

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

RESPONDENTS.

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

BRIEF FOR PETITIONER

**TEAM 5
COUNSEL FOR PETITIONER**

QUESTIONS PRESENTED

(I) Whether a professional sports league has individual or organizational standing to move for the return of property under Federal Rule of Criminal Procedure 41(g) where the property belongs to a third party, is unrelated to the league's official business, and was lawfully seized from that third party's premises?

(II) Whether the plain view exception to the Fourth Amendment's warrant requirement applies to digital searches where law enforcement agents who remain on a narrow search path prescribed by a valid search warrant would otherwise be forced to ignore evidence of serious criminal activity?

(III) Whether federal magistrates may continue to issue warrants authorizing the seizure of computer equipment and files for subsequent offsite review without placing limits on the execution of digital searches, as per the unprecedented guidelines announced by the Fourteenth Circuit?

TABLE OF CONTENTS

QUESTIONS PRESENTED..... i

TABLE OF CONTENTS..... ii

TABLE OF AUTHORITIES v

STATEMENT OF THE CASE..... 1

OPINIONS BELOW..... 4

SUMMARY OF ARGUMENT 5

ARGUMENT..... 6

I. THE CFL LACKS STANDING TO MOVE FOR THE RETURN OF STARTESTS’S PROPERTY..... 6

 A. The CFL Lacks Standing To Sue On Its Members’ Behalf..... 7

 1. No individual CFL member would have standing to bring this claim..... 7

 a. No individual CFL member has suffered an injury-in-fact. 8

 b. No individual CFL member has suffered an injury traceable to the government’s actions and no individual member could receive suitable redress. 9

 2. The CFL has failed to establish that the relief sought is germane to its organizational purpose..... 9

 3. The CFL has failed to establish that participation of its individual members would be unnecessary in this action. 10

 B. The CFL Lacks Standing To Bring This Claim On Its Own Behalf..... 10

 1. The CFL is not a “person aggrieved” under Rule 41(g). 11

 2. The CFL has failed to allege a valid property interest in StarTests’s records. 11

 3. The CFL has failed to allege a reasonable expectation of privacy in StarTests’s records. 11

 C. Returning The Evidence To The CFL Through a 41(g) Motion Wwould Be Unreasonable..... 12

 1. The agents did not callously disregard the CFL’s rights. 12

 2. The CFL has failed to establish an interest in and need for the return of the seized evidence. 13

 3. The CFL has failed to show that it would suffer an irreparable injury..... 13

 4. Alternate remedies at law exist for the CFL. 14

II. THE GOVERNMENT MAY RELY ON THE PLAIN VIEW EXCEPTION TO THE FOURTH AMENDMENT’S WARRANT REQUIREMENT IN DIGITAL SEARCHES. 14

 A. The Plain View Exception Applies To The Search Of StarTests’s Digital Files. 15

1.	StarTests’s digital data warrants no similar treatment as that afforded to physical data.....	15
a.	The digital evidence seized from StarTests is analogous to physical evidence found in plain view.....	16
b.	StarTests’s digital files require no more heightened fourth amendment protection than physical files.	17
c.	Applying the plain view exception to StarTests’s digital files would not condone law enforcement misconduct.	18
2.	Preventing the FBI from relying on the plain view exception would result in unacceptable social costs.	18
a.	Forswearing the plain view doctrine would force the FBI to willfully ignore evidence of serious criminal drug activity.	19
b.	Forswearing the plain view doctrine would unnecessarily impede the FBI’s investigation of known drug use amongst CFL players.....	20
3.	The jurisprudence of this Court firmly supports retaining the plain view exception in the digital context.....	20
a.	Current safeguards sufficiently protect StarTests from any potential government abuse of the plain view exception.	21
b.	Wholesale rejection of the plain view exception in the digital context is unwise and extreme.....	21
B.	The evidence kept by the government was validly seized because the search and seizure pass the plain view test.	22
1.	The government was lawfully present on StarTests’s computers.....	23
2.	The government had a lawful right of access to the evidence seized from StarTests. .	23
a.	The FBI’s warrant granted access to the database containing the contested evidence.	23
b.	The government’s warrant was not overbroad.....	24
i.	The government’s warrant satisfied the particularity requirement.....	24
ii.	A neutral and detached magistrate judge approved the government’s warrant.	25
c.	The FBI did not deviate from its warranted search path.....	25
3.	The government immediately discerned the incriminating character of the drug-test results.	26
III. FEDERAL MAGISTRATES MAY CONTINUE TO ISSUE WARRANTS FOR SEIZURE OF COMPUTER EQUIPMENT AND FILES FOR LATER OFFSITE REVIEW AND WARRANT ISSUANCE SHOULD NOT BE CONDITIONED ON COMPLIANCE WITH THE DIGITAL SEARCH GUIDELINES ANNOUNCED BY THE FOURTEENTH CIRCUIT.		
A.	Magistrates May Continue To Issue Warrants Authorizing Seizure Of Computer Equipment And Files For Later Sorting.....	28

1. Warrants routinely authorize seizure of computer files and equipment for later sorting because it is the most feasible way to search for digital evidence.....	28
2. Congress and the majority of circuits permit warrants to authorize seizure of computer equipment and files for later offsite review.	30
B. The digital search guidelines announced by the Fourteenth Circuit place unnecessary restrictions on search warrant execution and are unworkable.	31
1. The Fourteenth Circuit’s digital search guidelines do not heighten warrant particularity but rather place unnecessary limitations on the manner of search execution.	31
2. The Fourteenth Circuit’s digital search guidelines are unworkable and place an undue burden on law enforcement.....	33
a. Law enforcement should not be required to waive reliance on the plain view doctrine.	33
b. Warrants should not impose barriers on communication between investigators and computer forensics specialists.....	34
c. Warrants should not be required to list the actual risks of data concealment and destruction.....	35
d. Warrants should not be required to include search protocols.	35
e. Procedures already exist to ensure that the government returns nonresponsive data.....	36
CONCLUSION.....	36
APPENDIX.....	A-1

