

---

---

No. 2009-H20

---

IN THE  
SUPREME COURT OF THE UNITED STATES  
FEBRUARY TERM, 2010

---

UNITED STATES OF AMERICA,

*Petitioner,*

v.

STARTESTS, INC. and the COLONIAL FOOTBALL LEAGUE,

*Respondent.*

---

*On Writ of Certiorari to the U.S. Circuit Court of  
Appeals for the Fourteenth Circuit*

---

BRIEF FOR PETITIONER

---

TEAM NO. 15  
*Attorneys for Respondent*

**TABLE OF CONTENTS**

**PAGE(S)**

TABLE OF AUTHORITIES ..... iii

QUESTIONS PRESENTED..... 1

CONSTITUTIONAL PROVISIONS INVOLVED.....1

STATEMENT OF THE CASE.....2

OPINIONS BELOW:

    I.    DISTRICT COURT PROCEEDINGS .....5

    II.   CIRCUIT COURT PROCEEDINGS .....6

SUMMARY OF THE ARGUMENT .....7

ARGUMENT:

    I.    RESPONDENT CFL DOES NOT HAVE STANDING TO MOVE FOR THE RETURN OF THE ALLEDGEDLY IMPROPERLY SEIZED PROPERTY UNDER FEDERAL RULE OF CRIMINAL PROCEDURE 41(G).....10

    II.   THIS COURT SHOULD ALLOW MAGISTRATE JUDGES TO ISSUE WARRANTS AUTHORIZING THE GOVERNMENT TO SEIZE ALL COMPUTER EQUIPMENT AND FILES FOR LATER SORTING WHERE THE SEIZURE IS BOTH REASONABLY NECESSARY UNDER THE CIRCUMSTANCES AND SUBJECT TO ADEQUATE PROCEDURAL SAFEGUARDS. ....13

        A.    This Court Should Not Require Magistrate Judges to Comply with Specific, Predetermined Requirements in Issuing Search Warrants Authorizing the Seizure of Digital Evidence Because Magistrates Are Capable of Determining the Appropriate Breadth and Particularity of a Search Warrant in the Digital Evidence Context. ....15

        B.    This Court Should Refuse to Uphold the Test Adopted by the Ninth and Fourteenth Circuits Because the Constantly Changing Nature of Technology Cautions Against Fashioning Such an Overbroad Test.....25

        C.    The Requirements Enumerated by the Ninth and Fourteenth Circuits Are Unsuitable for Every Search and Seizure Case Involving Digital Evidence. .30

III.	WHEN PERFORMING DIGITAL SEARCHES, THE GOVERNMENT MAY RELY ON THE “PLAIN VIEW” EXCEPTION TO THE PARTICULARITY REQUIREMENT BECAUSE THE EXCEPTION IS FIRMLY EMBEDDED IN THIS COURT’S BODY OF PRECEDENT AND FINDS SUPPORT IN THE FUNDAMENTAL PRINCIPLES OF THE FOURTH AMENDMENT.....	34
A.	The Officers Were Lawfully Present in the Place Where the Evidence Was in Plain View.....	35
B.	The Incriminating Nature of Information in Plain View Was Immediately Apparent.....	36
C.	The Government Had a Lawful Right of Access to the Records Discovered in Plain View.....	38
D.	In the Instant Case, the Application of the Plain View Doctrine is Wholly Consistent with the Constitutional Protections Served by the Fourth Amendment’s Warrant Requirements.....	39
	CONCLUSION.....	40

## TABLE OF AUTHORITIES

<b>CASES</b>	<b>PAGE(S)</b>
<i>Andresen v. Maryland</i> , 427 U.S. 463 (1976) .....	22, 23, 27, 40
<i>Arizona v. Hicks</i> , 480 U.S. 321 (1987) .....	35
<i>Coolidge v. New Hampshire</i> , 403 U.S. 443 (1971) .....	<i>passim</i>
<i>Florida v. Jimeno</i> , 500 U.S. 248 (1991) .....	16
<i>Groh v. Ramirez</i> , 540 U.S. 551 (2004) .....	16
<i>Guest v. Leis</i> , 255 F.3d 325 (6th Cir. 2001).....	27
<i>Horton v. California</i> , 496 U.S. 128 (1990).....	30, 35, 36, 40
<i>In re Application of Madison</i> , No. 09-mc-647 (DLI), 2009 WL 3792280 (E.D.N.Y. 2009) .....	18
<i>Kyllo v. United States</i> , 533 U.S. 27 (2001).....	29, 30
<i>Marron v. United States</i> , 275 U.S. 192 (1927) .....	16
<i>Massachusetts v. Sheppard</i> , 468 U.S. 991 (1984) .....	16
<i>Ohio v. Robinette</i> , 519 U.S. 33 (1996).....	14
<i>Pennell v. City of San Jose</i> , 485 U.S. 1 (1988) .....	11
<i>Rakas v. Illinois</i> , 439 U.S. 128 (1978).....	11
<i>Retired Chicago Police Ass’n v. City of Chicago</i> , 76 F.3d 856 (7th Cir. 1996).....	12
<i>United States v. Abrams</i> , 615 F.2d 541 (1st Cir. 1980) .....	23
<i>United States v. Adjani</i> , 452 F.3d 1130 (9th Cir. 2008).....	19, 25, 27
<i>United States v. Alexander</i> , 574 F.3d 484 (8th Cir. 2009).....	30
<i>United States v. Carey</i> , 172 F.3d 1268 (10th Cir. 1999) .....	<i>passim</i>
<i>United States v. Comprehensive Drug Testing</i> , 513 F.3d 1085 (9th Cir. 2008).....	11, 13

<i>United States v. Comprehensive Drug Testing</i> , 579 F.3d 989 (9th Cir. 2009) .....	<i>passim</i>
<i>United States v. Crouch</i> , 648 F.2d 932 (4th Cir. 1981) .....	37, 38
<i>United States v. George</i> , 975 F.2d 72, 75 (2d Cir. 2002) .....	18
<i>United States v. Giberson</i> , 527 F.3d 882 (9th Cir. 2008) .....	<i>passim</i>
<i>United States v. Hill</i> , 459 F.3d 966 (9th Cir. 2006) .....	<i>passim</i>
<i>United States v. Leon</i> , 468 U.S. 897 (1984).....	14, 16
<i>United States v. Mann</i> , 389 F.3d 869 (9th Cir. 2004).....	18
<i>United States v. Ninety-Two Thousand Four Hundred Twenty-Two Dollars and Fifty-Seven Cents</i> (\$92,422.57), 307 F.3d 102 (3d Cir. 2002).....	22
<i>United States v. Raney</i> , 342 F.3d 551 (7th Cir. 2003) .....	18, 27
<i>United States v. Ribeiro</i> , 397 F.3d 43 (1st Cir. 2005).....	14
<i>United States v. Riley</i> , 906 F.2d 841 (2d Cir. 1990).....	27
<i>United States v. SDI Future Health</i> , 568 F.3d 684 (9th Cir. 2009) .....	19
<i>United States v. Smith</i> , 424 F.3d 992 (9th Cir. 2005).....	19
<i>United States v. Spilotro</i> , 800 F.2d 959 (9th Cir. 1986) .....	18, 19, 21
<i>United States v. Tamura</i> , 694 F.2d 591 (9th Cir 1981).....	14, 15, 22, 23
<i>United States v. Upham</i> , 168 F.3d 532 (1st Cir. 1999).....	36
<i>United States v. Wong</i> 334 F.3d 831 (9th Cir. 2003).....	14, 35, 37, 38
<i>Warth v. Seldin</i> , 422 U.S. 490 (1975).....	12
 <b>CONSTITUTIONAL AMENDMENTS</b>	
U.S. CONST. amend. IV. ....	1, 39

**OTHER AUTHORITIES**

Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75 (1994).....28

Thomas K. Clancy, *The Fourth Amendment of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L. J. 193 (2005).....28

U.S. Dep’t of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 43 (July 2002) .....24

## **QUESTIONS PRESENTED**

- (1) Does the Respondent, the Colonial Football League, have standing to sue on behalf of its players for the return of illegally seized property under Fed. R. Crim. P. 41(g)?
- (2) May the government rely on the “plain view” exception to the Fourth Amendment’s warrant requirement in digital searches, i.e., searches of computers, hard drives, disks, etc.?
- (3) May federal magistrates issue warrants authorizing the government to seize all computer equipment and files for later sorting, or must the particularity requirement be heightened in the digital evidence context, as per the guidelines announced by the Fourteenth Circuit below and in *United States v. Comprehensive Drug Testing*, 579 F.3d 989 (9th Cir. 2009)?

## **CONSTITUTIONAL PROVISIONS INVOLVED**

The Fourth Amendment of the United States Constitution provides in pertinent part that:

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

## STATEMENT OF THE CASE

In July 2008, the Federal Bureau of Investigation (FBI) began an investigation into the widespread use and distribution of illegal steroids by professional athletes. *StarTests v. United States* (“*StarTests I*”), Case No. 2010-W20, at \*1 (D. Wythe 2009); *StarTests v. United States*, (“*StarTests II*”), Case No. 2010-W23, at \*7 (14th Cir. 2009). During its investigation, the FBI collected a significant amount of evidence indicating that professional athletes, specifically players in the Colonial Football League (CFL), were illegally trafficking and using steroids. *StarTests II*, at \*7. During the course of the steroid investigation, the FBI assembled a case for probable cause that five professional football players had tested positive for steroid use. *StarTests I*, at \*1. Included in the evidence was information pertaining to illicit transactions as well as numerous eyewitness reports and taped conversations confirming that the five players discussed obtaining steroids in order to “keep the rivalry [between two of the prominent teams in the league] interesting” *StarTests II*, at \*7.

