
No. 2009-H20

**IN THE
SUPREME COURT OF THE UNITED STATES
October Term 2009**

UNITED STATES OF AMERICA,
Petitioner,

v.

**STARTESTS, INC. and the
COLONIAL FOOTBALL LEAGUE,**
Respondents.

**On Writ of Certiorari to the
United States Court of Appeals
for the Fourteenth Circuit**

BRIEF FOR PETITIONER

Team No. 13

ATTORNEYS FOR PETITIONER

QUESTIONS PRESENTED

- I. Whether a professional football league has standing to sue for the return of property documenting illegal drug use by its players, when a third party created those documents and had possession of them at the time of their seizure?
- II. Whether the “plain view” exception to the Fourth Amendment’s warrant requirement applies to digital searches of files on a computer similar to its application in the search of a house, a car, or paper copies of those files?
- III. Whether to burden a federal magistrate judge with the heightened particularity requirements listed by the court below and in *United States v. Comprehensive Drug Testing, Inc.*, when the judge issues a warrant authorizing the seizure of all computer equipment and files to accommodate the complex decryption and search algorithms necessary in those cases?

TABLE OF CONTENTS

Page

QUESTIONS PRESENTED..... i

TABLE OF AUTHORITIES.....v

OPINIONS BELOW.....1

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED1

STATEMENT OF THE CASE.....1

SUMMARY OF THE ARGUMENT6

ARGUMENT AND AUTHORITIES9

 I. THE CFL DOES NOT HAVE DIRECT OR ASSOCIATIONAL STANDING TO SUE
 UNDER RULE 41(g) FOR THE RETURN OF STARTESTS’ DATABASES10

 A. Even if the CFL Has Property Interest in StarTests’ Databases, the CFL
 Was Not One Against Whom the FBI’s Search Was Directed.....11

 B. The CFL Does Not Have Associational Standing to Sue for the Return of
 StarTests’ Databases13

 1. The player’s privacy interests are not germane to the CFL’s
 organizational purpose13

 2. The players do not have a legitimate expectation of privacy in their
 illegal drug test results which they gave to a private party14

 3. The claim asserted requires individual player participation in the
 lawsuit15

 II. THE PLAIN VIEW DOCTRINE APPLIES TO A SEARCH OF DIGITAL EVIDENCE
 AUTHORIZED BY A WARRANT CONTAINING A DESCRIPTION OF THE PLACE TO
 BE SEARCHED AND THE SPECIFIC INFORMATION TO BE SEIZED16

 A. The StarTests Warrant Issued to the FBI Complied with the Probable
 Cause and Particularity Requirements of the Fourth Amendment17

 1. The FBI had probable cause to believe that StarTests’ facilities
 contained test results confirming the five named players’ use of illegal
 steroids18

2. The StarTests warrant particularly described the facility in Millersville, Wythe as the place of search and seizure	19
3. The StarTests warrant specifically itemized the search and seizure of StarTests’ computer records and storage devices	19
4. The StarTests warrant particularly limited the search of the digital evidence to “information reasonably related to the investigation into the five named players’ illegal steroid use”	20
<i>a. A Fourth Amendment search of digital evidence occurs at the time an agent views a particular storage location on the storage device</i>	<i>21</i>
<i>b. A Fourth Amendment seizure of digital evidence occurs at the time an agent takes the storage device, and a plain view seizure of digital evidence occurs at the time an agent views data on the screen</i>	<i>22</i>
<i>c. Based on the facts in this case, the warrant particularity requirements do not need to change to limit the scope of a lawful Fourth Amendment search of digital evidence</i>	<i>23</i>
B. The Government Agents’ Seizure of the Additional Drug Test Results that Appeared in Plain View Was Within the Scope of the Agents’ Lawful Search for the Results on the Five Players Listed in the Warrant	25
1. The FBI computer forensic agents lawfully entered StarTests facilities with the right to search, seize, or make copies of computer storage devices.....	26
2. The computer forensics agents lawfully accessed the database files containing the drug test results for the five named players	27
3. The files containing the illegal steroid tests for the five named players also contained drug test results for other players and drug test results for cocaine, marijuana and hallucinogens.....	29
C. The Fourteenth Circuit Court of Appeals Erred when It Forced the Government to Return or Destroy the Database Information, Including the Copies	30

1. Even if this Court finds the Rule 41(g) motion reasonable, the Fourteenth Circuit Court of Appeals erred by forcing the government to destroy the copies of StarTests’ database files containing the additional drug test information.....	30
2. The Fourteenth Circuit Court of Appeals erred when it found that its exercise of Rule 41(g) was reasonable.....	32
<i>a. By ignoring the findings of fact in the record, the Fourteenth Circuit Court of Appeals abused its discretion in its application of the first, third, and fourth factors.....</i>	<i>33</i>
<i>b. The Fourteenth Circuit Court of Appeals also erred as a matter of law in its application of the third factor</i>	<i>34</i>
 III. THE HEIGHTENED PARTICULARITY REQUIREMENTS IMPOSED BY THE FOURTEENTH CIRCUIT COURT OF APPEALS CONTRADICT THIS COURT’S PRECEDENT AND ARE UNNECESSARY GIVEN THE FOURTH AMENDMENT SAFEGUARDS ALREADY IN PLACE	 35
A. This Court Has Rejected Heightening the Particularity Requirements Above Those Stated in the Fourth Amendment.....	35
B. Forcing the Government to Specify Its Search Method in Advance Presents Immense Practical Difficulties	37
C. Indiscriminate Suppression Remedies Are Not a Reasonable Means to Curb Potentially Unlawful Searches	38
 CONCLUSION.....	 40
 APPENDICES:	
APPENDIX “A”: CONSTITUTIONAL PROVISIONS.....	A-1
APPENDIX “B”: FEDERAL RULES.....	B-1

TABLE OF AUTHORITIES

	<i>Page(s)</i>
CASES:	
<i>Alderman v. United States</i> , 394 U.S. 165 (1969).....	10
<i>Andresen v. Maryland</i> , 427 U.S. 463 (1976).....	17, 19, 20, 24, 27
<i>Arizona v. Hicks</i> , 480 U.S. 321 (1987).....	23, 24, 29
<i>Ark. Chronicle v. Murphy</i> , 183 F. App'x 300 (4th Cir. 2006).....	38
<i>Bd. of Educ. v. Earls</i> , 536 U.S. 822 (2002).....	14, 15
<i>Berger v. New York</i> , 388 U.S. 41 (1967).....	20
<i>California v. Greenwood</i> , 486 U.S. 35 (1988).....	14
<i>Comprehensive Drug Testing v. United States</i> , 579 F.3d 989 (9th Cir. 2009) (en banc).....	22, 23, 24, 35
<i>Coolidge v. New Hampshire</i> , 403 U.S. 443 (1971).....	16, 25, 26
<i>Dalia v. United States</i> , 441 U.S. 238 (1979).....	37
<i>Groh v. Ramirez</i> , 540 U.S. 551 (2004).....	17, 20
<i>Herring v. United States</i> , 129 S. Ct. 695 (2009).....	28, 38, 39
<i>Horton v. California</i> , 496 U.S. 128 (1990).....	16, 25, 26, 29

<i>Hudson v. Michigan</i> , 547 U.S. 586 (2006).....	38
<i>Hunt v. Wash. Apple Adver. Comm’n</i> , 432 U.S. 333 (1977).....	11, 13
<i>Illinois v. Gates</i> , 462 U.S. 213 (1983).....	18, 38
<i>In re Search of Kitty’s E.</i> , 905 F.2d 1367 (10th Cir. 1990)	32, 33, 34
<i>Int’l Union v. Brock</i> , 477 U.S. 274 (1986).....	15
<i>J.B. Manning Corp. v. United States</i> , 86 F.3d 926 (9th Cir. 1996)	32
<i>Jones v. United States</i> , 362 U.S. 257 (1960).....	11, 12
<i>Katz v. United States</i> , 389 U.S. 347 (1967).....	11, 12, 14
<i>Kiesel Co. v. Householder</i> , 879 F.2d 385 (8th Cir. 1989)	34
<i>Kyllo v. United States</i> , 533 U.S. 27 (2001).....	21
<i>Maryland v. Garrison</i> , 480 U.S. 79 (1987).....	19, 20, 27
<i>Ohio v. Robinette</i> , 519 U.S. 33 (1996).....	16, 17
<i>Paton v. LaPrade</i> , 524 F.2d 862 (3d Cir. 1975).....	31
<i>Payton v. New York</i> , 445 U.S. 573 (1980).....	29
<i>Pennell v. City of San Jose</i> , 485 U.S. 1 (1988).....	13

<i>Pieper v. United States</i> , 604 F.2d 1131 (8th Cir. 1979)	32, 33
<i>Rakas v. Illinois</i> , 439 U.S. 128 (1978).....	10, 11, 12
<i>Ramsden v. United States</i> , 2 F.3d 322 (9th Cir. 1993)	9, 32, 33, 34
<i>Richey v. Smith</i> , 515 F.2d 1239 (5th Cir. 1975)	32, 35
<i>SEC v. Coldicutt</i> , 258 F.3d 939 (9th Cir. 2001)	9
<i>SEC v. O'Brien</i> , 467 U.S. 735 (1984).....	14
<i>Singleton v. Wulff</i> , 428 U.S. 106 (1976).....	10
<i>Smith v. Maryland</i> , 422 U.S. 735 (1979).....	12, 14
<i>Stanford v. Texas</i> , 379 U.S. 476 (1965).....	37
<i>Texas v. Brown</i> , 460 U.S. 730 (1983).....	16, 25, 26, 29
<i>United States v. Alexander</i> , 574 F.3d 484 (8th Cir. 1987)	28
<i>United States v. Calandra</i> , 414 U.S. 338 (1974).....	39
<i>United States v. Carey</i> , 172 F.3d 1268 (10th Cir. 1999)	20, 22, 24, 27, 29
<i>United States v. Eylicio-Montoya</i> , 18 F.3d 845 (10th Cir. 1994)	9, 10
<i>United States v. Farlow</i> , No. CR-09-38-B-W, 2009 WL 4728690 (D. Me. Dec. 3, 2009)	38