TABLE OF AUTHORITIES

UNITED STATES SUPREME COURT CASES

Allen v. Wright, 468 U.S. 737 (1984)..... 7

Andresen v. Maryland, 427 U.S. 463 (1976)..... 17

Arizona v. Hicks, 480 U.S. 321 (1987)..... 26

City of Los Angeles v. Lyons, 461 U.S. 95 (1983) 8

Coolidge v. New Hampshire, 403 U.S. 443 (1971)..... 21

Dalia v. United States, 441 U.S. 238 (1979)..... 27, 31, 32

Friends of the Earth, Inc. v. Laidlaw Envtl. Servs., 528 U.S. 167 (2000) 7

Golden v. Zwickler, 394 U.S. 103 (1969)..... 8

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

Hunt v. Wash. State Apple Advertising Comm'n, 432 U.S. 333 (1977) 7, 9, 10

Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992) 7, 8, 9

Minnesota v. Dickerson, 508 U.S. 366 (1993) 26

Payne v. Tennessee, 501 U.S. 808 (1991) 21

PGA Tour Inc. v. Martin, 532 U.S. 661 (2001)..... 9

Rakas v. Illinois, 439 U.S. 128 (1978)..... 10, 11

Randall v. Sorrell, 548 U.S. 230 (2006) 21

Rogers v. Tennessee, 532 U.S. 451 (2001)..... 22

SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735 (1984)..... 11

United States v. Grubbs, 547 U.S. 90 (2006)..... 27, 31

United States v. Leon, 468 U.S. 897 (1984) 25

Warth v. Seldin, 422 U.S. 490 (1975)..... 6, 7

UNITED STATES COURT OF APPEALS CASES

<u>Angel-Torres v. United States</u> , 712 F.2d 717 (1st Cir. 1983).....	14
<u>Carrelli v. Ginsburg</u> , 956 F.2d 598 (3d Cir. 1992)	11
<u>CoStar Group, Inc. v. LoopNet, Inc.</u> , 373 F.3d 544 (4th Cir. 2004).....	30
<u>Ctr. for Law and Educ. v. Dept. of Educ.</u> , 396 F.3d 1152 (D.C. Cir. 2005).....	8
<u>Guest v. Leis</u> , 255 F.3d 325 (6th Cir. 2001)	16
<u>J.B. Manning Corp. v. United States</u> , 86 F.3d 926 (9th Cir. 1996)	12
<u>Jackson v. United States</u> , 526 F.3d 394 (8th Cir. 2008)	13
<u>Presbyterian Church (USA) v. United States</u> , 870 F.2d 518 (9th Cir. 1989).....	8
<u>Ramsden v. United States</u> , 2 F.3d 322 (9th Cir. 1993)	12
<u>Richey v. Smith</u> , 515 F.2d 1239 (5th Cir. 1975).....	12
<u>San Juan County v. United States</u> , 420 F.3d 1197 (10th Cir. 2005).....	7
<u>Search of 4801 Flyer Ave. v. Householder</u> , 879 F.2d 385 (8th Cir. 1989).....	12, 13
<u>Tel. & Data Sys., Inc. v. FCC</u> , 19 F.3d 42 (D.C. Cir. 1984).....	9
<u>United States v. \$260,242.00 In U.S. Currency</u> , 919 F.2d 686 (11th Cir. 1990).....	11
<u>United States v. Alexander</u> , 574 F.3d 484 (8th Cir. 2009)	19, 30
<u>United States v. Brooks</u> , 427 F.3d 1246 (10th Cir. 2005)	29
<u>United States v. Burgess</u> , 576 F.3d 1078 (10th Cir. 2009).....	35
<u>United States v. Campos</u> , 221 F.3d 1143 (10th Cir. 2000).....	31
<u>United States v. Carey</u> , 172 F.3d 1268 (10th Cir. 1999)	16, 19, 21, 25
<u>United States v. Cavazos</u> , 288 F.3d 706 (5th Cir. 2002)	15, 28
<u>United States v. Clymore</u> , 245 F.3d 1195 (10th Cir. 2001).....	13
<u>United States v. Comprehensive Drug Testing, Inc.</u> , 579 F.3d 989 (9th Cir. 2009).....	4, 17, 20, 27

<u>United States v. Giberson</u> , 527 F.3d 882 (9th Cir. 2008)	passim
<u>United States v. Hay</u> , 231 F.3d 630 (9th Cir. 2000)	29
<u>United States v. Heldt</u> , 8 F.2d 1238 (D.C. Cir. 1981).....	17
<u>United States v. Hill</u> , 459 F.3d 966 (9th Cir. 2006).....	19, 24, 31, 32
<u>United States v. Lopez</u> , 777 F.2d 543 (10th Cir. 1985).....	19, 34
<u>United States v. Otero</u> , 563 F.3d 1127 (10th Cir. 2009).....	24
<u>United States v. Peters</u> , 92 F.3d 768 (8th Cir. 1996)	26
<u>United States v. Raney</u> , 342 F.3d 551 (7th Cir. 2003).....	16
<u>United States v. Towne</u> , 997 F.3d 537 (9th Cir. 1993).....	24
<u>United States v. Upham</u> , 168 F.3d 532 (1st Cir. 1999).....	16, 28, 31
<u>United States v. Vanhorn</u> , 296 F.3d 713 (8th Cir. 2002)	13
<u>United States v. Wong</u> , 334 F.3d 831 (9th Cir. 2003)	16, 19, 23
<u>United States v. Wuagneux</u> , 683 F.2d 1343 (11th Cir. 1982).....	30

UNITED STATES DISTRICT COURT CASES

<u>United States v. Farlow</u> , No. CR-09-38-B-W, 2009 WL 4728690 (D. Me. Dec. 3, 2009) ...	18, 22, 34
<u>United States v. Graziano</u> , 558 F. Supp. 2d 304 (E.D.N.Y. 2008)	33, 36
<u>United States v. Hunter</u> , 13 F. Supp. 2d 574 (D. Vt. 1998).....	16
<u>United States v. Kim</u> , No. H-09-302, 2009 WL 5185389 (S.D. Tex. Dec. 23, 2009).....	21
<u>United States v. Lievertz</u> , 247 F. Supp. 2d 1052 (S.D. Ind. 2002)	16