The FBI wanted to improve its case for possession and use by proving that the players had actually used the illegal steroids. *StarTests II*, at \*8. At this point in the investigation the FBI discovered that the CFL had administered a drug testing program beginning in 2003. *StarTests I*, at \*1; *StarTests II*, at \*8. As part of this program, the CFL hired Plaintiff StarTests, Inc. (StarTests) to conduct the tests and store the test results. *StarTests I*, at \*1; *StarTests II*, at \*8. StarTests is an independent business specializing in conducting drug tests for professional sports teams, corporations, and other organizations. *StarTests II*, at \*8. Since 2005, the CFL has required annual testing of all players, and StarTests has maintained all of the test results. *Id.* After discovering the CFL’s drug testing program, the FBI applied for a search warrant to seize

material related to their investigation into the five CFL players. *StarTests I*, at \*1; *StarTests II*, at \*8.

In its application before Magistrate Judge Leon in the United States District Court for the District of Wythe, the FBI sought the ability to search and seize “all computer records, files, and equipment” related to the StarTests-administered drug tests at StarTests’ facility in Millersville, Wythe. *StarTests II*, at \*8. The supporting affidavit explained that all computer equipment and files would need to be seized and reviewed at a later date because (1) the data to be retrieved was massive in quantity, and an “on-site” search was time prohibitive; (2) some file names may be mislabeled or deceptively labeled for confidentiality purposes (e.g. “FamilyPhoto3.jpg” for a test result sheet); and (3) de-encryption may require software not available on StarTests’ computers. *StarTests I*, at \*2. Magistrate Judge Leon was justifiably persuaded by the request and issued a warrant authorizing the FBI to search “computer equipment, storage devices, and—where an on-site search would be impractical—seizure of either a copy of all data or the computer equipment itself.” *StarTests I*, at \*2. Moreover, Judge Leon restricted the warrant to allow the search and seizure only of information “reasonably related to the investigation into the five named players’ illegal steroid use.” *StarTests I*, at \*2. The warrant also required that “law enforcement personnel trained in searching and seizing computer data” were to determine whether a computer needed to be seized. If computers or other equipment were seized, the warrant also required that “appropriately trained personnel were to review the data, retain the relevant information, and designate the remainder for return.” *StarTests I*, at \*2; *StarTests II*, at \*8.

On the morning of November 1, 2008, the FBI executed the search warrant on the StarTests Millerville facility. *StarTests I*, at \*2. It immediately became clear to the investigators that StarTests’ computer system configuration was far more complex than originally anticipated.

*StarTests II*, at \*8. The CFL was one of StarTests' largest clients, and the testing had been ongoing for the past four years. Therefore, StarTests' personnel indicated that most of the computers in the facility would include at least one database on the CFL drug test. *StarTests I*, at \*2. Moreover, in an effort to protect client confidentiality, StarTests employed a complex "computer-hopping" procedure whereby an individual's testing data was partitioned between three physically distinct computer databases. *StarTests I*, at \*2; *StarTests II*, at \*8. One database contained the players' personal and health information, another contained a database assigning ID numbers to individual players, and a third database contained the ID number along with the corresponding test results. *StarTests I*, at \*2; *StarTests II*, at \*8. Given the complexity of the data storage employed by StarTests, the head agent concluded that the search for the five players' information could take days, therefore, he ordered all computer equipment to be either seized or copied, depending on the equipment's ease of movement. *StarTests I*, at \*2. The seized or copied materials were then brought to the FBI computer forensics laboratory in Wythe City for further review. *StarTests II*, at \*8–9.

The FBI spent the next few weeks sorting through the vast databases. *StarTests II*, at \*9. Eventually, agents found the test results for the five players in question. During the course of the search, however, they also stumbled upon positive test results for other CFL players. *StarTests I*, at \*2; *StarTests II*, at \*9. Notably, the same documents containing the results of the five players listed in the search warrant included the test results for other players; the FBI did not encounter this information in documents for which it did not have probable cause. In addition to positive results for steroid use, the tests also showed that CFL athletes had tested positive for a myriad of other illegal substances, such as cocaine, marijuana, and various hallucinogens. *StarTests I*, at \*2. Rather than ignore this information, the FBI decided to expand their search to include within

the scope of the investigation all illegal drug possession and sale within professional football. *StarTests I*, at \*2. To this end, the FBI copied and inventoried StarTests' computer hard drives and databases, and returned all computer equipment and hard drives which did not contain information for which the FBI did not have probable cause. *StarTests I*, at \*2; *StarTests II*, at \*9.

## OPINIONS BELOW

### I. DISTRICT COURT PROCEEDINGS.

Following the FBI's seizure of electronic records and equipment, the Plaintiffs StarTests, Inc. (StarTests), and the Colonial Football League (CFL) filed a motion in the United States District Court for the District of Wythe for the return of property pursuant to Fed. R. Crim. P. 41(g). *StarTests II*, at \*9. The Appellants argued that the seizure of evidence was outside the scope of the warrant and therefore constituted an illegal search and seizure under the Fourth Amendment. *Id.* Consequently, Appellants claimed that the seized property must be returned. *Id.*

Relying upon the "plain view" doctrine explained by this Court in *Coolidge v. New Hampshire*, 403 U.S. 443 (1971), the government argued that no warrant was needed to seize the additional information because the information was in "plain view" when the government was performing a search supported by probable cause; therefore, the information was lawfully obtained and no 41(g) motion could stand. *StarTests II*, at \*9. Moreover, the government claimed that the Appellants' argument was moot as they lacked standing in the matter. *Id.*

Finding that other circuits had found the plain view exception applicable to digital evidence seizure cases, the district court applied a three-prong test and found that the government had met all the required elements. *Id.* First, the district court found that the officers were lawfully present when they located the additional evidence because they had not wandered

outside the scope of the initial search. *StarTests I*, at \*5; *StarTests II*, at \*9. Second, the FBI already had a lawful right of access because they were already performing a search of the relevant databases pursuant to a valid warrant supported by probable cause. *StarTests I*, at \*5; *StarTests II*, at \*9. Finally, the incriminating character of the information was immediately apparent to the searching agents because the incriminating test results appeared in a common database with the materials sought by the warrant, and no additional steps were required to open or access the results. *StarTests I*, at \*6; *StarTests II*, at \*9. Moreover, positive test results for “anabolic steroids” or “cocaine” made criminal activity immediately apparent. *StarTests I*, at \*6.

Based upon these facts, the district court sided with the majority of circuit courts and held that deference should be given to neutral and detached magistrates when determining the reasonableness of the restrictions on computer searches. *StarTests II*, at \*9. Finding that the warrant was valid and adopting the plain view doctrine, the district court denied the Plaintiffs’ 41(g) motion.

## **II. CIRCUIT COURT PROCEEDINGS.**

After the district court denied the 41(g) motion, the Plaintiffs filed a timely appeal. *StarTests II*, at \*9. In their appeal, the Plaintiffs’ argued that the district court erred in finding the plain view exception applicable in digital evidence cases. *Id.* Moreover, the Plaintiffs contended that even if the plain view exception were validly applied, their motion should still have been granted because Plaintiffs felt that the district court’s warrant was overbroad and therefore invalid. *Id.*

In reply, the government argued that, as a threshold issue, the CFL had no privacy interest in the electronic test results, and that therefore the CFL lacked the requisite standing to bring the 41(g) motion. *Id.* Furthermore, the government asserted (1) that the search warrant at

issue was not impermissibly overbroad; and (2) that the plain view doctrine should apply in the Fourteenth Circuit, as it does in a majority of the other circuits. As to the second argument, the government posited that the seizure of the electronic databases and equipment was lawful because the information was in “plain view” during a search supported by a warrant and probable cause. *Id.* at \*9–10. Breaking with the other circuit courts, the Fourteenth Circuit reversed the district court’s decision and instead adopted the five-prong test set forth by the Ninth Circuit in *United States v. Comprehensive Drug Testing* (“*CDT II*”), 579 F.3d 989 (9th Cir. 2009). *Id.* at \*17. The test announced by the Ninth Circuit requires a magistrate judge to observe the following rules when issuing a warrant in a digital evidence case:

- (1) Magistrates should insist that the government waive reliance upon the plain view doctrine.
- (2) Segregation and redaction of the computer evidence must be either done by specialized personnel or an independent third party. If done by government personnel, that personnel must agree not to disclose any information other than that which is the target of the warrant.
- (3) Warrants must disclose the actual risks of destruction or concealment of information, as well as prior efforts to seize that information in other courts.
- (4) The government’s search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by non-computer personnel agents.
- (5) The government must destroy, or, if the recipient may lawfully possess it, return non-responsive data, at all times keeping the court informed of its progress. *Id.* at \*17.