<i>United States v. Giberson</i> , 527 F.3d 882 (9th Cir. 2008)	21, 22, 28
<i>United States v. Grubbs</i> , 547 U.S. 90 (2006).....	17, 35, 37, 40
<i>United States v. Hay</i> , 231 F.3d 630 (9th Cir. 2000)	26
<i>United States v. Hill</i> , 459 F.3d 966 (9th Cir. 2006)	38
<i>United States v. Hill</i> , 322 F. Supp. 2d 1081 (C.D. Cal. 2004)	21, 28
<i>United States v. Jacobsen</i> , 466 U.S. 109 (1987).....	22
<i>United States v. Karo</i> , 468 U.S. 705 (1984).....	21
<i>United States v. Leon</i> , 468 U.S. 897 (1984).....	39
<i>United States v. Marolf</i> , 173 F.3d 1213 (9th Cir. 1999)	9
<i>United States v. Miller</i> , 425 U.S. 435 (1976).....	14
<i>United States v. Padilla</i> , 508 U.S. 77 (1993).....	13
<i>United States v. Ross</i> , 456 U.S. 794 (1982).....	27
<i>United States v. Search of Law Office, Residence & Storage Unit Alan Brown</i> , 341 F.3d 404 (5th Cir. 2003)	31, 32, 34
<i>United States v. Tamura</i> , 694 F.2d 591 (9th Cir. 1987)	22, 23
<i>United States v. Turner</i> , 169 F.3d 84 (1st Cir. 1999).....	28

<i>United States v. Upham</i> , 168 F.3d 532 (1st Cir. 1999).....	20
<i>Warth v. Seldin</i> , 422 U.S. 490 (1975).....	11, 12, 15
<i>Zurcher v. Stanford Daily</i> , 436 U.S. 547 (1978).....	20, 26, 37

CONSTITUTIONAL PROVISIONS AND FEDERAL RULES:

Fed. R. Crim. P. 41(g).....	<i>passim</i>
U.S. Const. amend. IV	<i>passim</i>

LAW REVIEWS:

Orrin S. Kerr, <i>Searches and Seizures in a Digital World</i> , 119 Harv. L. Rev. 531 (2005).....	21
Aaron Stanley, <i>The Continuing Evolution of Consent and Authority in Digital Search and Seizure</i> , 19 Fordham Intell. Prop. Media & Ent. L.J. 179 (2008).....	23

INTERNET RESOURCES:

LexisNexis Discovery Services, <i>How Many Pages in a Gigabyte</i> , http://www.lexisnexis.com/applieddiscovery/ lawlibrary/whitePapers/ADI_FS_PagesInA Gigabyte.pdf (last visited Jan. 8, 2010)	21
--	----

Steve Lohr,

Microsoft Tackles the Child Pornography Problem,
N.Y. Times Bits Blogs, Dec. 16, 2009,

<http://bits.blogs.nytimes.com/2009/12/16/microsoft-tackles-the-child-pornography-problem/>

23, 28

OPINIONS BELOW

The opinion of the United States District Court for the District of Wythe (No. 2010-W20) is unreported, but it appears in the record at pages 1–6. The opinion of the United States Court of Appeals for the Fourteenth Circuit (No. 2010-W23) is also unreported, but it appears in the record at pages 7–19.

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

This case involves the application of the Fourth Amendment of the United States Constitution, which is included as Appendix “A.” This case also involves the application of Fed. R. Crim. P. 41(g), which is included as Appendix “B.”

STATEMENT OF THE CASE

This case involves the application of traditional search and seizure doctrine in an age of computer-based media. Pursuant to a warrant, the FBI searched and seized computer storage devices from StarTests, Inc. (R. at 1.) StarTests subsequently filed a Rule 41(g) motion for the return of property, which it alleges the FBI seized unlawfully. (R. at 1.)

Drug Use in the League. In 2008, widespread media coverage caused the FBI to open an investigation into the distribution and use of illegal steroids by players in the Colonial Football league (CFL). (R. at 7.) During its investigation, the FBI found that players in the CFL were participating in this steroid drug ring to further the marketability of football as well as their personal status in the league. (R. at 7–8.)

The FBI also discovered that the CFL knew of the illegal drug abuse long before the FBI’s involvement. (R. at 1.) In 2005, the CFL hired StarTests, Inc. (StarTests), athlete drug-testing specialists, to investigate the use of illegal drugs in the CFL. (R. at 1.) To entice the franchises to agree to an investigation of their players, the CFL promised that StarTests would not disclose

individual results to the CFL, that all results would remain confidential in StarTests' possession, and that StarTests would only report drug use percentages to the CFL. (R. at 1, 7.) The CFL's interest in the results was to determine whether it should expand its testing program. (R. at 1.)

The FBI Investigation. At the outset of its investigation, the FBI uncovered an extensive network of distributors and users of illegal steroids within the CFL. (R. at 7.) As a starting point to the broader investigation, the FBI focused on five specific players, whom it believed acquired and used illegal performance-enhancing drugs. (R. at 8.) The FBI found paper trails of drug dealings, gathered eyewitness accounts from informants inside the players' organizations, and taped discussions of the players describing the sale and distribution of illegal steroids. (R. at 7.)

Later in the investigation, the FBI learned of StarTests' drug test program. (R. at 8.) The FBI immediately contacted a federal magistrate judge and presented its evidence supporting probable cause for a search warrant to obtain the drug test records from StarTests' facilities. (R. at 8.) The FBI requested that the search warrant include all computer and electronic storage equipment, physical documents, and urine samples located at the StarTests facility in Millersville, Wyeth.¹ (R. at 8.) Given the massive quantity of data and the likelihood of encryption, mislabeling, and deception in the storage of the information, the magistrate judge issued the warrant, subject to several restrictions. (R. at 2, 8.) First, law enforcement personnel trained in computer forensics should be on-site to determine the necessity of seizing a piece of equipment. (R. at 2, 8.) Second, the specially trained personnel should search only the digital data that is "reasonably related" to the five named players' illegal steroid use. (R. at 2, 8.) Lastly, the FBI must then return or destroy the remainder of the information. (R. at 2, 8.)

¹ Note that only the search related to the electronically stored data is at issue in this case.

Finding the Digital Evidence. StarTests' advanced concealment measures to keep the drug test results confidential surprised even the computer forensics agents, who executed the search warrant. (R. at 2.) Agents learned that nearly every single computer at StarTests contained some piece of the information sought under the warrant, but no single computer contained all of the information. (R. at 2.) At the motions hearing, StarTests' representatives described the division of the information into three separate files, no two of which could be found on any single computer. (R. at 2 & n.3.) The file with the drug test results only contained anonymous ID numbers, a different file contained names and personal health information, and a third file contained names and respective ID numbers. (R. at 2 & n.3.) StarTests encrypted some of the files, and it stored some of the files on hidden virtual drives. (R. at 2.) StarTests designed this method, called "computer hopping," to prevent even its own employees from piercing its confidentiality agreement with the CFL. (R. at 2 n.3.)

Given the complicated nature of the search and the inability of the StarTests employees to aid the process, the computer forensic agents seized or made copies of the necessary computer equipment from the facility. (R. at 2.) Once at their own facility, the computer forensics agents located and decrypted the three files that StarTests' employees told them contained the information. (R. at 2.) After finding and decoding the files, the agents inadvertently found additional drug test information. (R. at 5–6.) First, a look at each player's grid immediately revealed results for other controlled substances, such as cocaine, marijuana, and certain hallucinogens, because those results were placed "alongside" the illegal steroid tests result. (R. at 6.) Second, in the process of matching the identification numbers from the one file to the test results in the other file, the FBI agents came across the test results of illegal substances for some other players as well. (R. at 5.) As a result, the FBI inventoried and copied both the information

specified in the warrant as well as the additional drug test information, which it came across inadvertently. (R. at 6.) The FBI then returned StarTests' equipment, as required by the warrant. (R. at 2.)

The District Court. StarTests and the CFL since filed a motion with the United States District Court of Wythe for the return of records and equipment, pursuant to Fed. R. Crim. P. 41(g). (R. at 2–3, 9.) Specifically, the Plaintiffs claimed that information seized, other than that involving the five players listed in the warrant, was outside the scope of the warrant and should be returned or destroyed. (R. at 2–3.) The government countered, first asserting that the CFL did not have standing to sue since it was not the victim of the search. (R. at 3.) Second, the government argued that the “plain view” exception to a warrantless seizure of information should apply, since the agents found the additional information in the course of a reasonable search for the information specified in the warrant. (R. at 4.)

The district court rejected the government's argument that the CFL does not have standing. The district court found that the CFL has associational standing because the players have individual standing to sue, the players' participation in the suit is unnecessary because of the equitable nature of the remedy, and that the CFL has sufficient contractual obligations to protect the players' privacy. (R. at 3.) The district court further held that the StarTests warrant satisfied Fourth Amendment “particularity” requirements, because the limits on its scope was similar to other valid digital evidence warrants. (R. at 4.) The district court, using the plain view principles set forth by this Court, found that the FBI lawfully accessed the additional drug test information, because the agents narrowly tailored the search to find the information on the five players named. Lastly, the court found that the additional illegal activity was immediately apparent once the files containing the search warrant information were concatenated. (R. at 5–

6.) Thus, the district court held that the FBI seized the additional drug test information in plain view. (R. at 6.)

The Court of Appeals. On appeal, the Fourteenth Circuit Court of Appeals affirmed the district court on the CFL's standing. (R. at 10.) However, the Fourteenth Circuit Court of Appeals added that the CFL may have been "one against whom the search was directed," since the CFL paid for the drug testing and because StarTests labeled the data "CFL drug test databases." (R. at 9–10.)

The Fourteenth Circuit Court of Appeals, however, overruled the district court and held that the plain view doctrine fails to provide sufficient safeguards in digital evidence cases. (R. at 17.) Moreover, the court adopted additional warrant requirements from the Ninth Circuit Court of Appeals. (R. at 17.) Those new requirements are as follows: 1) the government must waive reliance on the plain view doctrine; 2) specialized government personnel or a third party must segregate and redact the data and must not disclose any information other than that targeted by the warrant; 3) the warrant must disclose the actual risk of destruction or concealment of information, and any prior efforts to seize the information; 4) the government's search protocol must be included and designed only to uncover the information for which it has probable cause; and 5) the government must destroy or return non-responsive data and keep the court informed of its progress. (R. at 17.)