MISCELLANEOUS AUTHORITIES

Brief for the United States, Comprehensive Drug Testing, Inc., (9th Cir. 2009) (No. CR Misc. 04-234 SI) 20, 34, 35

Fed. R. Crim. P. 41(e)(2)(B) advisory committee’s note..... 31

Federal Rule of Criminal Procedure 41(g)..... passim

Orin S. Kerr, Searches and Seizures in a Digital World, 119 HARV. L. REV. 531 (2005)..... 22

U.S. Department of Justice, Office of the Inspector General, “The Federal Bureau of Investigation’s Efforts to Combat Crimes Against Children Audit Report 09-08,” January 2009..... 34

UNITED STATES CONSTITUTIONAL PROVISIONS

U.S. CONST. amend IV..... 24, 26

UNITED STATES FEDERAL STATUTES

Fed. R. Crim. P. 41(g)..... 10, 36

STATEMENT OF THE CASE

Reports of rampant illegal steroid use by professional sports players have plagued the sports world for the past five years. Record (“R.”) 8. In 2005, the Colonial Football League (“CFL”) required all its franchise teams to test players for drug use to ensure compliance with federal law and league’s own professional standards. R. 1, 8. The CFL hired StarTests, Inc. (“StarTests”), an independent business specializing in drug-test administration, to test its players. R. 1. The CFL and StarTests repeatedly assured the players that the procedure was in place solely to determine whether five percent or more of them tested positive for illegal steroid use. R. 1. Unbeknownst to the players, however, the tests also screened for other controlled substances such as cocaine, marijuana, and hallucinogens. R. 2, 6. The CFL and StarTests further assured the players that the test results would remain confidential, and that StarTests would release to the CFL and the public only the percentage of players testing positive for steroids. R. 1. Once the CFL released this number, it would annually assess whether to continue drug-testing. R. 8. The CFL has required the drug-test every year since 2005. R. 8.

In 2008, as part of an investigation into illegal steroid use by professional athletes, the Federal Bureau of Investigation (“FBI”) discovered a network of illegal steroid distributors within the CFL. R. 7. Based on eyewitness reports and taped conversations gathered over several months, the FBI identified five CFL players in particular as major users and distributors of illegal steroids. R. 7. During its investigation, the FBI also learned that StarTests had screened these players for illegal drug use during the CFL’s mandatory drug-screening program. R. 8. To proceed with its case against the five players, the FBI applied for a search warrant to seize all materials from the StarTests facility related to the CFL drug-tests. R. 1.

The FBI supported its application for a search warrant with a detailed affidavit, requesting the ability to seize from StarTests's facility all computer equipment and files related to the drug-tests of CFL players. R. 1-2. The FBI explained in its supporting affidavit that it would need to seize StarTests's computer equipment and files for review at a later date because: (1) StarTests's files were substantial, and time would not permit an on-site search; (2) StarTests might have mislabeled files or labeled them deceptively to maintain confidentiality; and (3) de-encryption might require software not available at the StarTests facility. R. 2.

In the warrant, Magistrate Judge Leon authorized 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." R. 2. Judge Leon also restricted the warrant in a number of ways. R. 2. First, "law enforcement personnel trained in searching and seizing computer data" were to determine whether a computer needed to be seized. R. 2. Second, "appropriately trained personnel" would review the data on any computers or other equipment seized, retaining information authorized by the warrant and designating the rest for return. R. 2. Finally, the FBI could only search data "reasonably related to the investigation into the five named players' illegal steroid use." R. 2.

On the morning of November 1, 2008, the FBI executed the search warrant on the StarTests facility. R. 2. StarTests's employees told the FBI that most of the computers in the facility held at least one database containing information on the CFL. R. 2. The employees explained that the league was one of StarTests's largest clients and had generated four years worth of test results. R. 2. As the FBI suspected, StarTests stored the CFL data in a complex system meant to reduce the risk that an employee or third party might access it. R. 2. Specifically, StarTests used a "computer-hopping" procedure: one computer held a database of

the players' personal and health information, another held a database listing each player's assigned number, and a third held the actual test results with the subjects identified only by their assigned numbers. R. 2. StarTests repeated this procedure for every year in which it administered the tests. R. 2. Additionally, StarTests encrypted many of its databases or scattered them across various hard-drives. R. 2. Finding that StarTests's computer configuration was far more complex than originally anticipated and that the search for the five players' information could take at least a few days, the head FBI agent ordered the investigators, pursuant to the warrant, to seize or copy all of StarTests's computer data depending on the equipment's portability. R. 2, 8.

Computer forensics agents at the FBI bureau office eventually managed to decode StarTests's databases. R. 2. Afterwards, investigators began cross-referencing the five named players' identification numbers to the results database. R. 5. Upon opening the results database, a number of positive test results for unnamed players appeared on the screen alongside the names of controlled substances. R. 5-6. The database displayed positive test results for a variety of illegal substances, including steroids, cocaine, marijuana, and several hallucinogens. R. 2. Confronted with irrefutable evidence of criminal activity by additional CFL players, the FBI decided to expand the scope of its ongoing investigation to include illegal drug use and distribution for all of professional football. R. 2. Accordingly, the FBI determined that it needed to retain copies before returning any equipment. The FBI then returned all unneeded equipment to StarTests in compliance with the warrant. R. 2. Subsequently, StarTests and the CFL filed a motion under Federal Rule of Criminal Procedure 41(g) for the return of all seized property. R. 3.

OPINIONS BELOW

The United States District Court for the District of Wythe denied StarTests, Inc. (“StarTests”) and the Colonial Football League’s (“CFL”) motion for the return of computer equipment and files, filed pursuant to Federal Rule of Criminal Procedure 41(g). R. 1. The district court held that the CFL had organizational standing to sue on behalf of its members. R. 3. The district court further held that the government’s search and seizure of StarTests’s computer equipment was authorized by a valid warrant and was lawfully executed, and that the seizure of evidence not described in the warrant was lawful under the plain view exception. R. 6. Accordingly, the court denied the motion was.