The government now appeals the Fourteenth Circuit’s decision. *Id.* at \*20.

### **SUMMARY OF THE ARGUMENT**

This Court should reverse the Fourteenth Circuit’s decision granting StarTests’ and the CFL’s motion to return the allegedly improperly seized test results at issue in this case on three separate grounds.

First, the CFL does not have standing, under the associational standing doctrine, to bring a motion for the return of the allegedly improperly seized items under Federal Rule of Criminal

Procedure 41(g). The only parties with privacy interests at stake in the records are StarTests and the individual players whose tests results are involved in this case. The CFL has argued—and the District Court of Wythe and Fourteenth Circuit have accepted the argument—that the contractual privity it has with the players and with StarTests suffices to satisfy the elements of the associational standing doctrine. Although superficially appealing, this argument is specious because the interests sought to be protected are not actually germane to the organization’s purpose and because the CFL has a conflict of interest. This Court should therefore reverse the decision of the Fourteenth Circuit insofar as it held that the CFL has standing.

In any event, regardless of whether the CFL has standing to bring the Rule 41(g) motion, the Fourteenth Circuit’s decision should be reversed on the merits for two compelling reasons. First, magistrate judges should not be forced to comply with the five requirements imposed by the Fourteenth Circuit because they are capable of determining, *sua sponte*, the appropriate particularity of a warrant and the necessary procedural safeguards to protect the privacy interests involved. Second, the government should be entitled to rely on the plain view doctrine in digital evidence cases.

First, the Fourteenth Circuit erred in holding that the search warrant issued by Magistrate Judge Leon was not sufficiently particular; and by imposing five bright-line requirements on magistrates, the Fourteenth Circuit adopted a test unsupported by precedent and belied by the discretionary role traditionally given to magistrates in issuing search warrants. Notably, the Fourteenth Circuit did not cite to any case—other than a Ninth Circuit case which similarly is contradicted by its own precedent and should likewise be overruled—supporting its adoption of the five requirements. In addition, the Fourteenth Circuit’s test offends the notion that magistrates are capable of determining the appropriate breadth and particularity of a search

warrant, even in cases involving difficult technological issues. The tests previously endorsed by this Court and the circuit courts were both manageable and produced just results, and should not be replaced by overbroad, unproven restrictions on magistrates' discretion. Finally, given the context of digital evidence, it is often impossible for the government to know how or where a target has organized and/or classified documents. In light of the lack of precedent supporting the Fourteenth Circuit's decision, the ability of magistrates to issue appropriately particular search warrants without the help of an overbroad test, and the difficulties inherent in particularizing a warrant for digital evidence, this Court should (1) allow magistrates issue warrants authorizing the government to seize computer equipment and data for later sorting rather than hold magistrates to heightened requirements of particularity and (2) reverse the contrary holding of the Fourteenth Circuit.

Second, the Fourteenth Circuit should be overruled on the ground that the government should not be made to forswear reliance on the plain view exception to the warrant requirement. The plain view exception is firmly rooted in this Court's jurisprudence and is wholly consistent with the fundamental rights embodied in the Fourth Amendment. As this Court has held, the applicability of the plain view doctrine should be a fact driven determination, and not one that is universally proscribed in all digital evidence cases. Regardless of the case, three elements must exist before the plain view exception may be relied upon. These elements alone are sufficient to ensure that the government does not overstep the bounds of the Fourth Amendment, for when the government offends the Fourth Amendment it will also offend one of the three elements and the plain view doctrine will be held inapplicable to that particular set of facts. In the instant case, however, these three elements were met. The government was lawfully present in the location where the evidence was in plain view, the evidence's incriminating character was immediately

apparent, and the government agents had a right of access to the contested evidence.

Consequently, the evidence in this case was obtained in a manner entirely consistent with Fourth Amendment jurisprudence. As such, the Fourteenth Circuit's blanket rejection of the plain view doctrine in digital evidence cases is an unwise and simplistic bright line rule that excludes far more evidence than is constitutionally necessary, therefore, the holding below should be overruled.

## ARGUMENT

### **I. RESPONDENT CFL DOES NOT HAVE STANDING TO MOVE FOR THE RETURN OF THE ALLEGEDLY IMPROPERLY SEIZED PROPERTY UNDER FEDERAL RULE OF CRIMINAL PROCEDURE 41(G).**

The Fourteenth Circuit's holding that the CFL has standing to move for the return of StarTests' allegedly improperly seized property under Federal Rule of Criminal Procedure 41(g), because "the CFL was certainly 'one against whom the search was directed,' and is now therefore a person aggrieved by this potentially unlawful search and seizure," should be overruled because the CFL "is neither a victim nor a direct target," of the government's search. Rather, the CFL has attempted to substitute as its own interest the privacy interests of its individual players. *StarTests I*, at \*3; *StarTests II*, at \* 10.

Rule 41(g) permits "person[s] aggrieved by an unlawful search and seizure of property or by the deprivation of property [to] move for the property's return." Fed. R. Crim. P. 41(g). In *Rakas v. Illinois*, the Supreme Court held that "a person aggrieved by an unlawful search and seizure" is either a "victim [or] 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 v. Illinois*, 439 U.S. 128, 134–35 (1978). The CFL falls into the latter category because the search was not directed at the CFL, but at the individual

players of the CFL, through the information maintained by StarTests. The CFL has joined StarTests in bringing the 41(g) motion not because it is concerned about protecting its players' test results, but because it wants to avoid being sued by certain players or the Players' Union for breaching a confidentiality agreement into which the CFL entered with its players. Notably, the CFL did not tell its players that the tests it administered would be organized in such a way as to allow investigators to ascertain the identity of the players who tested positive for drugs.

An association has standing to assert the Fourth Amendment rights of its members, which encompasses the Rule 41(g) motion seeking return of seized property, if: (1) the members would otherwise have independent standing to sue; (2) the interests sought to be protected are germane to the organization's purpose; and (3) the claim asserted does not require the participation of individual members in the lawsuit. *Pennell v. City of San Jose*, 485 U.S. 1, 7 n.3 (1988); accord *United States v. Comprehensive Drug Testing* ("CDT P"), 513 F.3d 1085, 1096 (9th Cir. 2008). Here, the CFL cannot meet all three of these requirements—most notably the second and third—and should therefore be precluded from asserting standing on behalf of its players. The District Court for the District of Wythe held that the second element is met because “[the] CFL is charged with protecting [players’ privacy] interests—especially in an instance where their privacy was intruded upon under the CFL’s prerogative.” *StarTests I*, at \*3. This point is unpersuasive because it allows associations to satisfy the second element merely by showing contractual privity. This should be rejected because in light of the fact that there is almost always some form of contractual privity in the context of associational membership, which would essentially eviscerate the second requirement. The district court likewise held that the CFL did not need to establish the third element because the nature of the relief sought obviated the need for such a requirement. *Id.* As justification for this proposition, the court cited to

*Warth v. Seldin*, 422 U.S. 490 (1975), a case that was decided before *Pennell* and *Rakas*.

Additionally, some of the members who tested positive for drugs during the years in question would be required to participate in the lawsuit in order to protect their interests. In light of the district court's failure to address these point satisfactorily, and of the Fourteenth Circuit's failure to further address the issue, this Court should reverse the Fourteenth Circuit on the issue of standing.

In addition to its inability to meet the three required elements, the CFL does not have standing to bring this 41(g) motion on behalf of its players because an irreconcilable conflict of interest between itself and its players exists. Associational standing is inappropriate where the association's lawsuit, if successful, would result in detriment to the interests of some of its members, and therefore creates a "profound conflict of interest." *Retired Chicago Police Ass'n v. City of Chicago*, 76 F.3d 856, 864 (7th Cir. 1996). A sufficiently "profound conflict of interest" is established where litigation will simultaneously result in a benefit and a detriment to a portion of an association's members. *Id.* Although not immediately apparent, the CFL is not in the position to advocate for the privacy interests of the players because if the government decided to expand its investigation to include the CFL, the CFL would be compelled to argue that the issue concerns the players' steroid use rather than its own endorsement of steroids, which would be inconsistent with the players' position. Additionally, the CFL's purpose is inconsistent with the players' interests in maintaining the confidentiality of the test results, because disclosure of individual results to the CFL could result in disciplinary action resulting from "ensure[d] compliance with federal and state law." *StarTests I*, at \*3. By the terms of the CFL's agreement with its players, the CFL assured players that individual test results would remain anonymous to CFL officials. Thus, the CFL's claim of right to nothing more than an attempt to salvage the

appearance that it honored its prior commitment to its players. *StarTests I*, at \*1. (“The players were further assured that their names and test results would remain confidential and stored in [sic] at StarTests facility, with *only the percentage being released to the CFL* and the public.”) (emphasis added).

In *United States v. Comprehensive Drug Testing*, the government challenged the respondent’s standing to bring a Rule 41(g) motion for the return of drug testing records belonging to its members, arguing that the respondent-player’s association could not assert a property interest in the privacy interests of individual members. *CDT I*, 513 F.3d at 1096. The court held that the respondent had standing because the purpose of the player’s association was to protect the interests of the players, rendering their interests at trial sufficiently similar to warrant associational standing. *Comprehensive Drug Testing*, 473 F.3d at 926. The government contests this holding, as well as the holding of the Fourteenth Circuit, and urges this Court to find that the CFL does not have standing, under the associational standing doctrine, to bring a 41(g) motion for the return of *StarTests*’ documents containing the *players*’ information.