Thus, regardless of the care taken during the search, a computer forensics team may only disclose those captions of information from any single document that directly pertain to the information requested by the warrant. (R. at 13–14.) Although the Supreme Court does not require this method in any other type of search, the Fourteenth Circuit Court of Appeals found the additional burden necessary in light of "technological complexity." (R. at 14.) The court of

appeals retroactively applied these new requirements to the StarTests warrant and found that the additional drug test information was unlawfully seized. (R. at 17.) The court then held that it had the equitable jurisdiction to enforce the Rule 41(g) motion and ordered the return of all additional data to the StarTests facility. (R. at 15–17.)

SUMMARY OF THE ARGUMENT

This case involves the touchstone of the Fourth Amendment—reasonableness—in the context of the search and seizure of digital evidence. With the opportunity to revisit standing principles, the requirements and limitations on a Fourth Amendment search and seizure, and to review a court’s equitable jurisdiction to return unlawfully seized property, this Court should correct the significant legal errors made by the Fourteenth Circuit Court of Appeals.

I.

The lower courts erred by finding that the CFL has standing to sue. The CFL, as an organization, may directly assert Rule 41(g) standing because of injury to itself, or, in certain situations, vicariously because of injury to its members.

First, the CFL did not have direct standing. Federal Rule of Criminal Procedure 41(g) allows for the return of unlawfully seized property if the movant is the person aggrieved by the unlawful search. Fourth Amendment protection against unlawful search and seizure depends on a legitimate expectation of privacy in the invaded place. The CFL, however, neither controls the access to StarTests’ facilities nor controls the storage of and access to the drug test databases stored there. The CFL was not the victim of the FBI’s search; thus, it lacks the direct standing to complain about the search.

Second, the CFL cannot assert standing to sue on behalf of its players. The players’ privacy interests are not germane to the CFL’s organizational purpose. No evidence on the

record indicates that the CFL serves the players' interests as part of its mission; rather, the CFL had to negotiate with each of its member franchises, which represented the players' interests in this matter. Moreover, the players do not have a legitimate expectation of privacy in their illegal drug test results because they voluntarily gave urine samples to a private party. Nor may the CFL assert standing on behalf of the players, because assessing each player's expectation of privacy requires their individual participation in the lawsuit. Therefore, the CFL lacks associational standing to sue on behalf of the players.

II.

The Fourteenth Circuit Court of Appeals erred by adopting and retroactively applying additional warrant particularity requirements, by refusing to apply the plain view doctrine to the facts of this case, and by ordering the FBI to return or destroy the additional drug test information found in StarTests' database. The Fourth Amendment specifies exactly two things that a warrant shall contain: 1) a particular description of the place to be searched; and 2) a particular description of the place to be seized. The FBI agents in this case presented probable cause evidence to a neutral and detached magistrate judge. That judge, in turn, issued a warrant specifying that the agents may, subject to certain limitations, search and seize computer storage data reasonably related to the investigation of illegal steroid use by the five named players in the warrant.

The district court found that the FBI computer forensics agents complied with the terms of the warrant before seizing the computer storage devices from StarTests' facilities for further analysis. Moreover, the FBI agents narrowly tailored the search by using the particular descriptions given in the warrant and by searching for only the files that StarTests' employees told the agents had the drug test information. The additional drug test information came into

plain view during the examination of those specific databases. Thus, applying the plain view doctrine to the search of digital evidence presents no particular problem in this set of facts. This Court should reinstate the district court's findings that the StarTests warrant meets Fourth Amendment particularity requirements and that the agents seized the additional drug test information in plain view during the scope of a lawful search.

Further, the court of appeals erred by requiring the government to return or destroy its copies of the additional drug test information. The court's order ignores the express language of the Advisory Committee to the Federal Rules of Criminal Procedure and similar findings by the other courts of appeals—specifically, that the government may retain copies of illegally seized evidence for use in ongoing investigations. Nor did the court of appeals correctly apply the factors that it adopted to determine the reasonableness of exercising Rule 41(g) equitable jurisdiction. Additionally, the court disregarded several key findings of fact when it found that the government acted in callous disregard and that StarTests suffered irreparable harm. This Court should reverse the Fourteenth Circuit Court of Appeals and allow the FBI to retain copies of the additional drug test information for use in its ongoing investigation.

III.

The Fourth Amendment does not contemplate heightened particularity requirements. Moreover, this Court has rejected previous attempts to heighten the Fourth Amendment's listed requirements because they come at a substantial cost and are unnecessary given the Fourth Amendment safeguards already in place. This Court, in *Grubbs*, held that the Fourth Amendment does not require a warrant to specify the exact method of search, now required by the Fourteenth Circuit Court of Appeals. Requiring a warrant to specify the search protocol of digital evidence in advance is impractical given the ability to hide and conceal data. Such a

requirement also strains the time and technical knowledge of magistrate and district judges. For similar reasons, this Court, in *Zurcher*, held that there is no need for warrants to disclose the risk of destruction or concealment by the party holding the evidence—a requirement imposed by the court of appeals in this case.

Lastly, requiring government agents to forswear use of the plain view doctrine during the search of digital evidence amounts to an indiscriminate suppression of evidence. Such indiscriminate suppression comes at a substantial social cost repeatedly eschewed by this Court. Moreover, the exclusionary rule, by discouraging the government from overstepping the terms of a search warrant, provides sufficient protection for those rare cases where a zealous officer disregards an individual’s rights. Therefore, this Court should hold that the Fourth Amendment does not require heightened warrant particularity requirements, and, further, that they are unnecessary in the context of digital evidence.

ARGUMENT AND AUTHORITIES

StarTests and the CFL move for the return of unlawfully seized property under Rule 41(g). In reviewing a Rule 41(g) motion for return of property, the factual findings of the district court are reviewed for clear error. *United States v. Marolf*, 173 F.3d 1213, 1216 (9th Cir. 1999); *see also United States v. Eylicio-Montoya*, 18 F.3d 845, 848 (10th Cir. 1994) (stating that factual findings in similar Rule 41 motions to suppress are reviewed for clear error). However, a reviewing court reviews the exercise of equitable jurisdiction under Rule 41(g) for an abuse of discretion. *Ramsden v. United States*, 2 F.3d 322, 324 (9th Cir. 1993). A court abuses its discretion when it commits a “clear error of judgment in the conclusion it reached upon a weighing of the relevant factors.” *SEC v. Coldicutt*, 258 F.3d 939, 941 (9th Cir. 2001). Moreover, a lower court’s interpretation of Rule 41(g) is reviewed de novo. *Id.* Lastly, the

lawfulness of a search and seizure under the Fourth Amendment “is a conclusion of law that [is also] review[ed] de novo.” *Eylicio-Montoya*, 18 F.3d at 848.

I. THE CFL DOES NOT HAVE DIRECT OR ASSOCIATIONAL STANDING TO SUE UNDER RULE 41(g) FOR THE RETURN OF STARTESTS’ DATABASES.

The Fourth Amendment stands as a protective barrier from “unreasonable searches and seizures.” U.S. Const. amend. IV. To help ensure these rights, the Federal Government implemented Rule 41 of the Federal Rules of Criminal Procedure, which among other things, allows for the return of unlawfully seized property. *See* Fed. R. Crim. P. 41(g). Rule 41(g), however, requires that the movant be “a person aggrieved by an unlawful search and seizure.” *Rakas v. Illinois*, 439 U.S. 128, 134–35 (1978). Thus, in the case of a Rule 41(g) motion, “many of the traditional standing inquiries² . . . [are] more properly placed within the purview of substantive Fourth Amendment law.” *Id.* at 140.

The rights guaranteed under the Fourth Amendment are “personal rights which, like some other constitutional rights may not be vicariously asserted.” *Rakas*, 439 U.S. at 133 (quoting *Alderman v. United States*, 394 U.S. 165, 174 (1969)). Here, the Colonial Football League moved under Rule 41(g) for the return of StarTests, Inc.’s electronic databases. *See* (R. at 2–3). This Court should find that the Fourteenth Circuit Court of Appeals erred as a matter of law when it found that the CFL was “one against whom the search was directed,” because the CFL does not have access to StarTests’ facilities. *See* (R. at 10). Moreover, the District Court for the District of Wythe erred by holding that the CFL has associational standing to sue for the return of property on behalf of the CFL players. (R. at 3.) The CFL players do not have standing to sue

² Article III standing requires that the proponent have an “alleged an injury in fact,” and that “the proponent is asserting his own legal rights and interests.” *Rakas*, 439 U.S. at 139 (citing *Singleton v. Wulff*, 428 U.S. 106, 112 (1976)).

for the return of StarTests' property, the players' privacy interests are not germane to the CFL's organizational purpose, and the claim asserted requires the players' individual participation. *See Hunt v. Wash. Apple Adver. Comm'n*, 432 U.S. 333, 343 (1977)). Thus, this Court should overrule the courts below and hold that the CFL does not have standing to sue under Rule 41(g) for the return of StarTests' property.³

A. Even if the CFL Has Property Interest in StarTests' Databases, the CFL Was Not One Against Whom the FBI's Search Was Directed.

“In order to qualify as a ‘person aggrieved by an unlawful search and seizure’ one must have been a victim of a search or seizure, *one against whom the search was directed*, as distinguished from one who claims prejudice only through the use of evidence gathered as a consequence of a search or seizure directed at someone else.” *Rakas*, 439 U.S. at 134–35 (quoting *Jones v. United States*, 362 U.S. 257, 261 (1960)). However, “[t]he protection of the Fourth Amendment depends not upon a property right in the invaded place[,] but upon whether the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded place.” *Rakas*, 439 U.S. at 143 (quoting *Katz v. United States*, 389 U.S. 347, 353 (1967)).

The Fourteenth Circuit Court of Appeals maintains that the CFL was “one against whom the search was directed” because “the government searched the StarTests facility to acquire the [CFL's property].” *See* (R. at 10). This theory, however, amounts to the “target” theory that this Court rejected in *Rakas*. *See* 439 U.S. at 132–33. The problem with the target theory is that would allow defendants to exclude evidence “without having to inquire into the substantive

³ In its review of the government's motion for lack of standing, this Court should “accept as true all material allegations” which the complaining party asserts on the record. *See Warth v. Seldin*, 422 U.S. 490, 501 (1975).

question of whether the challenged search or seizure violated the Fourth Amendment rights of *that particular defendant.*” *Id.* at 138 (emphasis added). Thus, the CFL’s alleged property interest in the seized databases does not give it standing to sue.