StarTests and the CFL appealed the denial of the 41(g) motion to the United States Court of Appeals for the Fourteenth Circuit. The circuit court upheld the district court’s determination that the CFL had organizational standing to sue on behalf of its members, but reversed the decision that the evidence was lawfully seized for two reasons. First, the court refused to apply the plain view exception to the warrant requirement for digital searches. R. 1, 14. Second, the court held that the government’s search was invalid because its warrant was overbroad. The court premised its finding of overbreadth on the warrant’s failure to comport with five radical new restrictions on digital searches adopted by the Fourteenth Circuit in this case. R. 15. See also United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1006 (9th Cir. 2009). The circuit court ordered the government to return the seized property pursuant to the CFL’s 41(g) motion. R. 16.

This Court granted certiorari to consider the issues raised by the record.

SUMMARY OF ARGUMENT

I.

The CFL lacks standing to move for the return of StarTests's lawfully seized property. The CFL does not have standing to sue on behalf of its members because no individual member would have standing to seek the return of StarTests's equipment. Furthermore, the harm alleged by the CFL is not germane to its organizational purpose. Additionally, the CFL fails to establish standing to bring this claim on its own behalf because it is not a "person aggrieved" under Federal Rule 41(g). The CFL has failed to demonstrate a valid property or privacy interest in the evidence it seeks returned. Accordingly, this Court should remove the CFL as a party to this action.

II.

The FBI may rely on the plain view exception for StarTests's digital files primarily because digital files are indistinguishable from physical files for purposes of Fourth Amendment analysis. Abandoning the plain view exception would force investigators to willfully ignore evidence of serious crimes stored on computers. This Court should preserve the plain view doctrine for digital searches in order to uphold and reaffirm longstanding Fourth Amendment jurisprudence. This Court should also find that the government lawfully seized StarTests's digital files because the FBI's search satisfies the plain view test. The FBI satisfies all three prongs of the test because it was lawfully present on StarTests's computers during the search, had a lawful right of access to the drug-test results database, and immediately recognized the incriminating character of the evidence in plain view. Thus, the FBI permissibly seized the drug-test results from the StarTests facility.

III.

Federal magistrate judges have the authority to issue warrants authorizing seizure of computer equipment and files for later offsite review. Courts uphold such warrants because digital forensic analysis requires review of entire hard drives. On-site review of entire hard drives requires substantial time and expertise and is thus impracticable. Moreover, the Federal Rules of Criminal Procedure expressly authorize the seizure of computer equipment for offsite review. Therefore, this Court should hold that magistrates may issue warrants authorizing the government to seize computer files and equipment for offsite search.

This Court should also reject the radical restrictions that the Fourteenth Circuit imposed on digital searches. These restrictions fail to heighten warrant particularity. Rather, they impose unnecessary and burdensome limitations on the manner of search execution. Therefore, the Fourteenth Circuit erroneously held that the government's warrant was overbroad for failure to comply with these guidelines and the decision below should be reversed.

ARGUMENT

I. THE CFL LACKS STANDING TO MOVE FOR THE RETURN OF STARTESTS'S PROPERTY.

The CFL is not a proper party in this action. This Court has consistently held that a plaintiff in federal court must allege a personal injury and cannot sue on the basis of injury to third parties. Warth v. Seldin, 422 U.S. 490, 499 (1975). The standing requirement limits jurisdiction only to plaintiffs who can establish a valid case or controversy against a defendant. Id. at 498. The doctrine of organizational standing, which permits an organization to sue on behalf of the injuries of its members, is a singular exception to this principle. When, as here, a plaintiff-organization predicates its claim to standing not on injury to itself, but on injury to its individual members, its burden is "substantially more difficult" to establish. Allen v. Wright, 468

U.S. 737, 758 (1984); see also Lujan v. Defenders of Wildlife, 504 U.S. 555, 562 (1992); Warth, 422 U.S. at 505. The CFL fails to meet this burden here.

The CFL lacks standing to seek the return of the property seized from the StarTests facility for two reasons. First, the CFL may not assert this interest on its members' behalf. Second, the CFL may not bring a claim under Federal Rule of Criminal Procedure 41(g). Therefore, this Court should hold that the CFL lacks standing to seek the return of the property seized from StarTests's facility.

Questions of standing are reviewed de novo. San Juan County v. United States, 420 F.3d 1197, 1203 (10th Cir. 2005).

A. The CFL Lacks Standing To Sue On Its Members' Behalf.

The CFL fails to satisfy the requirements of organizational standing. An organization has standing to sue on behalf of its members only when: (1) its individual members would have standing to sue in their own right; (2) the interests at stake are germane to the organization's purpose; and (3) the participation of individual members would be unnecessary in the action. Hunt v. Wash. State Apple Advertising Comm'n, 432 U.S. 333, 343 (1977); see also Friends of the Earth, Inc. v. Laidlaw Env'tl. Servs., 528 U.S. 167, 181 (2000). The CFL does not satisfy any prong of this test and therefore lacks organizational standing to bring this action.

1. No individual CFL member would have standing to bring this claim.

The CFL fails the first prong of the Hunt test because no CFL member could satisfy the requirements for individual standing in this action. This Court established a three-prong test to determine individual standing in Lujan. 504 U.S. at 560-61. To satisfy the individual standing test, a plaintiff must show that: (1) it has suffered an injury-in-fact; (2) the injury is fairly traceable to the defendant; and (3) the injury is likely to be favorably redressed. Id.

No member has suffered an injury-in-fact stemming from the government's lawful search and seizure of StarTests's records and equipment. Additionally, no member has suffered an injury that is fairly traceable to the government's retention of criminal evidence seized from StarTests's facility. Finally, no member in this action could be redressed by a favorable decision. Accordingly, the CFL cannot sue on behalf of its members because no individual member would have standing to sue in this action.

a. No individual CFL member has suffered an injury-in-fact.

The harm alleged by the CFL is too approximate to establish an injury-in-fact. An injury-in-fact must be concrete and particularized. See Lujan, 504 U.S. at 560 n.1. An individual's subjective fear of a speculative future injury is insufficient to establish a concrete and particularized injury. See City of Los Angeles v. Lyons, 461 U.S. 95, 107 n.8 (1983) ("It is the reality of the threat of repeated injury that is relevant to the standing inquiry, not the plaintiff's subjective apprehensions") (emphasis in original). Even a heightened risk of injury is insufficient to show injury-in-fact. See, e.g., Ctr. for Law and Educ. v. Dept. of Educ., 396 F.3d 1152, 1161 (D.C. Cir. 2005). The CFL alleges an injury only to its organization. R. 9. Any injury to its individual members is speculative at best. R. 16. The CFL has no organizational standing because it fails to show that any individual member suffered a concrete, particular injury.