**II. THIS COURT SHOULD ALLOW MAGISTRATE JUDGES TO ISSUE WARRANTS AUTHORIZING THE GOVERNMENT TO SEIZE ALL COMPUTER EQUIPMENT AND FILES FOR LATER SORTING WHERE THE SEIZURE IS BOTH REASONABLY NECESSARY UNDER THE CIRCUMSTANCES AND SUBJECT TO ADEQUATE PROCEDURAL SAFEGUARDS.**

Contrary to the holdings of the Fourteenth Circuit in *StarTests v. United States (StarTests II)*, Case No. 2010-W23 (14th Cir. 2009) and the Ninth Circuit in *United States v. Comprehensive Drug Testing* (“*CDT II*”), 579 F.3d 989 (9th Cir. 2009), federal magistrate judges should be permitted to issue warrants authorizing government officials to seize all computer equipment and files for later sorting as long as the seizure is reasonably necessary

under the circumstances and is subject to adequate procedural safeguards, tailored to the specific facts of the case. Magistrate judges should not be held to the bright-line, prophylactic requirements set forth by the Ninth and Fourteenth Circuits because those requirements are inconsistent with this Court’s precedent as well as the compelling policy on which that precedent is established.

The very fact that the Ninth and Fourteenth Circuits have imposed bright-line requirements on magistrates offends this Court’s search and seizure precedent. *See Ohio v. Robinette*, 519 U.S. 33, 39 (1996) (“[W]e have consistently eschewed bright-line rules, instead emphasizing the fact-sensitive nature of the reasonableness inquiry.”). Furthermore, the requirements go beyond what is necessary to strike the appropriate balance between the “legitimate [investigatory] needs of law enforcement and the right of individuals and enterprises to the privacy that is at the heart of the Fourth Amendment.” *CDT II*, 579 F.3d at 1006. Magistrates are capable of protecting the privacy and property interests of individuals against overzealous government investigators by determining the appropriate breadth of a search warrant under the circumstances. For this reason, this Court—as well as federal circuit courts—has consistently underscored the importance of deferring to the judgment of detached, neutral magistrates, albeit not blindly. *See United States v. Leon*, 468 U.S. 897 (1984) (“[A] search warrant ‘provides the detached scrutiny of a neutral magistrate, which is a more reliable safeguard against improper searches than the hurried judgment of a law enforcement officer ‘engaged in the often competitive enterprise of ferreting out crime,’” [and] we have expressed a strong preference for warrants. . . . Deference to the magistrate, however, is not boundless.”); *United States v. Ribeiro*, 397 F.3d 43 (1st Cir. 2005); *United States v. Wong*, 334 F.3d 831, 836 (9th Cir. 2003); *United States v. Tamura*, 694 F.2d 591, 596 (9th Cir 1981) (“The essential

safeguard required is that wholesale removal [of evidence] must be monitored by a neutral, detached magistrate.”). Although magistrates should exercise “exacting scrutiny” on government applications for broad search warrants in the context of digital evidence (and should perhaps even consider imposing a meticulous procedure that government officers must comply with in carrying out the warrant if the facts of the case so require), magistrates should not be divested of their ability to exercise discretion by an imprecise and unsupported rubric, which is precisely the threat posed by the test adopted in *StarTests* and *Comprehensive Drug Testing*. See *Tamura*, 694 F.2d 591; *CDT II*, 579 F.3d at 1018 (Bea, J., concurring in part and dissenting in part) (“Given the numerous risks to privacy [implicated by issuing warrants authorizing the search and seizure of digital evidence] . . . we ought to require a magistrate to give *exacting scrutiny* to the scope of the search, so to ensure the search is as narrowly tailored as possible to the goal of seizing evidence specifically described in a warrant.”) (emphasis added). The same safeguards on which our system of criminal justice relies in the context of searches and seizures of tangible evidence should apply in the context of digital evidence, because the privacy risks implicated by seizures of digital evidence can be adequately protected by the vigilance of a magistrate acting *sua sponte*, as they were in the case before this Court.

A. **This Court Should Not Require Magistrate Judges to Comply with Specific, Predetermined Requirements in Issuing Search Warrants Authorizing the Seizure of Digital Evidence Because Magistrates Are Capable of Determining the Appropriate Breadth and Particularity of a Search Warrant in the Digital Evidence Context.**

This Court should refuse to adopt—and declare invalid—the tests set forth in *StarTests II* and *Comprehensive Drug Testing* because magistrates are capable of determining the appropriate breadth and particularity of a search warrant in any context, and because imposing bright-line requirements on magistrates in connection with the issuance of search warrants is unsupported

by this Court's precedent. In fact, the requirements listed in *Comprehensive Drug Testing*, adopted verbatim by *StarTests II*, run afoul of the Ninth Circuit's *own* precedent. Instead of binding magistrates by the strict requirements listed by the Ninth and Fourteenth Circuits, this Court should permit magistrates to issue warrants authorizing the seizure of all computer equipment if it is reasonable under the circumstances.

First, the requirements adopted by the Ninth and Fourteenth Circuits represent a drastic and unfounded departure from the search and seizure precedent of this Court as well as that of the Ninth Circuit. The Fourth Amendment requires, *inter alia*, that "search warrants describe the things to be seized with sufficient particularity to prevent general exploratory" searches by government officers. *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999) (citing *Marron v. United States*, 275 U.S. 192, 196 (1927)). A search warrant that fails particularly to describe the items to be searched and seized, as well as any search actually performed under such a warrant, is unconstitutional. *See Groh v. Ramirez*, 540 U.S. 551 (2004) (citing *Massachusetts v. Sheppard*, 468 U.S. 991 (1984)). While this Court's Fourth Amendment jurisprudence has constantly adapted to reflect the change in technology, it has never accepted a bright-line test imposing specific requirements on magistrate judges in issuing search warrants. Rather, this Court—and even the Ninth Circuit—has recognized that "under the Fourth Amendment, the standard is reasonableness." *United States v. Hill*, 459 F.3d 966 (9th Cir. 2006), *aff'g* 322 F. Supp. 2d 1081 (C.D. Cal. 2002); *Florida v. Jimeno*, 500 U.S. 248 (1991) ("[T]he touchstone of the Fourth Amendment is reasonableness."). The government concedes that the *Comprehensive Drug Testing* requirements may be reasonable in some situations. In fact, it may be unreasonable in some situations *not* to require specialized personnel to segregate data within the scope of the warrant's probable cause from data outside, and to redact the data where necessary

(the second requirement). In addition, it may be unreasonable *not* to require the government constantly to keep the magistrate apprised of what information retained and what is returned (the fifth requirement). Instead of fashioning a five-step test for magistrates to follow, however, this Court should continue to sanction magistrate judges' issuance of reasonably particular warrants based on probable cause. This Court has consistently analyzed Fourth Amendment issues by determining what is reasonable under the specific facts of the case, and should continue to allow the particularity requirement in the context of digital evidence search warrants to develop by the traditional "common law method of reasoned decision-making." *CDT II*, 579 F.3d at 1018 (Bea, J., concurring in part and dissenting in part).

This point was emphasized in a dissenting opinion in *Comprehensive Drug Testing*. There, Judge Callahan wrote that the "new guidelines are troubling because they are overbroad and restrict how law enforcement personnel can carry out their work without citing to a single legal authority that would support these new rules." *CDT II*, 579 F.3d at 1013 (Callahan, J., concurring in part and dissenting in part). StarTests and the CFL likewise cannot point to a single case which persuasively supports the adoption of these rules to take the place of the magistrate judge's discretion. In fact, one Ninth Circuit case, decided only one year before *Comprehensive Drug Testing*, refused to "impose heightened Fourth Amendment protections in computer search cases as a result of a computer's ability to store large amounts of potentially intermingled information" because "heightened protection[] must be 'based on a principle that is not technology-specific.'" *Id.* (quoting *United States v. Giberson*, 527 F.3d 882, 887–88 (9th Cir. 2008)). As Judge Callahan observed and as is argued *infra*, the rule adopted by the Ninth and Fourteenth Circuits is technology-specific, and could be rendered obsolete by further advances in technology within the next five years. If, for example, reasonably-priced software

becomes available that gives government agents the ability to perform pinpointed searches to accurately locate documents containing certain images, words, or numbers, the second and fourth requirements would both become superfluous: such an accurate program would obviate the need for specialized, independent personnel because the software would in effect accomplish the role of the personnel, and the software would be designed so that the government accessed only that information for which it has probable cause, so the fourth requirement would be meaningless. The government urges this Court to hold that there is no reason to grant heightened Fourth Amendment protection to searches of computers and digital evidence in light of the dearth of support in the case law. *See Hill*, 459 F.3d at 973–75; *Carey*, 172 F.3d at 1272–73; *United States v. Raney*, 342 F.3d 551 (7th Cir. 2003).