Lastly, the CFL does not have standing because it does not have a legitimate expectation of privacy in StarTests’ premises. *See id.* at 134 (stating that no Fourth Amendment violation occurs when a person is aggrieved by the illegal search and seizure of a third party’s premises). An individual has a legitimate expectation of privacy in a place when the individual “has exhibited an actual (subjective) expectation of privacy” and when “the individual’s subjective expectation of privacy is one that society is prepared to recognize as reasonable.” *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (citation omitted). An individual exhibits a subjective expectation of privacy when “he seeks to preserve [something] as private” and that subjective expectation is objectively reasonable when the individual’s expectation is “justifiable under the circumstances.” *Id.*

The CFL does not have a legitimate expectation of privacy in StarTests’ facilities or the databases stored there, because only StarTests “had complete dominion [and] control . . . [to] exclude others” from accessing them. *See* (R. at 10); *Rakas*, 439 U.S. at 149; *see also Jones*, 362 U.S. at 265 (holding that defendant a had legitimate expectation of privacy in friend’s apartment because he had the key to the apartment and could exclude others from it); *Katz*, 389 U.S. at 352 (holding that defendant who closed door to telephone booth and paid toll had expectation of privacy). Moreover, the CFL promised to the franchises that it would not have access to the information except those percentages that StarTests promised to release. (R. at 8.) Additionally, StarTests hid the information in such a way that even its own employees could not access all of it at once. (R. at 2 n.1.) Thus, the CFL did not have a legitimate expectation of privacy in the

databases because it had no control over who could access them. *See United States v. Padilla*, 508 U.S. 77, 82 (1993) (rejecting the idea that control over an area through a joint venture operation is sufficient to establish a legitimate expectation of privacy).

B. The CFL Does Not Have Associational Standing to Sue for the Return of StarTests' Databases.

An association may sue on behalf of its members when it meets the following criteria: 1) its members would otherwise have standing to sue in their own right; 2) the interests that the association seeks to protect are germane to the organization's purpose; and 3) neither the claim asserted or the relief requested requires the participation of individual members in the lawsuit. *Pennell v. City of San Jose*, 485 U.S. 1, 7 n.3 (1988) (citing *Hunt*, 432 U.S. at 343). Here, the players do not have standing to sue for the return of property because they voluntarily turned over their tests for illegal drugs to the hands of a private party. Moreover, the CFL represents the interests of the franchises, not the players. Lastly, the government's investigation only implicates specific players, whose presence is necessary to obtain relief.

1. The player's privacy interests are not germane to the CFL's organizational purpose.

The interests that an association seeks to protect must be "germane to the purpose of the organization." *Hunt*, 432 U.S. at 343. In *Pennell*, the Court found that a homeowners association had standing to protect its tenants from a rent control ordinance. *See* 485 U.S. at 4. Specifically, that association was "organized for the purpose of representing the interests of the owners and lessors of real property." *Id.* at 7 n.3.

Unlike *Pennell*, the record in the instant case lacks an organizational description of the CFL. Rather, the CFL is an organization of professional football league franchises, not individual players, evidenced by the fact that the CFL dealt directly with the franchises in this matter. (R.

at 1, 8.) Without more evidence on the record, this Court should reject the argument that the interests of the players are germane to the CFL's organizational purpose.

2. The players do not have a legitimate expectation of privacy in their illegal drug test results which they gave to a private party.

An individual has a Fourth Amendment cause of action when “the person invoking its protections can claim . . . a *legitimate expectation of privacy* that has been invaded by government action.” *Smith*, 422 U.S. at 740 (emphasis added). An individual has a legitimate expectation of privacy in an area when “the individual, by his conduct, exhibited an actual (subjective) expectation of privacy . . . [and when] the expectation is one that society is ready to recognize as reasonable.” *Id.* (citing *Katz*, 389 U.S. at 353).

“It is established that, when a person communicates information to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information . . . to law enforcement officials.” *SEC v. O'Brien*, 467 U.S. 735, 743 (1984) (citing *United States v. Miller*, 425 U.S. 435, 443 (1976)). Here, the players waived their subjective expectation of privacy in their drug test results by voluntarily submitting to the CFL's drug-testing program. As an “incentive” to participate in the program the players were told that their names were to be kept confidential. (R. at 1.) However, the players never took action against nor protested the testing program. *Cf. Bd. of Educ. v. Earls*, 536 U.S. 822, 826–27 (2002) (detailing very similar drug-testing program among high-school athletes, but athletes did not voluntarily submit to testing).

Although society recognizes a legitimate expectation of privacy in medical records, it does not recognize such an expectation for illegal drug test results given to a private party. *See California v. Greenwood*, 486 U.S. 35, 43 (1988) (stating that “Fourth Amendment analysis must turn on such factors as ‘our societal understanding that certain areas deserve more scrupulous

protection from government invasion” than others) (citations omitted). In *Board of Education v. Earls*, this Court upheld a mandatory drug-testing program where student athletes were forced to submit to drug-testing programs, but the results were kept separate from their student records and were not obtained for law enforcement purposes. *See* 536 U.S. at 832–33. The Court found that society is willing to accept the drug-testing program to force the students’ participation to help curb the “nationwide epidemic of drug use” among “our Nation’s youth.” *Id.* at 834. Unlike the students in *Board of Education*, the CFL players are adults who understand the consequences of illegal drugs, and the prosecution of professional athletes for illegal drug use furthers society’s goal of curbing illegal drug use by children. *Cf. Bd. of Educ.*, 536 U.S. at 832–33. Thus, this Court should find that the players’ expectation of privacy in their illegal drug test results held by a private party is not one that society is willing to recognize.

3. The claim asserted requires individual player participation in the lawsuit.

The ability of an association to sue on behalf of its members depends in substantial measure on the nature of the relief sought.” *Int’l Union v. Brock*, 477 U.S. 274, 287 (1986). If individual participation is required from the members, then the association cannot bring suit on their behalf. *Id.*; *see Warth v. Seldin*, 422 U.S. 490, 515–16 (1975). Rule 41(g) of the Federal Rules of Criminal Procedure governs the requested relief in the instant case. As discussed above, Rule 41(g) standing is a question of “whether the challenged search or seizure violated the Fourth Amendment rights of that particular defendant.” *Rakas*, 439 U.S. at 138; *see also* Fed. R. Crim. P. 41(g). Thus, the Court must decide the individual subjective expectations of privacy of each of the players implicated in this suit. *See Int’l Union*, 477 U.S. at 287 (stating that construction firm cannot seek damages on behalf of members because the injury suffered “is peculiar to the individual member . . . [and] would require individualized proof”). Similarly,

deciphering individual expectations of privacy prevents the CFL from suing on behalf of each individual player who seeks relief.

II. THE PLAIN VIEW DOCTRINE APPLIES TO A SEARCH OF DIGITAL EVIDENCE AUTHORIZED BY A WARRANT CONTAINING A DESCRIPTION OF THE PLACE TO BE SEARCHED AND THE SPECIFIC INFORMATION TO BE SEIZED.

The Fourth Amendment ensures “the right of the people to be secure in their . . . papers, and effects, against unreasonable searches and seizures” U.S. Const. amend. IV. Moreover, no “[w]arrants shall issue” to supersede that right except by “[o]ath or affirmation, and [by] particularly describing the place to be searched, and the things to be seized.” *Id.* The amendment protects privacy interests in property by prohibiting unreasonable searches and by requiring a description of the search location. *Horton v. California*, 496 U.S. 128, 143 (1990) (citing *Texas v. Brown*, 460 U.S. 730, 747 (1983)). Additionally, the Fourth Amendment protects an individual’s possessory interest in property by prohibiting unreasonable seizures and by requiring the warrant to “particularly describ[e] . . . the . . . things to be seized.” *Id.*

The general rule, therefore, is that a search or seizure is *per se* unreasonable within the meaning of the Fourth Amendment, unless it is accomplished by a sufficient showing of probable cause to a neutral magistrate, who issues a warrant with the aforementioned “particularity requirements.” *Id.* However, this Court recognizes “flexible, *common-sense* exceptions” to the warrant requirement “in a wide range of diverse situations.” *Brown*, 460 U.S. at 735–36 (emphasis added). Regarding the issues before this Court, “it is well established that under certain circumstances the police may seize evidence in plain view without a warrant.” *Coolidge v. New Hampshire*, 403 U.S. 443, 465 (1971).

The “touchstone of the Fourth Amendment is reasonableness.” *Ohio v. Robinette*, 519 U.S. 33, 39 (1996). However, the Fourteenth Circuit Court of Appeals held that the plain view

exception never applies to the search and seizure of digital evidence (R. at 14), and that warrants for the search and seizure of digital evidence require additional descriptions above those stated in the Fourth Amendment (R. at 17). This Court measures reasonableness by examining the totality of the circumstances. *Robinette*, 519 U.S. at 39. For that reason, this Court’s Fourth Amendment jurisprudence “eschew[s]” the creation of “bright-line rules,” and instead, “emphasizes the fact-specific nature of the reasonableness inquiry.” *Id.* Thus, this Court should overrule the Fourteenth Circuit Court of Appeals by holding that the plain view doctrine applies to digital evidence cases, and that the FBI agents found additional drug test information in plain view while performing a search narrowly tailored to the particular descriptions in a valid warrant.

A. The StarTests Warrant Issued to the FBI Complied with the Probable Cause and Particularity Requirements of the Fourth Amendment.

The Fourth Amendment’s particularity requirements, in conjunction with probable cause, make “general searches . . . impossible and prevent[] the seizure of one thing under a warrant describing another.” *Andresen v. Maryland*, 427 U.S. 463, 481 (1976) (citations omitted). Probable cause for a warrant exists when “there is a fair probability that contraband or evidence of a crime will be found in a particular place.” *United States v. Grubbs*, 547 U.S. 90, 95 (2006) (citation omitted). These requirements give “the individual whose property is searched or seized [assurance] of the lawful authority of the executing officer . . . and the limits of his power to search.” *Groh v. Ramirez*, 540 U.S. 551, 561 (2004) (citation omitted).