The CFL only alleges injuries that might occur at some indeterminate point in the future. If the injury has not already occurred, a plaintiff must demonstrate a credible threat of injury that is real and immediate to satisfy the injury-in-fact requirement. Golden v. Zwickler, 394 U.S. 103, 109 (1969); see, e.g., Presbyterian Church (USA) v. United States, 870 F.2d 518, 528-29 (9th Cir. 1989). The CFL alleges an injury to its organizational integrity, but makes no mention of a

specific, impending threat to its players. R. 9. The government merely decided to expand its underlying investigation of known illegal drug activity to professional football in general and not to any individual player. R. 2. Thus, the CFL lacks organizational standing because no individual member can demonstrate a credible threat of injury that is real and immediate.

b. No individual CFL member has suffered an injury traceable to the government's actions and no individual member could receive suitable redress.

The CFL fails to establish individual standing because no CFL member can assert an injury that is fairly traceable to the lawful search and seizure of StarTests's equipment. An injury is fairly traceable when the alleged offender is responsible for the injury at issue. Tel. & Data Sys., Inc. v. FCC, 19 F.3d 42, 47 (D.C. Cir. 1984); see also Lujan, 504 U.S. at 562.

StarTests and the CFL failed to uphold their repeated promises to test solely for illegal steroids and to keep test results anonymous. R. 1. If the CFL members have suffered a cognizable injury, CFL and StarTests are responsible, not the government. The only action traceable to the government is a lawful search and seizure. Because the government would not be the proper defendant in an individual member's action, no individual member could receive suitable redress. Therefore, the CFL fails to show that any of its members would have standing to sue in their own right for the return of the seized evidence.

2. The CFL has failed to establish that the relief sought is germane to its organizational purpose.

The CFL fails Hunt's second prong because this action is not germane to the CFL's organizational purpose. Organizational standing requires that the interest asserted in the litigation be germane to the purpose of the organization. Hunt, 432 U.S. at 343. The CFL's purpose, like that of other sports leagues, is to generate profit from the public's appetite for sports entertainment. Cf. PGA Tour Inc. v. Martin, 532 U.S. 661, 670 (2001) (viewing the

Professional Golfers' Association "as a commercial enterprise operating in the entertainment industry for the economic benefit of its members"). The CFL's purpose is not to protect the privacy interests of illegal drug users. Thus, the CFL lacks organizational standing because its interest in this action is unrelated to its organizational purpose.

3. The CFL has failed to establish that participation of its individual members would be unnecessary in this action.

Finally, the CFL lacks organizational standing in this action because the participation of individual CFL members would be necessary to bring this claim. An organization may not sue on behalf of its members if the relief requested requires the participation of individual members in the lawsuit. Hunt, 432 U.S. at 343. The crux of the CFL's claim is that it repeatedly assured players that their drug-tests would remain anonymous. R. 1. Adjudicating this claim would require each member to undergo a fact-intensive inquiry to verify the scope of the confidentiality guarantees. Therefore, the CFL lacks organizational standing because bringing this claim would require the individual participation of every allegedly injured player.

B. The CFL Lacks Standing To Bring This Claim On Its Own Behalf.

Even if the CFL could meet the requirements for organizational standing, it lacks standing to bring a 41(g) motion on its own behalf. Rule 41(g) provides that only a person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return. Fed. R. Crim. P. 41(g). The movant must also have a reasonable expectation of privacy in the location or the items searched. Rakas v. Illinois, 439 U.S. 128, 143 (1978). The CFL is not a "person aggrieved" by an unlawful search and seizure. The CFL also fails to establish either a property or a privacy interest in the evidence seized. Therefore, the CFL fails to meet the requirements for standing under Federal Rule of Criminal Procedure 41(g).

1. The CFL is not a “person aggrieved” under Rule 41(g).

The CFL lacks standing because it is not a person aggrieved by an unlawful search and seizure. A person aggrieved by an unlawful search and seizure is “one against whom the search is directed.” Rakas, 439 U.S. at 134-35 (holding that one who merely fears that evidence seized from a third party will be used against her is not a person aggrieved). Here, the FBI directed its search against StarTests. R. 1-2. The CFL merely speculates that the evidence seized from StarTests may damage its business. R. 10. Thus, the CFL lacks standing to seek return of the seized evidence because it is not an aggrieved person for the purposes of Rule 41(g).

2. The CFL has failed to allege a valid property interest in StarTests’s records.

The CFL also lacks standing because it cannot assert a property interest in the evidence seized from StarTests. To prevail on a 41(g) motion, a claimant must show a possessory interest in the property sought. United States v. \$260,242.00 In U.S. Currency, 919 F.2d 686, 687-88 (11th Cir. 1990). The CFL was never in possession of the records and equipment. It paid StarTests to render a service. R. 10. Accordingly, the CFL lacks 41(g) standing because it does not have a property interest in StarTests’s records and equipment.

3. The CFL has failed to allege a reasonable expectation of privacy in StarTests’s records.

The CFL cannot properly invoke a 41(g) motion because it had no reasonable expectation of privacy in the records seized. Defendants typically have no reasonable expectation of privacy in drug-tests or other records given to a third party, even when promised confidentiality. See Carrelli v. Ginsburg, 956 F.2d 598, 607 (3d Cir. 1992); see also SEC v. Jerry T. O’Brien, Inc., 467 U.S. 735, 743 (1984) (finding no expectation of privacy in financial records given to a third party, even under understanding of confidentiality). The situation here is no different: the CFL hired StarTests, a third party, to process and store drug-test results under an understanding of

confidentiality. R. 1, 8. The CFL has failed to demonstrate a reasonable expectation of privacy in the seized evidence and therefore lacks standing to sue for its return.