Second, the *Star Tests II* and *Comprehensive Drug Testing* requirements should be rejected by this Court because magistrates are capable of determining the appropriate breadth and particularity of a warrant without hard and fast guidelines. The particularity clause of the Fourth Amendment requires that “[t]he description [in the search warrant] . . . must be specific enough to enable the person conducting the search reasonably to identify the things authorized to be seized.” *United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986); *see also United States v. Mann*, 389 F.3d 869, 877 (9 Cir. 2004) (“While a search warrant must describe items to be seized with particularity to prevent a general, exploratory rummaging in a person’s belonging, it need only be reasonably specific, rather than elaborately detailed.”); *In re Application of Madison*, No. 09-mc-647 (DLI), 2009 WL 3792280 (E.D.N.Y. 2009) (citing *United States v. George*, 975 F.2d 72, 75 (2d Cir. 2002) (“A warrant is sufficiently particular if it ‘enable[s] the executing officer to ascertain and identify with *reasonable certainty* those items that the magistrate has authorized him to seize.”)). The inquiry is fact-sensitive and requires the

magistrate to exercise discretion to determine what would be reasonable under the circumstances. Furthermore, “[t]he specificity required in a warrant varies depending on the circumstances of the case and the type of items involved. Warrants which describe generic categories of items are not necessarily invalid if a more precise description of the items subject to seizure is not possible.” *Spilotro*, 800 F.2d at 963; accord *United States v. SDI Future Health*, 568 F.3d 684 (9th Cir. 2009); *Hill*, 459 F.3d at 976; *United States v. Adjani*, 452 F.3d 1130, at 1147 (9th Cir. 2008) (“[T]he level of detail necessary in a warrant is related to the particular circumstances and the nature of the evidence sought.”). StarTests and the CFL have attempted to demonstrate that the requirements are merely guideposts which merely focus the inquiry which magistrates must make. This argument is a half-truth, because although the requirements do not entirely replace the judgment of a magistrate, they do push the discretion of a magistrate to the vanishing point. The requirements dictate what a magistrate must consider in the context of a warrant authorizing the search of digital evidence, and if those requirements are not met, the warrant must not be issued. *See StarTests II*, at \*17. This result is inconsistent with the role traditionally afforded to magistrate judges.

The restrictions imposed by Magistrate Judge Leon in this case reveal the overbreadth of the *StarTests* rubric in practice, and demonstrate that magistrates are capable of determining the appropriate breadth of a search warrant even in the complex digital evidence context. The generic search warrant in this case was valid despite not following all of the five requirements because, given the complex nature in which StarTests organizes and classifies its data and the government’s lack of knowledge about StarTests’s organization and classification at the time the warrant was issued, it was impossible for the government to offer a more precise description of the items without sacrificing its ability to locate the information for which it had probable cause

to search. *Cf. United States v. Smith*, 424 F.3d 992 (9th Cir. 2005) (holding that a search warrant for “virtually all of [the defendant’s] personal and business records, electronic documents, photographs and videotapes” was sufficiently particular in light of the fact that the government had probable cause, supported by a detailed affidavit, to believe that the crime “permeated the entire business operation”). Here, as in *Smith*, the information regarding the CFL players permeated the StarTests computer equipment and documents.

Notably, Judge Leon did impose the second and fourth requirement on the government’s warrant because those requirements are reasonable in this case. First, Judge Leon ordered that “‘law enforcement personnel trained in searching and seizing computer data’ were to determine whether a computer needed to be seized.” *StarTests I*, at \*2. This restriction would not be necessary in every case, such as where the search involves an individual’s residence rather than a corporation with a legion of computers and high-tech equipment, but was necessary in this case to protect the privacy interests of individuals outside the scope of the investigation in this case. Second, “[i]f computers or other equipment were seized, ‘appropriately trained personnel’ were to then review the data, retaining the information authorized by the warrant and designating the remainder for return.” *Id.* This precaution was likewise well-suited to the facts of this case; given the narrow scope of the investigation and the massive quantity of equipment and databases on which the relevant information was stored, it was necessary here to limit the ability of government officers to review all of the data stored on the StarTests computers. Third, “the judge restricted the search and seizure to information ‘reasonably related to the investigation into the five named players’ illegal steroid use.’” *Id.* This restriction essentially assured that the seizure was a permissibly particular one; the fact that the judge ordered that evidence not relating to the ten players was to be returned ensured that the search only permitted the seizure of

evidence for which the government had probable cause. All of these restrictions protect against individual privacy interests and show that magistrates are capable of striking an appropriate balance between the government's investigatory prerogative with privacy and property interests without the imposition of bright-line requirements.

Although magistrate judges may not always be as thoughtful and deliberative as Magistrate Judge Leon, there are procedural safeguards in place to mitigate against the damages caused by an overbroad search warrant, namely, the motion to suppress and the motion to return improperly seized property. *See* Fed. R. Crim. P. 41(g) (“A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property’s return.”), 41(h) (“A defendant may move to suppress evidence in the court where the trial will occur, as Rule 12 provides.”). Courts frequently are called to determine whether a search warrant issued by a magistrate was sufficiently particular. In order to make this determination, courts reviewing a magistrate’s warrant generally consider (1) “whether probable cause exists to seize all items of a particular type described in the warrant[;]” (2) “whether the warrant sets out objective standards by which executing officers can differentiate items subject to seizure from those which are not[;]” and (3) “whether the government was able to describe the items more particularly in light of the information available to it at the time the warrant was issued.” *Spilotro*, 800 F.2d at 963 (citations omitted). These three considerations are neither exhaustive requirements nor necessary elements; they are simply three factors for the court to consider in analyzing whether the warrant was sufficiently particular. In reviewing these factors, courts “ensure[] that the magistrate issuing the warrant is fully apprised of the scope of the search and thus determine whether the entire search is supported by probable cause.” *Id.* Search warrants are not always sufficiently particular and magistrates may at times be swayed by the

government's ex parte argument that it would be unjustifiably difficult to narrow the scope of a search warrant. However, these realities do not compel the conclusion that magistrates should be required to consult a set of requirements before issuing a search warrant. Rather, they justify an individual's ability to contest a search warrant as insufficiently particular, a safeguard that protects the right to privacy in and of itself. This Court should continue to allow magistrates to issue warrants that authorize the wholesale seizure of digital evidence if it is appropriate under the circumstances; if the search warrant sanctions the seizure of more evidence than the government has probable cause for, and does not provide for the return of that evidence, there are adequate remedies at law to prevent the government from using it.

Finally, imposing additional requirements on magistrates is unnecessary because the precedent in place before *Comprehensive Drug Testing* and *StarTests II* was perfectly manageable and produced just results. Before *Comprehensive Drug Testing* was decided, the Ninth Circuit relied on the landmark case of *United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982). Under the rule fashioned by *Tamura*, which is similar to the rules which the majority of circuits currently embrace (see *United States v. Ninety-Two Thousand Four Hundred Twenty-Two Dollars and Fifty-Seven Cents (\$92,422.57)*, 307 F.3d 102 (3d Cir. 2002); *United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999)):

In the comparatively rare instances where documents are so intermingled that they cannot feasibly be sorted on site, we suggest that the government and law enforcement officials generally can avoid violating Fourth Amendment rights by *sealing and holding the documents pending approval by a magistrate of a further search*, in accordance with the procedures set forth in the American Law Institute's Model Code of Pre-Arrest Procedure. If the need for transporting the documents is known to the officers prior to the search, they may *apply for specific authorization for large-scale removal of material*, which should be granted by the magistrate issuing the warrant only *where on-site sorting is infeasible and no other practical alternative exists*. The essential safeguard required is that wholesale removal must be monitored by the judgment of a neutral, detached magistrate.

*Tamura*, 694 F.2d at 595–96 (emphasis added). *Tamura* suggests that in certain cases, “responsible officials” should conduct searches of the documents so as to “minimize[] unwarranted intrusions into privacy.” *Id.* at 596 n.4 (quoting *Andersen v. Maryland*, 427 U.S. 463, 482 n.11 (1976)). *Tamura* noted 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 search.” *Id.* at 595. The court distinguished a search of all items in a set of files, however, from a seizure of all items, observing that “the wholesale *seizure* for later detailed examination of records not described in a search warrant is significantly more intrusive, and has been characterized as “the kind of investigatory dragnet that the Fourth Amendment was designed to prevent.” *Id.* (quoting *United States v. Abrams*, 615 F.2d 541, 543 (1st Cir. 1980)). Although this observation was true in that case, it does not apply with equal force here. *Tamura* involved the seizure of paper documents located in twelve boxes, which the government could have reviewed on-site without incurring much difficulty and without unduly intruding on the defendant’s privacy rights. By contrast, the situation here involved several computers containing hundreds of thousands of documents, all of which potentially contained the information for which the government had probable cause to search. It would be unreasonable, and indeed more intrusive, to require the government to inspect all of those computers on-site. Such a search may have taken several days. Additionally, although *Tamura* and *Abrams* recognized that the search would be more intrusive, it did not say that such a search was per se unconstitutional.