However, the Fourth Amendment does not state general particularity requirements that may increase or decrease depending on the factual circumstance; rather, it specifies exactly two matters that the warrant must particularly describe: the place to be searched and the things to be seized. *Grubbs*, 547 U.S. at 97. The Fourteenth Circuit Court of Appeals, however,

retroactively imposed additional particularity requirements on warrants for the search and seizure of digital evidence. *See* (R. at 14–15). The court imposed the additional requirements in an effort to curb what it viewed as an exponential growth in unlawful searches of digital evidence. *See* (R. at 13). However, the StarTests warrant fully complied with this Court’s Fourth Amendment jurisprudence, and the particular descriptions in the warrant allowed the computer forensics agents to perform a narrowly tailored search of the digital evidence. Therefore, this Court should hold that the StarTests warrant was facially valid and reject the additional particularity requirements imposed by the Fourteenth Circuit Court of Appeals.

1. The FBI had probable cause to believe that StarTests’ facilities contained test results confirming the five named players’ use of illegal steroids.

The probable cause standard is a “practical, nontechnical concept[]” which contemplates the totality of the circumstances when determining whether a reasonable person might suspect that contraband or evidence is located in a particular place. *Illinois v. Gates*, 462 U.S. 213, 230–31 (1983). The probable cause standard is significantly less than standards used in judicial proceedings, such as preponderance of the evidence. *Id.* at 235. Thus, “the task of the issuing magistrate is simply to . . . make a common-sense decision . . . that there is a fair probability that contraband or evidence of a crime will be found at a particular place.” *Id.* at 238.

The FBI had probable cause to believe that StarTests’ facilities stored test results for the use of illegal steroids by players named in the warrant application. During its investigation, the FBI collected transactional evidence, eyewitness reports, and taped conversations that substantiated its suspicion that these players procured and used illegal steroids. (R. at 7.) During the collection of this evidence, the FBI learned that the players participated in a drug-testing program involving StarTests, Inc. (R. at 8.) The FBI made the case to the magistrate judge that,

due to the confidentiality of the drug-testing program, StarTests likely stored the results electronically, which would allow it to hide or encrypt the files. (R. at 8.) Thus, the magistrate judge correctly found probable cause to authorize the search and seizure of the electronic storage devices.

2. The StarTests warrant particularly described the facility in Millersville, Wythe as the place of search and seizure.

The validity of the description of the place to be searched, and the items to be seized is determined “on the basis of the information that the officers disclosed, or had a duty to disclose, to the issuing Magistrate.” *Maryland v. Garrison*, 480 U.S. 79, 85 (1987). The StarTests warrant issued by the Magistrate judge described the agents authority to search and seize items from the StarTests facility in Millersville, Wythe. (R. at 8.) Nothing in the record indicates that StarTests has other facilities in Millersville. Therefore, the warrant sufficiently described the place to be searched. *See Garrison*, 480 U.S. at 85 (holding facially valid a warrant describing one apartment, even though there were two connected apartments at that address and on that floor).

3. The StarTests warrant specifically itemized the search and seizure of StarTests’ computer records and storage devices.

A warrant describing a specific list of general types of documents to be searched and/or seized may satisfy the particularity requirement for “items to be seized.” *Andresen*, 427 U.S. at 482 n.10. This Court dealt with a similar situation in *Andresen*. There, the defendant argued that a warrant particularly describing “books, records, documents, papers, [or] memoranda . . . showing or tending to show a fraudulent intent” constituted a general warrant because it knowingly allowed the search and seizure of some items that would not be relevant to the end investigation. *Id.* However, in a complex scheme, where “bits of evidence” need to be pieced

together, like a “jigsaw puzzle,” a valid warrant allows the seizure of various types of evidence in the suspect’s possession for which there is probable cause linking it to the alleged crime. *Id.*

Similar to the *Andresen* warrant specifying a broad list of items pertaining to a specific crime with respect to a specific lot, *see id.* at 480, the StarTests warrant authorized the agents to search and seize documents, samples, computers, and computer storage that reasonably may contain evidence of illegal steroid use by the five named players (R. at 2). Thus, the StarTests warrant sufficiently described the things to be seized, as required by the Fourth Amendment. *See Zurcher v. Stanford Daily*, 436 U.S. 547, 550 (1978) (validating a warrant which allowed the seizure of “negatives, film, and pictures . . . relevant to the identity of the perpetrators” of the assault on nine officers); *cf. Groh*, 540 U.S. at 558 (holding a warrant invalid that did not describe the items to be seized, and instead listed “single dwelling residence . . . blue in color”); *Berger v. New York*, 388 U.S. 41, 57–58 (1967) (invalidating statute that authorized eavesdropping warrants without describing any particular offense being committed, nor any particular description of the types of conversation to be seized).

4. The StarTests warrant particularly limited the search of the digital evidence to “information reasonably related to the investigation into the five named players’ illegal steroid use.”

The circuit courts of appeals have affirmed the validity of warrants particularly describing the seizure of digital storage devices, where the particularity requirements sufficiently narrow the scope of the search of those devices. *See United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999) (allowing the seizure of a computer and all available disks”); *see also United States v. Carey*, 172 F.3d 1268, 1270–73 (10th Cir. 1999) (approving validity of warrant to search and seize computers for “names, telephone numbers, ledger receipts, [etc.]”). As a starting point, “[t]he scope of a lawful warrant is defined by the object of the search and the places in which

there is probable cause to believe that they may be found.” *Garrison*, 480 U.S. at 85 (citation omitted).

a. A Fourth Amendment search of digital evidence occurs at the time an agent views a particular storage location on the storage device.

A Fourth Amendment search of digital evidence⁴ does not take place until either the forensic software displays,⁵ or an agent decides to view, a particular storage location.⁶ This Court hinted at that result in *United States v. Karo*. 468 U.S. 705, 712 (1984). There, the Court found that the placement of a hidden voice transmitter was not an invasion of the Fourth Amendment right to privacy, but that the receipt of those transmissions by law enforcement officials would be such a violation. *Id.* By analogy, a software’s access of digital evidence is not an invasion of an individual’s right to privacy, but an agent viewing the data would be. *See id.* Moreover, in *Kyllo v. United States*, this Court criticized the notion that the presence of technology in an area necessarily results in a search, unless an officer can discern information from it. 533 U.S. 27, 39 (2001). Similarly, an agent gathers no discernable information from a digital storage medium until the agent physically views it on a screen.

⁴ Digital storage devices can store thousands of times the information of a file cabinet. *See* LexisNexis Discovery Services, *How Many Pages in a Gigabyte*, http://www.lexisnexus.com/applieddiscovery/lawlibrary/whitePapers/ADI_FS_PagesInAGigabyte.pdf (last visited Jan. 8, 2010) (noting that there are about 65,000 Microsoft Word document pages or about 15,000 image files capable of being stored in one gigabyte).

⁵ *See United States v. Giberson*, 527 F.3d 882, 885 (9th Cir. 2008) (detailing some of the search options for which information will be output to the screen using the “ILOOK” forensics software; *see also United States v. Hill*, 322 F. Supp. 2d 1081, 1091 (C.D. Cal. 2004) (talking about the government’s use of the “EnCase” forensics software to locate child pornography on defendant’s computer).

⁶ *See* Orrin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 551–54 (2005) (stating that that the best answer for when a search occurs on a storage device is when the data is exposed to human observation).

b. A Fourth Amendment seizure of digital evidence occurs at the time an agent takes the storage device, and a plain view seizure of digital evidence occurs at the time an agent views data on the screen.

“A seizure deprives the individual of dominion over his or her person or property.” *United States v. Jacobsen*, 466 U.S. 109, 113 (1987). Similar to files and papers, a seizure of digital evidence first occurs when an agent takes or makes a copy of the physical medium storing the information. *Compare United States v. Tamura*, 694 F.2d 591, 595–96 (9th Cir. 1987) (specifying search and seizure procedure for boxes of intermingled documents that cannot be sorted on site), *with Carey*, 172 F.3d at 1270–73 (approving validity of warrant to seize search seized computers for “names, telephone numbers, ledger receipts . . .”).

However, a plain view seizure of digital evidence occurs upon a lawful search of the digital evidence. *See Carey*, 172 F.3d at 1273 (stating that “it is the contents of the files” which were seized during a search of digital evidence); *United States v. Giberson*, 527 F.3d 882, 885, 890 (9th Cir. 2008) (holding plain view seizure of child pornography occurred when images came into view during forensics software search for other evidence); *Comprehensive Drug Testing v. United States*, 579 F.3d 989, 1016 (9th Cir. 2009) (en banc) (Bea, J., dissenting) (stating that a “plain view” seizure of digital evidence only truly occurs if the search of the digital evidence is first narrowly tailored).

This rule for the plain view seizure of digital evidence comports with the courts’ handling of the search and seizure of physical files. For example, in *Andresen*, this Court implied that the information located in seized files does not immediately come into plain view, when it stated that “we observe to the extent that such papers *were not within the scope of the warrants or were otherwise improperly seized*, the State was correct in returning them voluntarily.” 427 U.S. at 482 n.10. Moreover, in a search of intermingled files, it is important that “responsible officials,

including judicial officials, must take care to assure [the search and seizure is] conducted in a manner that minimizes unwarranted intrusions.” *Id.* Thus, this Court implied that not all of the information in a search of intermingled files is in plain view and that the method of searching those documents must be narrowly tailored to the warrant. *Id.*; *see also Tamura*, 694 F.2d at 595 (stating that “all items in a set of files may be inspected during a search, provided that *sufficiently specific guidelines for identifying the documents* sought are provided in the search warrant and are followed by the officers conducting the work”) (emphasis added).

c. Based on the facts in this case, the warrant particularity requirements do not need to change to limit the scope of a lawful Fourth Amendment search of digital evidence.