C. Returning The Evidence To The CFL Through a 41(g) Motion Would Be Unreasonable.

Even if the CFL could establish standing to bring a 41(g) motion, returning the evidence to the CFL would be unreasonable. The return of evidence pursuant to a 41(g) motion is an equitable remedy that must be “reasonable under all the circumstances.” J.B. Manning Corp. v. United States, 86 F.3d 926, 928 (9th Cir. 1996). The circuit courts have enumerated four factors in determining whether the return of evidence would be reasonable: (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 sought; (3) whether the movant would be irreparably injured by denying return of the property; and (4) whether the movant has an alternate remedy at law for the redress of his grievance. Ramsden v. United States, 2 F.3d 322, 324-25 (9th Cir. 1993) (citing Richey v. Smith, 515 F.2d 1239, 1243-44 (5th Cir. 1975)). An application of these factors to this case demonstrates that the CFL does not have standing to bring a 41(g) motion because the return of the copied evidence to the CFL would be unreasonable.

1. The agents did not callously disregard the CFL’s rights.

The government did not display a callous disregard for the CFL’s constitutional rights. Government agents do not callously disregard constitutional rights when they act in an objectively good faith manner and pursuant to a valid warrant. See Search of 4801 Flyer Ave. v. Householder, 879 F.2d 385, 388 (8th Cir. 1989). Here, the federal agents searched StarTests’s premises with a facially valid warrant. R. 1, 2. Furthermore, the agents adhered to the warrant’s restrictions regarding the use of computer forensics experts, believing that all evidence was

lawfully seized. R. 4. Thus, because the officers acted in good faith and in compliance with the warrant, returning the evidence would be unreasonable.

2. The CFL has failed to establish an interest in and need for the return of the seized evidence.

The CFL has not established a sufficient need for the StarTests records and equipment retained by law enforcement. To establish an interest in and need for the return of evidence, the movant must show lawful entitlement. See United States v. Clymore, 245 F.3d 1195, 1201 (10th Cir. 2001) (per curiam). This requirement is often satisfied by showing that the property was in the movant's possession when seized. See Jackson v. United States, 526 F.3d 394, 396 (8th Cir. 2008). Here, StarTests administered and possessed the drug-tests until the FBI's seizure. R. 2. The CFL asserts an interest in preserving its own integrity, but fails to demonstrate possessory interest in StarTests's records and equipment. R. 9. The CFL lacks an interest in and need for the evidence because it fails to establish lawful entitlement to the data, rendering its return unreasonable.

Moreover, the return of the evidence would be unreasonable because the government has a continued need for retaining the property as evidence. Courts should deny 41(g) motions if an ongoing government investigation requires retention of the property as evidence. United States v. Vanhorn, 296 F.3d 713, 719 (8th Cir. 2002). The FBI must retain the seized evidence for the purpose of its ongoing criminal investigation. R. 2. Therefore, returning the evidence documenting the players' criminal activity would be unreasonable.

3. The CFL has failed to show that it would suffer an irreparable injury.

The CFL cannot show that it would suffer irreparable harm if the FBI retains copies of the drug-tests. The threat of criminal prosecution or unsupported allegations of business disruption are insufficient to show irreparable harm. See, e.g., Search of 4801 Flyer Ave., 879

F.2d at 388-89. Here, the potential harm alleged is that CFL players could be removed from the field as a result of unspecified, future litigation. R. 16. This unsubstantiated fear of a business disruption is insufficient to show irreparable harm. Absent such a showing, return of the property would be unreasonable.

4. Alternate remedies at law exist for the CFL.

Even if the CFL could allege a legally cognizable claim, alternate remedies at law exist. Where a movant shows no immediate need for the return of seized property, alternate remedies such as filing a motion to suppress, or reapplying to the district court for return of property, exist to justify the denial of a 41(g) motion. Angel-Torres v. United States, 712 F.2d 717, 720 (1st Cir. 1983). Here, the CFL demonstrates no immediate need for the seized data and equipment. Therefore, because the CFL has other adequate remedies at law, return of the property under 41(g) would be unreasonable.

II. THE GOVERNMENT MAY RELY ON THE PLAIN VIEW EXCEPTION TO THE FOURTH AMENDMENT'S WARRANT REQUIREMENT IN DIGITAL SEARCHES.

This Court should find that the government may rely on the plain view exception in its search of StarTests's digital data. The plain view exception permits investigators to seize evidence of criminal activity that it encounters while executing a lawful search. Horton v. California, 496 U.S. 128, 136-37 (1990). The facts of this case implicate the precise reason why the plain view doctrine exists: the government found evidence of other serious crimes during the course of its lawful criminal investigation. Circuit courts have extended the plain view exception to the digital context. See, e.g., United States v. Giberson, 527 F.3d 882, 888 (9th Cir. 2008). The Fourteenth Circuit, instead, chose to follow a recent Ninth Circuit decision forbidding reliance on the doctrine in its entirety, and forcing the FBI to ignore evidence of criminal activity

that is in plain sight. This Court should reverse the Fourteenth Circuit’s decision and acknowledge the legality of the FBI’s search.

The government lawfully seized StarTests’s digital files because the FBI satisfied all three prongs of the plain view test. The government properly seizes evidence under the plain view test when its investigators: (1) are lawfully present in the place where the evidence can be plainly viewed; (2) have a lawful right of access to the evidence seized; and (3) find the incriminating character of the evidence to be “immediately apparent.” Horton, 496 U.S. at 136-37. The government complied with all three requirements of the plain view test, and thus lawfully seized the digital evidence from the StarTests facility.

Courts review findings of fact for clear error and conclusions of law de novo when determining whether a search violated the Fourth Amendment. See United States v. Cavazos, 288 F.3d 706, 709 (5th Cir. 2002).

A. The Plain View Exception Applies To The Search Of StarTests’s Digital Files.

The FBI may rely on the plain view exception for StarTests’s files. This Court should afford the same treatment to digital data as it does to physical data. Furthermore, the plain view doctrine is especially important here because police should not be asked to willfully ignore evidence of serious criminal activity in plain view. Finally, existing law endorses the plain view exception for digital searches. Therefore, this Court should apply the plain view exception to the FBI’s lawful search of StarTests’s digital files.