Expanding on *Tamura*, the Ninth Circuit in *Hill* emphasized that the government’s affidavit should justify why a search warrant permitting a broad seizure would be appropriate under the facts of the case: “Although computer technology may in theory justify blanket

seizures [of digital evidence], the government must still demonstrate to the magistrate *factually* why such a broad search and seizure authority is reasonable in the case at hand.” 459 F.3d at 975 (“[T]here must be some threshold showing before the government may ‘seize the haystack to find the needle.’”). In support of this proposition, *Hill* cited a Department of Justice recommendation, which explains that “the affidavit should explain th[e] expectation [that seizure may be necessary] and its basis to the magistrate judge[,] . . . inform the court of the practical limitations of conducting an on-site search, and . . . articulate the plan to remove the entire computer from the site if it becomes necessary.” *Id.* at 976 (quoting U.S. Dep’t of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 43, 69 (July 2002)). The procedures and tests outlined in *Tamura* and honed by *Hill* are entirely appropriate in the context of digital evidence, and need not be replaced by the five-prong requirements set forth by *StarTests II* and *Comprehensive Drug Testing*. Instead of imposing these requirements, this Court should allow magistrate judges to impose requirements *sua sponte*, as they deem necessary given the circumstances of the case.

Because the tests adopted by the Ninth and Fourteenth Circuits find no refuge in this Court’s—or any circuit court’s—precedent, and because magistrates are capable of determining the appropriate breadth and particularity of a search warrant given the facts and circumstances of each case, this Court should reject the requirements imposed by those circuits on magistrates. The main risk which led the majority in *Comprehensive Drug Testing* to adopt the five-prong test at issue, that “every warrant for electronic information will become, in effect, a general warrant, [will] render[] the Fourth Amendment irrelevant,” was vastly overstated by that court. 579 F.3d at 1004. As long as neutral, detached magistrates exercise appropriate judgment, the risk will be mitigated or avoided completely. While it is true that magistrates must be ever-mindful of the

risk of infringing on privacy rights, and accordingly must fashion appropriate procedural safeguards, tailored to the case, to protect the privacy and property interests of individuals, imposing bright-line requirements on magistrates is the incorrect way to address this risk. This Court should guide other courts to “employ[] the traditional common law method of deciding novel questions of law . . . by limiting [] decisions as precisely as possible to the case at hand . . . [and thereby] evaluat[ing] different cases over time to discern the most sensible rule given the technologies that develop.” 579 F.3d at 1018 (Bea, J., concurring in part and dissenting in part).

**B. This Court Should Refuse to Uphold the Test Adopted by the Ninth and Fourteenth Circuits Because the Constantly Changing Nature of Technology Cautions Against Fashioning Such an Overbroad Test.**

The Fourth Amendment’s requirement that warrants particularly describe “the place to be searched, and the persons or things to be seized” is difficult to satisfy in the context of digital evidence because it is often impossible for the government to know precisely where evidence is stored within a computer or comparable technological device. *See, e.g., Adjani*, 452 F.3d at 1150; *Giberson*, 527 F.3d 882; *Hill*, 459 F.3d at 978. But, as one court has noticed, “[c]omputers are simultaneously file cabinets . . . and locked desk drawers; they can be repositories of innocent and deeply personal information, but also of evidence of crimes. The former must be protected, the latter discovered.” *Adjani*, 452 F.3d at 1152. Although the requirements set forth by *StarTests II* and *Comprehensive Drug Testing* may provide for increased privacy under some circumstances, the requirements unduly restrict the government’s ability constitutionally to search for information stored in computers or other digital databases. The requirements go beyond what is necessary to protect the interests of individual privacy and straightjacket the government’s ability to perform constitutionally valid searches and seizures. Because of the unique difficulties presented by search warrants for digital evidence and the constantly changing

nature of technology, it is necessary to allow magistrates to issue warrants authorizing government officers to seize all computer equipment and files for later sorting in appropriate cases and with appropriate procedural safeguards.

Due to the many complex ways in which one can organize, disguise, and encrypt potentially inculcating electronic files on a computer, perhaps only a clairvoyant could identify, *ex ante*, the particular location of digital evidence in a suspect's or target's computer. Specifically, and as the government has argued both in *StarTests II* and *Comprehensive Drug Testing*, computer files can be manipulated in any of the following ways to complicate the retrieval of electronic data: (1) files can be given misleading names or a false extensions; (2) "data might be erased or hidden;" (3) "there might be booby traps that 'destroy or alter data if certain procedures are not scrupulously followed[;]'" (4) it may be impossible to access certain files without proper software, "which may not be available on the computer that is being searched;" (5) the quantity of the information might make it impracticable to search everything at the location of the evidence; (6) "data might be encrypted or compressed, requiring passwords, keycards, or other external devices to retrieve[;]" and (7) the procedures necessary to "maintain the integrity of the evidence" may be extremely time-consuming due to the precision with which they must be carried out. 579 F.3d at 995 (internal citation omitted). This list is not exhaustive, but merely exemplary. Additionally, there are legitimate, lawful reasons a person or entity may conceal, encrypt, or compress data: "protection of privacy, preservation of privileged communications, warding off industrial espionage or preventing general mischief such as identity theft." *Id.*

As the majority opinion in *Comprehensive Drug Testing* noted, it is arduous and time-consuming to find digital evidence on a computer without a "thorough understanding of the

filing and classifications used,” which government officials do not possess when sifting through unfamiliar documents, classified or stored in deceptive or misleading ways, on computers with state-of-the-art software. 579 F.3d at 1004. Furthermore, “[t]here is no way to be sure exactly what an electronic file contains without somehow examining its contents . . . . By necessity, government efforts to locate particular files will require examining a great many other files to exclude the possibility that the sought-after data are concealed there.” *Id.* Thus, courts should “accept the reality that . . . over-seizing is an inherent part of the electronic search process . . . [and] will be far more common than in the days of paper records.” *Id.* at 1006.

Ninth Circuit cases decided prior to *Comprehensive Drug Testing*, as well as cases in other circuits, have identified this reality in cases concerning searches and seizures of digital evidence. *See, e.g., Adjani*, 452 F.3d at 1150 (“[W]ere we to limit the warrant to such a specific search protocol, much evidence could escape discovery simply because of [the defendant’s] labeling of the files documenting [his] criminal activity.”); *Giberson*, 527 F.3d at 890 (“There was no reasonable way to sort relevant and irrelevant graphics files because the [criminal files] were innocuously labeled.”); *Hill*, 459 F.3d at 978 (“There is no way to know what is in a file without examining its contents, just as there is no way of separating talcum from cocaine except by testing it.”); *Raney*, 342 F.3d 551; *Guest v. Leis*, 255 F.3d 325, 335 (6th Cir. 2001) (“Defendants may legitimately have checked to see that the contents of the directories corresponded to the labels placed on the directories. Suspects would otherwise be able to shield evidence from a search simply by ‘misfiling’ it in a [different] directory . . . .”); *Carey*, 172 F.3d 1268; *United States v. Riley*, 906 F.2d 841, 845 (2d Cir. 1990) (“[F]ew people keep documents of their criminal transactions in a folder marked ‘[crime] record.’”).

Likewise, this Court has recognized that “[i]n searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized. . . . [R]esponsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy.” *Andersen*, 427 U.S. at 482 n.11. Because papers located in containers are analogous to files in computers, the statement made by this Court in *Andersen* applies with equal force in the context of digital evidence. *See Giberson*, 527 F.3d at 887–88; *see also* Thomas K. Clancy, *The Fourth Amendment of Computer Searches and Seizures: A Perspective and a Primer*, 75 MISS. L. J. 193, (2005) (discussing several cases in which courts have analogized the search and seizure of digital evidence to the search and seizure of paper files, and therefore refused to adopt a special rule to apply to cases involving evidence stored on computers; and concluding that no special rule should be applied). Although the court in *Carey* concluded that “[r]elying on analogies [between computers and] closed containers or file cabinets may lead courts to ‘oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of modern computer storage,’” the extrapolation is suitable for the limited purpose of applying this Court’s statement in *Andersen* to this case. 172 F.3d at 1275 (citing Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 104 (1994)). This is not to say that digital evidence is in all respects akin to tangible evidence. Rather, in some searches, the items that the government seizes will far outnumber the items that the government has no probable cause to seize because the government has probable cause and because there is no other legitimate, unobtrusive way for the government to obtain the evidence.

This Court has held that “[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.” *Kyllo v. United States*, 533 U.S. 27, 33–34 (2001). Although technology may be changing our notions of privacy, it should not change our test for determining what constitutes a reasonably particular warrant. The framework established by this Court and refined by federal circuit and district courts has resulted in the appropriate balance for determining whether a search warrant is sufficiently particular in the past, and will continue to do so into the Twenty-First Century. Although a magistrate, acting sua sponte, should be allowed to impose heightened requirements or a meticulous search protocol for government officials to follow in executing a search warrant, and although it may be unreasonable in some circumstances for a magistrate not to impose such requirements or such a protocol, it would be unwise for this Court to impose those requirements on magistrates in every case concerning digital evidence.