The particularity requirements may reasonably narrow the scope of a search of digital evidence, given the ability to use forensics software to decide which parts of the digital media to view.⁷ In this manner, the forensics software, or whatever search method used, becomes the means of probable cause to determine which storage locations to search on the device. *See Arizona v. Hicks*, 480 U.S. 321, 326 (1987) (holding that probable cause is required for the seizure of evidence in plain view). Similar to the search of physical files, however, some information not described in the warrant may be seized, as was the case here. *See id.* at 482 n.10 (stating that in a search of files “it is certain that some innocuous documents will be examined, at least, cursorily, in order to determine whether they are . . . authorized to be seized . . . [but,]

⁷ *See* Aaron Stanley, *The Continuing Evolution of Consent and Authority in Digital Search and Seizure*, 19 Fordham Intell. Prop. Media & Ent. L.J. 179, 191–92 (2008) (detailing the many various options of the “EnCase” forensics software, including the ability to search every individual storage location on a digital media, bits on a hard drive, for specified keywords); *see also* Steve Lohr, *Microsoft Tackles the Child Pornography Problem*, N.Y. Times Bits Blogs, Dec. 16, 2009, <http://bits.blogs.nytimes.com/2009/12/16/microsoft-tackles-the-child-pornography-problem/> (describing Microsoft’s free new tool that allows forensics agents to match images on a hard drive against a database of known child pornography images, even if the images have been modified).

judicial officers should take care to assure . . . [the search is] conducted in a manner that minimizes unwarranted intrusions).

The StarTests warrant required computer forensics agents to limit their search of the digital evidence to “information reasonably related to the investigation into the five named players’ illegal steroid use.” *See* (R. at 8). StarTests’ employees informed the agents that they needed to find three separate files to determine the drug test information for the five players named in the warrant. (R. at 8.) The employees told FBI agents that one file contained names and identification numbers, one file contained names and personal information, and one file contained identification numbers and test results. (R. at 8.) The StarTests employees also told the agents that some of the files may be hidden or encrypted. (R. at 8.) Thus, the FBI agents had sufficient information to comply with the scope of the warrant. *See Andresen*, 427 U.S. at 481 (stating that the particularity requirement ensures that “nothing [to be taken] is left to the discretion of the executing officer”). Moreover, the district court found that the agents only searched the database files including the information on the five named players. (R. at 5.) Thus, the Fourteenth Circuit Court of Appeals erred when it held that the StarTests warrant was overbroad. *See* (R. at 15); *see also Comprehensive Drug Testing*, 579 F.3d at 1019 (Bea, J., dissenting) (speculating that the test for a lawful seizure of digital evidence should be whether the search was narrowly tailored to the particularity requirements of the warrant); *cf. Carey*, 172 F.3d at 1273 n.4, 1274 (holding that deliberate search for child pornography was outside the scope of a warrant for evidence of drug transactions, except for first picture inadvertently found).

B. The Government Agents' Seizure of the Additional Drug Test Results that Appeared in Plain View Was Within the Scope of the Agents' Lawful Search for the Results on the Five Players Listed in the Warrant.

The plain view doctrine allows government agents to seize incriminating evidence that they come upon during an otherwise lawful search. *Brown*, 460 U.S. at 739. A search compromises an individual's interest in privacy; whereas, a seizure deprives an individual of dominion over his or her property. *Horton*, 496 U.S. at 133. Therefore, the seizure of property in the plain view of an agent involves no further invasion of privacy because the owner's remaining interest is merely that of possession and ownership. *Id.*

The central question in most plain view cases is whether the government agent had a prior justification for the intrusion. *Coolidge*, 403 U.S. at 466. Thus, the plain view doctrine is not the exception to the general rule that warrantless searches are presumptively unreasonable. *Horton*, 496 U.S. at 133. Three requirements guarantee that the seizure of property in plain view was not the product of an unreasonable search: 1) the agent was lawfully located in the place that the object was in plain view; 2) the agent had a lawful right of access to the object itself; and 3) the incriminating character of the object was immediately apparent. *Id.* at 137.

The FBI forensics agents searching StarTests' computer storage devices viewed additional drug test information while conducting a narrowly tailored search of databases which they had probable cause to believe contained the information on the five named players. *See* (R. at 5). Thus, the Fourteenth Circuit Courts of Appeals erred in concluding that the plain view doctrine does not act "as a procedural safeguard in the digital evidence context." *See* (R. at 12).

1. The FBI computer forensic agents lawfully entered StarTests facilities with the right to search, seize, or make copies of computer storage devices.

An agent has lawful presence in a location when the agent makes a lawful initial entry by which he or she can view a particular area. *Brown*, 460 U.S. at 737. For instance, the police officer in *Horton* had a warrant to enter the defendant's house to look for rings taken during a robbery, when he found other evidence linked to the robbery in plain view. *See Horton*, 496 U.S. at 130–31. Similarly, the officer in *Coolidge* entered the defendant's property pursuant to a warrant for arrest, when he also seized the car sitting in the driveway. *See Coolidge*, 403 U.S. at 447–48.

Similar to the officers in *Horton* and *Coolidge*, the FBI agents were lawfully present when they seized or made copies of the computer storage information, because they followed the specific terms of the magistrate's warrant. The magistrate's warrant required specially trained law enforcement personnel to assess the practicality of searching the storage devices on-site versus seizing the equipment where necessary. (R. at 2.) The computer forensics agents learned that StarTests stored the authorized information across several different computers and in encrypted or hidden files. (R. at 2.) Because StarTests' employees did not know how to find the information, the forensics agents seized or copied all of the computer data and took it back to their facilities in Wythe City. (R. at 2); *see also United States v. Hay*, 231 F.3d 630, 637 (9th Cir. 2000) (affirming the seizure of an entire computer system when the agents "had no way of knowing where the images were stored" and the agents had "the magistrate judge's authorization to do so").

2. The computer forensics agents lawfully accessed the database files containing the drug test results for the five named players.

“[T]he scope of a lawful search is “defined by the object of the search and the place in which there is probable cause to believe that it may be found.” *Garrison*, 480 U.S. at 84 (stating that “probable cause to believe that undocumented aliens are being transported in a van will not justify a warrantless search of a suitcase” (quoting *United States v. Ross*, 456 U.S. 794, 824 (1982))). Thus, a lawful search of digital evidence must be narrowly tailored to the storage locations for which there are probable causes to view. *See Carey*, 172 F.3d at 1273 (suppressing evidence found on digital storage device when officer exceeded scope of search for drug evidence to find child pornography). As explained previously, this Court implied that result in *Andresen*. *See* 427 U.S. at 482 n.10 (stating that in a search of intermingled files, “responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions”).

The FBI forensics agents in this case complied with the warrant’s restrictions to access only the files “reasonably related to the investigation into the five named players’ illegal steroid use.” (R. at 8.) Moreover, the FBI complied with the warrant restriction that computer forensics agents conduct the search of the computer storage devices. (R. at 5.) The computer forensics agents only viewed the three database files containing the information described in the warrant.⁸ (R. at 5.) Nothing in the record indicates that the agents visually inspected any other files. Thus, the forensic agents’ lawfully accessed StarTests’ databases containing the additional dug test

⁸ The information for the five players was stored in three different file databases: one containing the players’ personal and health information, one containing the player’s names and assigned identification number, and the last containing the actual tests results matched only with the identification numbers. (R. at 2.)

information. (R. at 5); *see also Giberson*, 527 F.3d at 885 (finding lawful access when search was narrowly tailored to find fake I.D. evidence).

The Fourteenth Circuit Court of Appeals emphasized that “gaining access to the desktop is the same as having access to all the files in the My Computer file folder,” and that new precautions are needed to safeguard the Fourth Amendment in digital evidence searches. (R. at 11); *see also United States v. Alexander*, 574 F.3d 484, 490–91 (8th Cir. 1987) (holding that lawful access to the area in which a computer was located was lawful access to the computer itself). *But see United States v. Turner*, 169 F.3d 84, 88–89 (1st Cir. 1999) (holding that scope of consent to search apartment for evidence of assault did not include search of files on computer located in apartment). It is paramount to note that the reasoning of the Fourteenth Circuit Court of Appeals fails to take into account existing software, which can access all of the information on a storage device and choose which information an agent will view.⁹ These search solutions will continue to develop,¹⁰ because the courts force agents to justify that plain view results are the product of a narrowly tailored search. *See Herring v. United States*, 129 S. Ct. 695, 699 (2009) (stating that the exclusionary rule applies where “it results in appreciable [future] deterrence”) (citations omitted); *see also Comprehensive Drug Testing*, 579 F.3d at 1020 (Bea, J., dissenting) (stating that it is more reasonable for magistrate to have discretionary power to expand warrant

⁹ *See, e.g., Giberson*, 527 F.3d at 885 (detailing some of the search options and options for which information will be output to the screen using the “ILOOK” forensics software; *see also Hill*, 322 F. Supp. 2d at 1091 (discussing the government’s use of the “EnCase” forensics software to locate child pornography on defendant’s computer); Stanley, *supra*, at 191–92.

¹⁰ *See, e.g., Lohr, supra* (describing Microsoft’s free new tool that allows forensics agents to match images on a hard drive against a database of known child pornography images, even if the images have been modified).

once agent convinces additional incriminating evidence was the power of a narrowly tailored search).

3. The files containing the illegal steroid tests for the five named players also contained drug test results for other players and drug test results for cocaine, marijuana and hallucinogens.

Evidence that comes into plain view during an otherwise lawful search is admissible if its incriminating nature is immediately apparent. *Horton*, 496 U.S. at 142. An agent must make a showing of “probable cause to associate the property with criminal activity” to satisfy the “immediately apparent” requirement. *Brown*, 460 U.S. at 741 (quoting *Payton v. New York*, 445 U.S. 573, 587 (1980)) (holding that a deflated and uniquely tied party balloon falling from driver’s hand was probable cause to suspect drug activity). The lower courts of appeals have held that the immediately apparent requirement is no different for digital evidence than for physical objects—the contents of a specific storage location viewed on a screen either are or are not probable cause of criminal activity. *See Carey*, 172 F.3d at 1273 (holding that once the agent viewed the child pornography in the first picture format file, he had probable cause to believe the remaining picture format files contained similar materials).

Because StarTests structured the test results database in a grid fashion, all of the test results for any identification number were immediately apparent when looking at that grid row. (R. at 5.) The district court found that the test results information for anabolic steroids, cocaine (R. at 5), marijuana, and other hallucinogens were “alongside” one another. (R. at 2); *cf. Hicks*, 480 U.S. at 324–25 (holding that the criminal nature of equipment was not immediately apparent when officer had to move the equipment to get the serial numbers). Moreover, the district court found that the test results of other players not specified in the warrant came into plain view during the process of matching the identification numbers in the grid row to the player’s

information in the other file.¹¹ (R. at 5.) Thus, the additional drug test information came into plain view during a narrowly tailored search of the computer storage devices.