1. StarTests’s digital data warrants no similar treatment as that afforded to physical data.

This Court should treat StarTests’s digital data like any other legally seized evidence. StarTests’s computer records are analogous to its physical records. This Court should not afford these records any higher Fourth Amendment protection than StarTests’s physical files would

receive. Moreover, the search of digital files is no more susceptible to law enforcement misconduct than the search of non-digital files. Therefore, the plain view exception applies to StarTests's digital data in the same way that it would apply to its physical data.

a. The digital evidence seized from StarTests is analogous to physical evidence found in plain view.

The government may rely on the plain view exception for StarTests's digital files because the plain view exception applies to paper files. Courts routinely analogize searches of digital files to those of paper files. See Guest v. Leis, 255 F.3d 325, 334-35 (6th Cir. 2001); see, e.g., Giberson, 527 F.3d at 888; United States v. Wong, 334 F.3d 831, 838 (9th Cir. 2003); United States v. Raney, 342 F.3d 551, 559 (7th Cir. 2003); United States v. Upham, 168 F.3d 532, 536 (1st Cir. 1999); United States v. Carey, 172 F.3d 1268, 1272 (10th Cir. 1999). The FBI agents opened StarTests's digital file containing the test results for the five players named in the warrant and a plethora of drug-test results immediately appeared on the screen. R. 6. Had the FBI opened a paper file of the same information, it would have likewise encountered a plethora of positive test results. Courts treat searches of paper and digital files in the same way; therefore, the government may rely on the plain view exception for StarTests's digital files.

This Court should not jettison the plain view doctrine for StarTests's digital files because preserving plain view in the digital context maintains uniform application of the law. Distinguishing between digital and paper files would result in an inconsistent application of Fourth Amendment protection because there is no fundamental difference between the two. See United States v. Lievertz, 247 F. Supp. 2d 1052, 1063 (S.D. Ind. 2002); see also United States v. Hunter, 13 F. Supp. 2d 574, 584 (D. Vt. 1998) (finding "no justification for favoring those who are capable of storing their records on computer[s] over those who keep hard copies"). If StarTests had stored the drug-test results in paper files, the government could have relied on the

plain view exception. Thus, forswearing the plain view doctrine here would arbitrarily grant higher Fourth Amendment protection to StarTests's digital files.

b. StarTests's digital files require no more heightened fourth amendment protection than physical files.

The intermingling of players' test results in StarTests's database does not preclude the application of the plain view doctrine. Intermingled digital files require no more Fourth Amendment protection than intermingled paper files. See Giberson, 527 F.3d at 888-89 (finding the reasonableness requirement a sufficient safeguard for both digital and paper intermingled files); see also Andresen v. Maryland, 427 U.S. 463, 482 n.11 (1976) (finding that sorting through intermingled paper documents was necessary and appropriate). Here, upon lawfully opening the drug-test results file, agents encountered the five named players' test results commingled with those of other, unnamed players. R. 6. A similar file stored on paper would likely also contain commingled results. Thus, the plain view doctrine need not be forsworn in the plain view context due to the intermingling of StarTests's data.

The plain view doctrine is still applicable even though the FBI agents seized a large number of StarTests's files. The magnitude of a search and seizure is irrelevant provided it satisfies the reasonableness requirement. See United States v. Heldt, 8 F.2d 1238, 1254 (D.C. Cir. 1981) (admitting documents in plain view after determining that seizure of thousands of documents was reasonable under the circumstances); cf. Comprehensive Drug Testing, Inc., 579 F.3d at 1006 (acknowledging that the wholesale seizure for digital searches is often inevitable). Due to the fragmented and encrypted nature of StarTests's data, the FBI acted reasonably in seizing a large number of files. R. 2, 8. If StarTests had scattered and encoded its files in paper form, the agents would have likewise been reasonable in seizing a large number of those files.

Thus, the plain view doctrine should be applicable to the digital data seized from StarTests's facility because the search and seizure were reasonable.

c. Applying the plain view exception to StarTests's digital files would not condone law enforcement misconduct.

Imposing a unique set of restrictions on digital searches like this one is unreasonable because law enforcement misconduct is not especially prevalent in the digital search context. Law enforcement misconduct in digital searches is the exception, not the rule. United States v. Farlow, No. CR-09-38-B-W, 2009 WL 4728690, at *6 n.3 (D. Me. Dec. 3, 2009) (finding no evidence that police misconduct in digital searches compels such "onerous pre-issuance" restrictions as forswearing the plain view doctrine). The FBI remained within the parameters of their warrant in conducting their search and seizure. R. 2. They used appropriately trained personnel to carry out their search and focused their search on the five players name in the warrant. R. 5. Therefore, digital searches should not be unduly restricted by the elimination of plain view based on the false presumption that digital searches encourage police misconduct.

2. Preventing the FBI from relying on the plain view exception would result in unacceptable social costs.

Eliminating the plain view doctrine for digital searches would have grave consequences. First and foremost, forbidding the use of plain view for digital evidence seized from StarTests would force the FBI to ignore evidence of serious criminal drug activity. Second, jettisoning the doctrine would hamper the FBI's criminal investigation of drug use in the CFL and serve as a windfall to criminals. Finally, preserving the plain view doctrine in the digital context is particularly important because evidence of crimes is easily concealed on computers. Therefore, this Court should recognize the need for the plain view exception in the digital context.

a. Forswearing the plain view doctrine would force the FBI to willfully ignore evidence of serious criminal drug activity.

Forbidding the use of plain view for the digital evidence seized from StarTests would force the FBI to ignore evidence of the players' drug activity and other serious crimes. It is a long standing principle that law enforcement should not be required to willfully ignore evidence of criminal activity that is in plain view during a lawful search, even if it is outside the scope of the warrant. See United States v. Lopez, 777 F.2d 543, 547 (10th Cir. 1985); see, e.g., Wong, 334 F.3d at 838 (admitting evidence of child pornography found while performing a valid digital search for evidence of murder in image files); Giberson, 527 F.3d at 885 (admitting digital evidence of child pornography found while lawfully searching for evidence related to production of false I.D.s). Here, the FBI agents encountered evidence of criminal drug use during their lawful digital search. R. 6. It is the duty of the FBI, as federal investigators, to pursue and prosecute criminals. Thus, this Court abandoning the plain view doctrine for the evidence seized from StarTests would force the FBI to disregard their duties and willfully ignore evidence of serious criminal activity.