Indeed, as the Ninth Circuit recognized in *Hill*, “judicial decisions regarding the application of the Fourth Amendment to computer-related searches may be of limited longevity. Technology is rapidly evolving and the concept of what is reasonable for Fourth Amendment purposes will likewise have to evolve.” 459 F.3d at 979. In light of this rapid change, the rules set forth by the Ninth and Fourteenth Circuits may make sense in some cases, but are impractical in others. This Court should reject the Ninth and Fourteenth Circuit’s invitation to create five bright-line requirements, and consider that: “the supposedly ‘bright-line rule’ the Court has created in response to its concerns about future technological advances . . . is unnecessary, unwise, and inconsistent with the Fourth Amendment. . . . It would be far wiser to give legislators an unimpeded opportunity to grapple with these emerging issues rather than to

shackle them with prematurely devised constitutional constraints.”). *Kyllo*, 533 U.S. at 41, 51 (Stevens, J., dissenting).

The constantly evolving, unpredictable nature of technology vitiates against the formulaic, “check-the-box” rule adopted in *StarTests* and *Comprehensive Drug Testing*, and compels the conclusion that courts should continue to adjudicate each case based on its facts to determine whether a search warrant for digital evidence is reasonable and valid. It is not the government’s position that magistrates should be permitted to issue sweepingly broad warrants in every case involving digital evidence, as *StarTests* and the CFL have suggested. Rather, if an unobtrusive on-site search of evidence promises to be impracticable in light of the circumstances, the magistrate should be allowed to issue a warrant providing for the seizure of that evidence as long as the seizure is objectively reasonable to further the government’s legitimate investigatory function. Where the government has probable cause to search for digital evidence, but does not know where the evidence is stored, it must peruse through a greater amount of data than is typical in usual search and seizure contexts to be able to fulfill its investigatory function. This unfortunate consequence of technology is particularly acute in the context of cases involving child pornography and fraud. *See, e.g., United States v. Alexander*, 574 F.3d 484 (8th Cir. 2009). Despite the difficulties of identifying the location of digital evidence, this Court should not jettison traditional Fourth Amendment jurisprudence, which embraces the plain view doctrine and cautions against bright-line rules in favor of the arbitrary and unprecedented test created by the Ninth and Fourteenth Circuits.

**C. The Requirements Enumerated by the Ninth and Fourteenth Circuits Are Unsuitable for Every Search and Seizure Case Involving Digital Evidence.**

Though appropriate in some cases, the five “guidelines” which *StarTests* and *Comprehensive Drug Testing* require magistrates to satisfy before issuing a warrant in a digital

evidence case are unsuitable for every case involving digital evidence search warrants. The requirements pose great difficulties for the government, are equally difficult for magistrates to enforce, and are overbroad because they render invalid some constitutionally sound warrants. The government has specific concerns with respect to each of the individual requirements.

The first requirement is that the magistrate must take measures to ensure that the government “waives reliance upon the plain view doctrine.” *StarTests II*, at \*17. The Fourteenth Circuit erred when it followed *Comprehensive Drug Testing* by adopting this requirement. Indeed, this requirement is the most controversial of the five, and therefore is discussed in a separate section below.

The second requirement is that “[s]egregation and redaction of the computer evidence must be either done by specialized personnel or an independent third party.” *Id.* Furthermore, if the segregation and redaction are performed by government personnel, the personnel must not disclose any information other than that specified in the warrant. *Id.* This requirement is imposed by *StarTests II* and *Comprehensive Drug Testing* without citing a single authority explaining why it is appropriate to do so in *every* for every case involving a search warrant for digital evidence. In some cases, as the government has conceded, it may be appropriate to have specialized personnel or independent third parties separate the wheat—the evidence for which the government has probable cause to search and which is contained within the ambit of the search warrant—from the chaff—everything else that the government has no right to possess. Nevertheless, to require this in every case is unnecessary. For example, this procedure would be unnecessary in a case where the government is investigating an individual case of tax fraud and has probable cause to search the individual’s personal computer. The personal computer contains no more or less information than tangible files which a government would be able to

search in any other context. In addition, as the dissent of *Comprehensive Drug Testing* alluded to, there are “practical, cost-related concerns” raised by this requirement:

To comply, an agency would have to expand its personnel, likely at a significant cost . . . . The alternative would be to use an independent third party consultant, which no doubt carries its own significant expenses. Both of these options would force law enforcement agencies to incur great expense, perhaps a crushing expense for smaller police departments that already face tremendous budget pressures.

579 F.3d at 1013 (Callahan, J., concurring in part and dissenting in part). In light of these practical considerations, as well as the lack of precedent to support this requirement, the second requirement should not be required in all digital evidence cases.

The third requirement is that, “[w]arrants must disclose the actual risks of destruction or concealment of information, as well as prior efforts to seize that information in other courts.” *Id.* This second part of this requirement makes sense, but the disclosure of actual risks of destruction or concealment does not. This requirement prevents the government from describing the difficulties of particularly identifying the precise location of digital evidence as a justification for a broad search warrant. But in order to explain to a magistrate the context under which it is applying for a search warrant, it must outline these difficulties so that the magistrate understands the case. In certain cases, these difficulties and the factual context in which they apply are the only thing the government can identify before actually conducting a search. As the dissent below suggested, “[the government] may never be able to specifically state what it is looking for in any particular search, or precisely how it will find it. Often these decisions cannot be made until a computer technician . . . analyzes the system.” *StarTests II*, at \*18 (Oneida, J., dissenting). Requiring the government to point to actual risks would require the government to engage in unnecessary speculation which duplicates the work that an affidavit can accomplish, as

the Ninth Circuit outlined in *Hill*. 459 F.3d at 975–77. This requirement should therefore be rejected.

Fourth, the government’s method for searching must be intended to discover only “information for which it has probable cause, and only that information may be examined by non-computer personnel agents.” *Id.* In light of the problems with the second requirement identified above, this requirement should also be discarded.

The fifth and final requirement imposed by the circuit courts is that, “[t]he government must destroy, or . . . return non-responsive data, at all times keeping the court informed of its progress.” *Id.* This is perhaps the only requirement that the government concedes should apply in almost all cases. Indeed, the government should not be given the windfall of being allowed to keep more than that for which it has probable cause to seize. To make this a requirement, however, is duplicative because magistrates must abide by this rule in any event. Indeed, in this case Magistrate Judge Leon ordered that the government “retain[] the information authorized by the warrant and designat[e] the remainder for return.” *StarTests I*, at 2. And because it is the only requirement left after the other four are discarded, it should not stand alone as its own “requirement”.

The government challenges the rigid five-prong analysis of the Ninth and Fourteenth Circuits because it imposes undue burdens on the government in every situation involving digital evidence. Instead of the Ninth and Fourteenth Circuits’ approach, magistrates should be permitted to issue search warrants in the context of digital evidence in the same way as with other evidence: by determining what is reasonable under the circumstances, and outlining a warrant which proscribes the seizure of evidence for which the government does not have probable cause. Although the context of digital evidence requires magistrates to “give exacting

scrutiny to the scope of the search, so to ensure the search is as narrowly tailored as possible to the goal of seizing evidence specifically described in a warrant,” bright-line requirements should not be imposed. *CDT II*, 579 F.3d at 1018 (Bea, J., concurring in part and dissenting in part). The requirements do not strike the appropriate balance “between the government’s legitimate interest in law enforcement and the people’s right to privacy and property,” the majority’s major concern in *StarTests* and *Comprehensive Drug Testing*. *CDT II*, 579 F.3d at 994.

The government recognizes that magistrates must play an active, deliberative role to protect individuals’ privacy, and does not advocate that broad warrants are appropriate in all cases. In cases where the digital evidence is located among several different computers and different files and is deceptively hidden, however, such a search warrant is necessary, so long as it is subjected to procedural safeguards tailored to the facts of the case. The rule adopted by the Ninth and Fourteenth Circuits is capricious and unprecedented, and makes it possible for the next generation of digital vigilantes and child pornography peddlers to escape the grasp of the government. This Court should thus reverse the decision of the Fourteenth Circuit, reject the rule embraced by *StarTests II*, and remand the case for further proceedings; it was reasonably necessary under the circumstances for Magistrate Judge Leon to issue a broad warrant under the facts of this case, and the magistrate imposed adequate procedural safeguards to protect the privacy rights of all individuals concerned.

**III. WHEN PERFORMING DIGITAL SEARCHES, THE GOVERNMENT MAY RELY ON THE “PLAIN VIEW” EXCEPTION TO THE PARTICULARITY REQUIREMENT BECAUSE THE EXCEPTION IS FIRMLY EMBEDDED IN THIS COURT’S BODY OF PRECEDENT AND FINDS SUPPORT IN THE FUNDAMENTAL PRINCIPLES OF THE FOURTH AMENDMENT.**

By forcing the government to forswear the plain view doctrine, the lower court severely impedes the government’s legitimate ability to search and seize electronic information. The

lower court abandons the fact-intensive analysis applied by the majority of circuits, instead requiring bright-line procedural safeguards that reach far beyond constitutional standards. Such a blanket denial of the application of the plain view doctrine is an extreme and overly expansive remedy that creates risks far graver than the benefits it seeks to instill. Consequently, this Court should reverse the decision of the Fourteenth Circuit, thereby rejecting the restrictive standards that would require the government to waive its reliance upon the plain view doctrine.