C. The Fourteenth Circuit Court of Appeals Erred when It Forced the Government to Return or Destroy the Database Information, Including the Copies.

Even if this Court finds the seizure of the additional drug test information unlawful, the Fourteenth Circuit Court of Appeals erred when it held that the government must also return or destroy the copies of the additional test results. *See* (R. at 16). Moreover, the court abused its discretion by ignoring some of the findings of fact of the district court. Lastly, the court erred as a matter of law in applying some of the factors, which it adopted from another circuit court of appeals, to determine the reasonableness of Rule 41(g) equitable jurisdiction. *See* (R. at 16).

1. Even if this Court finds the Rule 41(g) motion reasonable, the Fourteenth Circuit Court of Appeals erred by forcing the government to destroy the copies of StarTests' database files containing the additional drug test information.

The advisory committee notes to the 1989 amendments of Rule 41¹² clearly state that the government may retain the ability to use unlawfully seized evidence for law “enforcement purpose[s].” *See* Fed. R. Crim. P. 41 advisory committee’s notes to 1989 amendment. “[Rule 41(g)] is not intended to deny the United States the use of evidence permitted by the [F]ourth

¹¹ The information for the five players was stored in three different file databases: one containing the players’ personal and health information, one containing the player’s names and assigned identification number, and the last containing the actual tests results matched only with the identification numbers. (R. at 2.)

¹² Prior to the 1989 amendments, a motion to suppress and a motion to return property were both Rule 41(e) motions. Those two motions were separated, and a motion to return property remained a Rule 41(e) motion until 2002. *See* Fed. R. Crim. P. 41 advisory committee’s notes to the 1989 amendments.

[A]mendment . . . even if the evidence might have been unlawfully seized.”¹³ *Id.* Moreover, “[a]s amended, Rule [41(g)] avoids an all or nothing approach whereby the government must . . . return records and make no copies” *Id.*

There is one exception to the general rule that the government may retain copies of seized property, but that exception does not apply to these facts. *See id.* (stating that “[i]n some circumstances . . . equitable considerations might justify an order requiring the government . . . to destroy all copies of records that it has seized (citing *Paton v. LaPrade*, 524 F.2d 862, 867–69 (3d Cir. 1975)). In *Paton*, the FBI flagged a student for sending a letter to the Socialist Work Party, but did not destroy her file once it learned that the student sent the letter to request information pursuant to a class assignment. 524 F.2d at 865. The student filed suit to expunge the file, but the Third Circuit Court of Appeals overruled the motion. *Id.* at 869. *Paton*, however, “did not concern an ongoing criminal investigation, but instead a closed one. The balance of equities in such a situation would more likely favor complete destruction . . . [of the evidence].” *United States v. Search of Law Office, Residence & Storage Unit Alan Brown*, 341 F.3d 404, 413 (5th Cir. 2003). Unlike the closed investigation in *Paton*, the FBI in this case was just beginning its investigation into the use of illegal steroids in the CFL (R. at 1), and decided to expand the investigation after learning of the use of additional types of illegal drugs by the players (R. at 6).

¹³ In December 2002 Rule 41(e) was relettered as Rule 41(g). The only difference between the old Rule 41(e) and the new Rule 41(g) is that 41(e) contained as the last sentence in the provision: “If a motion for return of property is made or comes on for hearing in the district of trial after an indictment or information is filed, it shall be treated also as a motion to suppress under Rule 12.” The new Rule 41(g) does not contain such a statement, but Rule 41(h) now provides, “A defendant may move to suppress evidence in the court where the trial will occur, as Rule 12 provides.” *United States v. Search of Law Office, Residence & Storage Unit Alan Brown*, 341 F.3d 404, 408 (5th Cir. 2003); *see also* Fed. R. Crim. P. 41.

Many of the lower courts of appeals agree that a successful Rule 41(g) motion does not foreclose the government's use of illegally seized property. In *J.B. Manning Corp. v. United States*, the Ninth Circuit Court of Appeals ordered the government to return all of the unlawfully seized original documents, but allowed it to “cop[y] . . . [the] documents necessary for investigation or prosecution.” 86 F.3d 926, 928 (9th Cir. 1996). Similarly, the Fifth Circuit Court of Appeals held that “[Rule 41(g)] does not permit a district court to order complete suppression of seized evidence absent, at the very least, a substantial showing of irreparable harm.” *Search of Law Office*, 341 F.3d at 413–14.

2. The Fourteenth Circuit Court of Appeals erred when it found that its exercise of Rule 41(g) was reasonable.

Several of the circuit courts of appeal agree¹⁴ on the following factors to determine the reasonableness of a court's Rule 41(g) equitable jurisdiction before criminal charges have been filed:

- 1) whether the government displayed a callous disregard for the constitutional rights of the movant; 2) whether the movant has an individual interest in and need for the property he wants returned; 3) whether the movant would be irreparably injured by denying return of the property; and 4) whether the movant has an adequate remedy at law for the redress of his grievance.

Ramsden v. United States, 2 F.3d 322, 324–25 (9th Cir. 1993) (quoting *Richey v. Smith*, 515 F.2d 1239, 1243–44 (5th Cir. 1975)). Moreover, the circuit courts of appeals agree that the exercise

¹⁴ See *Richey v. Smith*, 515 F.2d 1239, 1243–44 (5th Cir. 1975) (establishing four factors to determine the reasonableness of a pre-indictment Rule 41(g) motion; *Ramsden v. United States*, 2 F.3d 322, 325 (9th Cir. 1993) (adopting the four factors from *Richey* to determine the same); *Pieper v. United States*, 604 F.2d 1131 (8th Cir. 1979) (adopting factors from *Richey*); *In re Search of Kitty's E.*, 905 F.2d 1367, 1371 (10th Cir. 1990) (using two of the same factors from *Richey* to determine Rule 41(g) reasonableness).

of jurisdiction under Rule 41 should be exercised with great restraint and caution.¹⁵ With three of the four factors weighing against the reasonableness of a Rule 41(g) motion, the Fourteenth Circuit Court of appeals erred in forcing the government to return or destroy property pursuant to Rule 41(g).

a. By ignoring the findings of fact in the record, the Fourteenth Circuit Court of Appeals abused its discretion in its application of the first, third, and fourth factors.

The Fourteenth Circuit Court of Appeals found that the first factor weighed in favor of reasonableness because the government “essentially shut [StarTests’] facility down by seizing its equipment.” (R. at 16.) However, even that court found evidence on the record that “the computer system configuration at StarTests’ facilities was far more complex than . . . anticipated” (R. at 8) and that even most of StarTests’ employees could not access all of the necessary databases (R. at 2). Moreover, the court ignored the district court’s findings of fact that the warrant authorized the government to seize the equipment if necessary, and that the FBI agents complied with the terms of the warrant in making that decision. (R. at 5.) The court also gave no deference to the district court’s finding of fact that the agents narrowly tailored their search of the files. (R. at 5.)

The Fourteenth Circuit Court of Appeals also abused its discretion when it ignored the district courts finding of fact that the FBI had already returned the hard drives. *See* (R. at 2) (“After thoroughly copying and inventorying the computer hard drives, the FBI returned the unneeded equipment.”). Instead, the court incorrectly found that StarTests’ suffered irreparable harm because it “cannot operate without its computer equipment.” (R. at 16.)

¹⁵ *See Ramsden*, 2 F.3d at 324; *In re Search of Kitty’s E.*, 905 F.2d at 1370; *Pieper*, 604 F.2d at 1133.

Lastly, the court found that StarTests and the CFL do not still have an adequate remedy at law; however, those parties may challenge the seizure of the additional drug test information in any future criminal proceedings. *Cf. Ramsden*, 2 F.3d at 326 (holding that defendant did not have adequate remedy at law to challenge seizure that occurred under United States law in a United Kingdom courtroom). Even the Fourteenth Circuit Court of Appeals noted that there may be future suppression hearings on the additional drug test information. (R. at 16 n.5.)

b. The Fourteenth Circuit Court of Appeals also erred as a matter of law in its application of the third factor.

The Fourteenth Circuit Court of Appeals erred, as a matter of law, when it found that the potential breach of the CFL’s confidentiality agreement with the players and that the potential harm to StarTests’ business reputation constitute irreparable harm. (R. at 16.) The court adopted the factors used by the Fifth and Ninth Circuit Courts of Appeals. (R. at 16.) Those two circuit courts have held that “the mere threat of prosecution does not constitute irreparable harm,” because “every potential defendant” could invoke this power and the court’s “exercise of its equitable jurisdiction would . . . be quite ordinary.” *Search of Law Office*, 341 F.3d at 415 (quoting *Ramsden*, 2 F.3d at 326). Moreover, in *Search of Law Office*, the Fifth Circuit Court of Appeals held that reputational damage, resulting from the potential threat of litigation, was irrelevant to a finding of irreparable injury to the reasonableness of a Rule 41(g) motion. *See id.* Overruling its precedent to the contrary,¹⁶ the Fifth Circuit Court of Appeals found the advisory committee’s emphasis on the “movant’s *possessory interest* in the property . . .” persuasive. *Id.* at 415 n.53 (quoting advisory committee notes to the 1989 amendments) (emphasis added). *But*

¹⁶ In doing so, the Fifth Circuit also joined the Eighth, Ninth, and Tenth Circuit Courts of Appeals in holding that the threat of future prosecution constitutes irreparable harm. *See Ramsden*, 2 F.3d at 326; *In re Search of Kitty’s E.*, 905 F.2d at 1371; *Kiesel Co. v. Householder*, 879 F.2d 385, 387 (8th Cir. 1989).

see Richey, 515 F.2d at 1243 n.10 (stating that a ““wrongful indictment . . . works a grievous, irreparable injury””) (citations omitted).

III. THE HEIGHTENED PARTICULARITY REQUIREMENTS IMPOSED BY THE FOURTEENTH CIRCUIT COURT OF APPEALS CONTRADICT THIS COURT’S PRECEDENT AND ARE UNNECESSARY GIVEN THE FOURTH AMENDMENT SAFEGUARDS ALREADY IN PLACE.

