. The courts have only had a handful of years to grapple with the application of this doctrine to these emerging technologies. Resorting to ex ante rules now only make it difficult for courts to adapt to technological advancement. In addition, as described above, the “fact-intensive” nature of computer forensics searches lend to ex post standards rather than ex ante rules.

Moreover, existing Fourth Amendment doctrine as applied to ex post review of computer searches provides an excellent balance between privacy interests and societal interest in prosecution of crime. As described above, the “immediately apparent” prong of the plain view exception ensures that agents cannot simply “explore” around a computer. See Carey, 172 F.3d at 1273 (rejecting the government’s plain view argument).

By contrast, the CDT requirements mean that every computer search warrant ever obtained and executed in the Ninth and Fourteenth Circuits is presumably now unconstitutional, as no one could have predicted these requirements. Every criminal case with a search warrant involving computers has suddenly been awarded a new suppression issue. Barring some kind of new, supplementary retroactivity jurisprudence from the two circuits, this illustrates the dangers of sudden and significant departures from stare decisis. The common law approach, “recogniz[ing] the limitations of human ingenuity and wisdom,” allows us to “discern the most sensible rule” by “limiting our decisions as precisely as possible to the case at hand.” Comprehensive Drug Testing, 579 F.3d at 1018 (Bea, J., dissenting).

CONCLUSION

The CFL has failed to demonstrate their standing for the Rule 41(g) motion. Furthermore, requiring the government to forswear reliance on the plain view doctrine and follow the requirements of Comprehensive Drug Testing finds no basis in the Constitution and threatens to severely hinder effective enforcement of the law. Freezing the development of our evolving Fourth Amendment jurisprudence is a needlessly overbroad solution to a problem better dealt with through the traditional common law method. The judgment of the Fourteenth Circuit should be reversed.

Respectfully submitted,

Competitor #17

Counsel for Petitioner

APPENDIX A

U.S. Const. amend. IV.

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

APPENDIX B

Federal Rule of Criminal Procedure

Rule 41. Search and Seizure

(f) Executing and Returning the Warrant.

(1) Warrant to Search for and Seize a Person or Property.

...

(B) Inventory. An officer present during the execution of the warrant must prepare and verify an inventory of any property seized. The officer must do so in the presence of another officer and the person from whom, or from whose premises, the property was taken. If either one is not present, the officer must prepare and verify the inventory in the presence of at least one other credible person. In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.

...

(g) Motion to Return Property.

A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return. The motion must be filed in the district where the property was seized. The court must receive evidence on any factual issue necessary to decide the motion. If it grants the motion, the court must return the property to the movant, but may impose reasonable conditions to protect access to the property and its use in later proceedings.