In support of this argument, this Court held in its seminal decision on the matter that, “it is well established that under certain circumstances the police may seize evidence in plain view without a warrant.” *Coolidge*, 403 U.S. at 465. In subsequent decisions, this Court went on to elaborate upon *Coolidge* and articulated three conditions that must be met for the plain view exception to be applicable. *Horton*, 496 U.S. at 136–37; *see also Arizona v. Hicks*, 480 U.S. 321, 326–27 (1987). Based upon the instant facts, it is clear that all three essential predicates have been met.

**A. The Officers Were Lawfully Present in the Place Where the Evidence Was in Plain View.**

First, this Court held as a threshold issue that the plain view exception would only be valid in cases in which “the officer did not violate the Fourth Amendment in arriving at the place from which the evidence could be plainly viewed.” *Horton*, 496 U.S. at 136. Absent exigent circumstances, this requirement is typically met when the search is supported by a valid warrant. *Coolidge*, 403 U.S. at 465. While the facial validity of the warrant has already been well established by earlier discussion, a cursory reference to the expansive case law on the issue is valuable and enlightening.

Recognizing the difficulties inherent to electronic media and information searches, the circuits have held that the “particularity” requirement may be less exacting when applied to

digital evidence cases. *See Hill*, 459 F.3d at 973–75; *Wong*, 334 F.3d at 836; *Carey*, 172 F.3d at 1272–73; *United States v. Upham*, 168 F.3d 532, 534–36 (1st Cir. 1999) (holding warrant listing materials to be seized as “any and all computer software and hardware, . . . computer disks, disk drives, [and] any and all visual depictions, in any format or media” sufficiently particular). As the *Upham* court explained, “a sufficient chance of finding some needles in the computer haystack was established by the probable cause showing in the warrant application” therefore, the warrant was not facially overbroad. *Id.* at 535. As is clear on the record, the instant case involves an analogous set of facts where a warrant asked to seize “all [StarTests related] computer records, files, and equipment” because the massive quantity of data involved, time it would take to perform an on-site search, risk of mislabeled files, and level of analysis required would either preclude a limited on-site search or render it impractical. *StarTests I*, at \*1–2. Conversely, had the circumstances lent themselves to an on-site inspection of the files, or if there were practical means of separating the files that were connected with a crime from those that were not, the court may have held that the seizure of *all* computer equipment was unjustified and unlawful, however, those were not the facts here. Rather, due to the complexity of StarTests electronic storage systems, and use of “computer hopping” procedures, a search limited solely to the records named in the warrant was a practical impossibility. *StarTests I*, at \*1–2; *StarTests II*, at \*8–9. Accordingly, the government agents were lawfully present where the evidence was in plain view because their presence there was supported by a valid search warrant.

**B. The Incriminating Nature of Information in Plain View Was Immediately Apparent.**

The second element required for the application of the plain view exception is also met because the incriminating nature of the material was immediately apparent. *Horton*, 496 U.S. at 136. As the district court correctly noted, the instant case is distinguishable from the body of

cases in which the courts found this immediately apparent quality lacking. *StarTests II*, at \*6. In *Carey*, for example, the scope of the search warrant was circumscribed to evidence pertaining to drug trafficking, specifically computer files containing “names, telephone numbers, ledgers, receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances.” *Carey*, 172 F.3d at 1272–73. By the searching officer’s own admission, he extended the search beyond the scope of the warrant when he began to open image files which he believed would contain child pornography. *Id.* at 1273. After finding the first erotic image the officer no longer believed he would find material related to drugs in the image files, rather, he had commenced a new search for material of a completely crime and nature. *Id.* Unlike the instant case, the officer in *Carey* did not merely stumble upon incriminating files while operating within the scope of his initial search. *StarTests I*, at \*8. Instead, the officer had “abandoned” his original search for evidence of drug dealing and had commenced a new search without judicial authority. *Carey*, 172 F.3d at 1273.

The present facts are more akin to those cases in which the courts find the incriminating character of the evidence immediately apparent and the plain view doctrine applicable. *See Wong*, 334 F.3d 831; *Giberson*, 527 F.3d 882; *United States v. Crouch*, 648 F.2d 932 (4th Cir. 1981). In *Wong*, computer forensic specialists obtained a valid warrant and searched a computer for graphics files relating to a murder. *Wong*, 334 F.3d at 834–35. During the course of the search the agent discovered child pornography, but he merely noted the file locations and continued with his original search for files pertaining to the murder. *Id.* at 835. The incriminating character of the images the agent stumbled upon was immediately apparent because many of the images depicted children as young as age three engaging in sexual acts. *Id.*

Similarly, in *Crouch* the evidence in dispute was discovered inadvertently during the execution of a search warrant for materials “used in the illegal manufacture of methamphetamines.” *Crouch*, 648 F.2d at 933. During the search the agents discovered a number of letters located in a desk drawer discussing the manufacture of methamphetamine. *Id.* While there was nothing incriminating about the envelopes, the court rightly held that the incriminating character of the letters was immediately apparent when the writing was exposed to view when the open envelopes were searched for chemicals and paraphernalia named in the warrant. *Id.* As with incriminating text in *Crouch*, the incriminating character of the test results was immediately apparent to the searching agents because the patient records clearly evinced dealings in illicit drugs. *StarTests II*, at \*8. Given these facts, it is well established that the incriminating character of the material was immediately apparent to the searching agents.

**C. The Government Had a Lawful Right of Access to the Records Discovered in Plain View.**

Given that the officers were lawfully present where the evidence was in plain view, and the material’s incriminating character was immediate apparent, the only remaining element the plain view exception requires is that the government had to have a “right of access” to the contested material. *Wong*, 334 F.3d at 838. Even where the government was acting under a valid search warrant, Plaintiffs argue that the FBI did not have a “right of access” to *that* information. *StarTests I*, at \*5. This argument is as convenient as it is flawed.

First, it is easy to imagine how criminals could use a misapplied “right of access” theory to insulate themselves from prosecution. For example, in every instance where the government stumbles upon incriminating evidence outside the scope of the initial warrant the defendant can protest and attempt to impute dastardly motives to the government. Such a rule would run contrary to the public interest, therefore, a majority of circuits apply a fact-intensive analysis that

only suppresses plain view evidence when it is located during a search that ventures beyond the scope of the supporting warrant. *See Carey*, at 1271–73. Respondents seek to turn what is essentially a constitutional shield into a sword that would deal a heavy blow to lawful searches and the interests they serve. Accordingly, this Court should follow the holding in *Giberson*, which recognized that government agents had a “right of access” so long as they merely stumbled across the evidence while continuing to search for evidence particular named in the warrant. *See Giberson*, 527 F.3d 890.

**D. In the Instant Case, the Application of the Plain View Doctrine is Wholly Consistent with the Constitutional Protections Served by the Fourth Amendment’s Warrant Requirements.**

Addressing the issue of constitutional concerns raised by the “plain view” doctrine, this Court reasoned that “the minor peril to Fourth Amendment protections” was justified and permitted in light of the “major gain in effective law enforcement.” *Id.* at 467. As this Court explained, the two fundamental evils the Fourth Amendment seeks to protect against are searches not based on probable cause or unparticular, general warrants that would permit the government to explore or rummage through a person’s belongs until something incriminating comes to light. *See id.* The plain view doctrine is not in conflict with either of these fundamental objectives.

The first constitutional protection articulated in *Coolidge* is met when police officers “had a prior justification for an intrusion,” that is, probable cause supporting a warrant, or “an exception [to the warrant requirement] such as ‘hot pursuit’ or search incident to a lawful arrest.” *Id.* at 466, 467. Under the instant facts, it is readily apparent that this first objective is met because the FBI assembled and presented a case for probable cause against five CFL players in a supporting affidavit. *StarTests II*, at \*8. Since the initial intrusion was justified by a warrant

based on probable cause, it cannot be said to violate the Fourth Amendment. *See Coolidge*, 403 U.S. at 467; U.S. CONST. amend. IV.

On the second point, the seizure in the instant case was wholly consistent with the Fourth Amendment because it occurred as the result of a search executed entirely within the confines of what was reasonably necessary to locate the materials particularized in the warrant. The five individual drug test records named in the warrant were stored in a database alongside a myriad of other records. *StarTests I*, at \*1. The records were not easily distinguishable, and indeed this Court has long recognized that when searching records such as personal papers, “it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized.” *Andresen*, 427 U.S. at 482 n. 11. In this case the scope of the search never extended beyond where one might reasonably expect to find records for the five CFL players named in the warrant. *StarTests II*, at \*8–9. Rather, the incriminating test results were located intermingled with the records and materials sought in the warrant and their discovery occurred during the normal and lawful course of the initial search. *StarTests I*, at \*2. The seizure of materials that come into plain view during the course of such a search “does not convert the search into a general or exploratory one.” *Coolidge*, 403 U.S. at 467. Accordingly, when a valid warrant to search for one item is exercised, as was the case here, this Court sees no need to “immunize [a] second item from seizure if it is found during a lawful search for the first.” *Horton*, 496 U.S. at 139.

## **CONCLUSION**

For the foregoing reasons, the decision of the Fourteenth Circuit should be reversed, the requirements established by the Ninth and Fourteenth Circuits should be rejected, and the case should be remanded.