The Fourteenth Circuit Court of Appeals erred as a matter of law by adopting heightened requirements for judges to observe before issuing a warrant to search and seize digital evidence.¹⁷ (R. at 17.) The new warrant requirements include that:

- 1) the government must waive reliance on the plain view doctrine; 2) specialized government personnel or a third party must segregate and redact the data and must not disclose any information other than that targeted by the warrant; 3) the warrant must disclose the actual risk of destruction or concealment of information, and any prior efforts to seize the information; 4) the government’s search protocol must be included and designed only to uncover the information for which it has probable cause; and 5) the government must destroy or return non-responsive data and keep the court informed of its progress.

(R. at 17); *see also Comprehensive Drug Testing v. United States*, 579 F.3d 989, 1000–01 (9th Cir. 2009) (en banc). The court adopted these additional requirements to prevent, what it deemed, unlawful searches by the government. (R. at 16); *see also Comprehensive Drug Testing*, 579 F.3d at 1001.

A. This Court Has Rejected Heightening the Particularity Requirements Above Those Stated in the Fourth Amendment.

The requirement that a warrant designate the search protocol in advance is no different from a similar requirement that this Court rejected in *United States v. Grubbs*. *See* 547 U.S. at 97. There, a magistrate judge granted a warrant on the condition that the package containing

¹⁷ Note that neither the Fourteenth Circuit Court of Appeals opinion in this case nor the Ninth Circuit Court of Appeals opinion in *Comprehensive Drug Testing* define the scope of what is a digital evidence case. *See generally* (R. at 7–17); *Comprehensive Drug Testing v. United States*, 579 F.3d 989 (9th Cir. 2009).

child pornography, which the defendant purchased from an undercover postal inspector, was actually delivered. *Id.* at 93. The Ninth Circuit Court of Appeals held that the warrant was invalid, even though it satisfied the Fourth Amendment’s particularity requirements, because it did not specify the triggering condition. *Id.* at 93. This Court rejected the triggering condition requirement, and it affirmed the literal meaning of the Fourth Amendment’s particularity requirements. *See id.* at 99 (holding that “[b]ecause the Fourth Amendment does not require that the triggering condition . . . be set forth in the warrant . . . the Court of Appeals erred in invalidating [the warrant]”).

Similarly, requiring a warrant to disclose the risk of destruction or concealment of the evidence before seizure replicates the additional warrant requirements this Court rejected in *Zurcher v. Stanford Daily*. *See* 436 U.S. 547, 559–60 (1978). There, a district court attempted to impose heightened warrant particularity requirements to justify a search for evidence on the premises of a newspaper, which was not implicated in the crime. *Id.* Local police officers obtained a warrant and searched the premises of the newspaper for “negatives, film, and pictures showing the events and occurrences” of clashes between riot police and students. *Id.* at 551. The district court held that prior to obtaining a warrant to search a third parties’ premises the government must demonstrate that the third party would be willing to disobey a court order to preserve the evidence. *Id.* at 554. The district court, however, erred because “[t]he seemingly blameless third party . . . may not be innocent at all; and if he is, he may nevertheless be so related or so sympathetic with the culpable that he cannot be relied upon to retain and preserve [any incriminating evidence].”¹⁸ *Id.* at 561.

¹⁸ StarTests is a non-implicated third party similar to the Stanford Daily News reporters in *Zurcher*. (R. at 1.) Moreover, the degree to which StarTests hid and encrypted the data indicates a potential willingness to destroy the information. (R. at 2.) However, StarTests’ willingness to

The Fourteenth Circuit Court of Appeals maintains that these additional warrant requirements are necessary to protect privacy interests by preventing the government from “seiz[ing] the haystack to find the needle.” (R. at 13.) Contrary to the court’s goal, “the absence of a constitutional requirement that the warrant be exhibited at the outset of the search . . . is . . . evidence that the requirement of particular description does not protect an interest monitoring searches.” *Grubbs*, 547 U.S. at 97. Moreover, “[n]othing in the language of the Constitution or in this Court’s decisions interpreting that language suggests that, in addition to the [requirements set forth in the text], search warrants also must include a specification of the precise manner in which they are to be executed.” *Id.* at 98 (quoting *Stanford v. Texas*, 379 U.S. 476, 481 (1965)).

B. Forcing the Government to Specify Its Search Method in Advance Presents Immense Practical Difficulties.

“It would extend the Warrant Clause to the extreme to require . . . the court [to] set forth precisely the procedures to be followed by the executing officers.” *See Dalia v. United States*, 441 U.S. 238, 258 (1979). Thus, the Fourth Amendment does not require that a warrant detail the manner in which agents will carry out the search authorized by a warrant. *See id.* at 257–59 (rejecting warrant requirement that Magistrate place specific details in the warrant of the covert operation to place an electronic bug). The Fourth Amendment also does not require more description because “in executing a warrant, police may find it necessary to interfere with privacy rights not explicitly considered by the judge who issued the warrant.” *Id.* at 257. Moreover, police sometimes have to enter a suspect’s home in order to arrest him, or sometimes they damage property in the process of executing a warrant, both of which interfere with privacy or freedom of movement. *Id.* at 257–58.

comply is irrelevant to a warrant application, because this Court rejected very similar requirements in *Zurcher*. *See* 436 U.S. at 561.

In digital evidence cases, the courts “should not tie the hands of law enforcement by expecting an investigative officer to know the exact format electronically store evidence will take,” or be able to “discern a more precise way to describe items stored in electronic format.” *Ark. Chronicle v. Murphy*, 183 F. App’x 300, 306 (4th Cir. 2006). The practical problem with specifying a search protocol in advance is that the computer forensics agent, or a software search tool, first needs to analyze the method in which the data was stored. *See United States v. Hill*, 459 F.3d 966, 978 (9th Cir. 2006) (commenting that “[c]omputer records are extremely susceptible to tampering, hiding, or destruction, whether deliberate or inadvertent . . . [and that] [c]riminals 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”) (citations omitted). Additionally, “[e]ven the most computer literate of judges would struggle to know what protocol is appropriate in any individual case, and the notion that a busy trial judge is going to be able to invent one . . . [out of the blue] seems unrealistic” and will greatly hinder judicial efficiency. *United States v. Farlow*, No. CR-09-38-B-W, 2009 WL 4728690, at *6 n.3 (D. Me. Dec. 3, 2009).

C. Indiscriminate Suppression Remedies Are Not a Reasonable Means to Curb Potentially Unlawful Searches.

Suppression of evidence “has always been [this Court’s] last result, not [its] first impulse.” *Hudson v. Michigan*, 547 U.S. 586, 591 (2006). Moreover, this Court has “rejected ‘indiscriminate application’ of the [exclusionary] rule.” *Id.* at 591 (citations omitted). The exclusionary rule has a “costly-toll upon truth-seeking and law enforcement objectives” *Id.* (citation omitted). Thus, “the fact that a Fourth Amendment violation occurred . . . does not necessarily mean that the exclusionary rule applies.” *Herring v. United States*, 129 S. Ct. 695, 697 (2009) (quoting *Illinois v. Gates*, 462 U.S. 213, 223 (1983)).

The Fourteenth Circuit Court of Appeals now requires that the party searching the digital evidence suppress any information that is not the target of the warrant. (R. at 13); *see also United States v. Calandra*, 414 U.S. 338, 347 (1974) (stating that the purpose of the exclusionary rule is “to deter . . . by removing the incentive to disregard” constitutional guarantees). However, “the exclusionary rule has never been interpreted to proscribe the use of illegally seized evidence in all proceedings against all persons.” *Calandra*, 414 U.S. at 348. Moreover, this Court’s “cases have consistently recognized that unbending application of the exclusionary sanction to enforce the ideal of governmental rectitude would impede unacceptably the truth-finding function of judge and jury.” *United States v. Leon*, 468 U.S. 897, 907 (1984).

This new requirement indiscriminately suppresses evidence by requiring the personnel performing the search to withhold information outside the warrant, even if it is found during a lawful search. *See id.* at 907 (holding that exclusionary rule should not apply to evidence gathered by agents acting in “objective good faith” on the terms of a warrant which later was deemed invalid); *see also Herring*, 129 S. Ct. at 703 (holding that invalid warrant due to negligence was not sufficient basis to exclude incriminating evidence found in subsequent search incident to arrest). Moreover, the court gives no justification for the suppression of evidence that has never come before a neutral and detached court. (R. at 16); *see also Calandra*, 414 U.S. at 351–52 (refusing to extend the exclusionary rule to grand jury proceedings). Lastly, this requirement leaves the legal conclusion of which incriminating evidence falls within the scope of a warrant to a forensics agent or a third party. (R. at 17.)

The exclusionary rule still stands as an adequate safeguard in cases where the “police have been shown to be reckless in maintaining a warrant system, or have knowingly made false entries to lay the groundwork for future arrests.” *Herring*, 129 S. Ct. at 703. In this case, the Fourteenth

Circuit Court of Appeals imposed these *ex-ante* warrant restrictions to prevent the “government [from] seiz[ing] the haystack to look for the needle.” (R. at 13.) However, “the Constitution protects property owners by . . . interposing, *ex ante*, the deliberate, impartial judgment of a judicial officer . . . and by providing, *ex post*, a right to suppress evidence improperly obtained and a cause of action for damages.” *Grubbs*, 547 U.S. at 99. Thus, requiring the computer forensics agents to suppress any incriminating evidence they find in a search authorized by a warrant extends the Fourth Amendment protection beyond its intended meaning. *See id.*

CONCLUSION

This Court should REVERSE the holding of the United States Court of Appeals for the Fourteenth Circuit in all respects. Specifically, this Court should DISMISS the CFL for a lack of standing, and it should REINSTATE the decision of the United States District Court for the District of Wythe that the magistrate judge’s search warrant was legal within the context of the Fourth Amendment of the United States Constitution. Further, this Court should REINSTATE the district court’s decision to deny the Rule 41(g) motion because the additional drug test evidence was lawfully seized in plain view during a search that was narrowly tailored to the warrant.

Respectfully submitted,

ATTORNEYS FOR PETITIONER

APPENDIX TABLE OF CONTENTS

	<i>Page</i>
APPENDIX "A": CONSTITUTIONAL PROVISIONS.....	A-1
APPENDIX "B": FEDERAL RULES.....	B-1

APPENDIX “A”

CONSTITUTIONAL PROVISIONS

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 or things to be seized.

APPENDIX “B”

FEDERAL RULES

Fed. R. Crim. P. 41(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.