Preserving the plain view doctrine in the digital context is particularly important because evidence of serious crimes, such as the evidence of drug activity in StarTests's files and child pornography, is often stored digitally. The majority of criminal evidence uncovered through the plain view doctrine in digital searches is evidence of child pornography. See, e.g., United States v. Alexander, 574 F.3d 484, 491 (8th Cir. 2009); United States v. Hill, 459 F.3d 966 (9th Cir. 2006); Wong, 334 F.3d at 838; Carey, 172 F.3d at 1272. Eliminating the plain view doctrine would not only shield evidence of criminal drug activity but also evidence of child pornography and other serious crimes. Thus, the plain view doctrine is vital in the digital context as society

has a strong interest in prosecuting criminal drug activity and a moral imperative to expose child exploitation.

b. Forswearing the plain view doctrine would unnecessarily impede the FBI's investigation of known drug use amongst CFL players.

Jettisoning the plain view exception for StarTests's digital data would hamper criminal investigations and allow these and other criminals to go free. The recent Ninth Circuit decision eliminating plain view for digital searches has already tied the hands of federal law enforcement. Brief for the United States in Support of Rehearing en banc by the full court at 6, *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 1006 (9th Cir. 2009) (No. CR Misc. 04-234 SI); see also *Comprehensive Drug Testing, Inc.*, 579 F.3d at 1006. For example, federal investigators in the Ninth Circuit have begun asking state authorities to conduct digital searches to avoid CDT's heightened requirement. Brief for the United States at 6, *Comprehensive Drug Testing, Inc.*, (9th Cir. 2009) (No. CR Misc. 04-234 SI). Here, without the use of the plain view doctrine, the FBI's investigation into criminal drug activity would probably have been delayed or compromised. R. 7. Thus, forswearing the plain view doctrine for digital searches would likely interfere with ongoing and future federal investigations like this one.

3. The jurisprudence of this Court firmly supports retaining the plain view exception in the digital context.

The government's reliance on the plain view exception in the digital context comports with existing law. This Court has already issued a test to limit unreasonable applications of the plain view doctrine, which the circuits have consistently applied to digital and non-digital searches. Furthermore, rejecting the plain view doctrine in its entirety is a drastic measure, inconsistent with the traditional development of the common law. Therefore, this Court should

not change existing Fourth Amendment jurisprudence by abandoning the plain view doctrine for digital searches.

a. Current safeguards sufficiently protect StarTests from any potential government abuse of the plain view exception.

Eliminating the plain view exception is unnecessary because courts already have recourse to curtail potential abuses by law enforcement. This Court has already created a test to curb the application of the plain view doctrine. Horton, 496 U.S. at 136-37. For the last twenty years, lower courts have applied this test and suppressed unreasonably seized evidence in both the digital and non-digital contexts. See, e.g., Carey, 172 F.3d at 1276 (suppressing evidence of child pornography because search and seizure failed the plain view test); see also United States v. Kim, No. H-09-302, 2009 WL 5185389, at *18 (S.D. Tex. Dec. 23, 2009). If the Fourteenth Circuit found the search overbroad, it should have applied the plain view test to evaluate the admissibility of the evidence. R. 12. Therefore, this Court should reject the Fourteenth Circuit's decision to abandon the plain view exception because courts can and do exclude digital evidence by applying the current plain view test.

b. Wholesale rejection of the plain view exception in the digital context is unwise and extreme.

This Court should preserve plain view in the digital context because it is a well-established doctrine of Fourth Amendment jurisprudence. This Court should adhere to its own decisions and respect stare decisis. Randall v. Sorrell, 548 U.S. 230, 234 (2006). Courts should not depart from precedent, especially where the principle at issue has become settled over a long period and is widely accepted and applied. See Payne v. Tennessee, 501 U.S. 808, 827-28 (1991). The plain view exception has been universally adopted and consistently applied for almost forty years. See Coolidge v. New Hampshire, 403 U.S. 443 (1971). The government

believed that it could rely on the plain view exception during its digital search of StarTests's files, as it could in other circuits. R. 2, 9. Retaining plain view for digital searches maintains consistent application of Fourth Amendment jurisprudence and prevents unpredictable and inconsistent case holdings.

The Fourteenth Circuit's summary dismissal of the plain view exception for digital searches strays from the process by which Fourth Amendment jurisprudence develops. The foundation of our common law system is based upon the incremental and measured evolution of legal precedent. Rogers v. Tennessee, 532 U.S. 451, 452 (2001); see also Orin S. Kerr, Searches and Seizures in a Digital World, 119 HARV. L. REV. 531, 582-83 (2005) (calling the wholesale elimination of the plain view doctrine for digital searches "too severe"). Indeed, recent district court opinions have rejected the CDT decision because more traditional remedies should be tried first. See, e.g., Farlow, 2009 WL 4728690, at *6. Instead of imposing limitations on the plain view exception in the digital context, the Fourteenth Circuit eliminated the doctrine in its entirety. R. 17. This wholesale eradication of the plain view exception for digital searches runs contrary to the process by which legal doctrine is developed.

B. The evidence kept by the government was validly seized because the search and seizure pass the plain view test.

The FBI lawfully seized the contested evidence because its search satisfies the widely accepted plain view test. Evidence is lawfully seized under the plain view test if investigators: (1) are lawfully present in the place where the evidence can be plainly viewed; (2) have a lawful right of access to the evidence seized; and (3) find the incriminating character of the evidence to be "immediately apparent." Horton, 496 U.S. at 136-37. The government's search satisfies all three prongs of the plain view test. Thus, the FBI permissibly seized the drug-test results from the StarTests facility.

1. The government was lawfully present on StarTests’s computers.

The government satisfies the first prong of the plain view test because it was lawfully present on StarTest’s computers when it accessed drug-test information about the CFL players. Investigators are lawfully present when they are acting on a facially valid search warrant. Horton, 496 U.S. at 135-36; see also Wong, 334 F.3d at 838. The FBI agents acted upon a valid search warrant when they accessed the drug-test information at StarTests’s facility. R. 5. The government thus satisfies the first prong of the plain view test because the FBI agents were lawfully present.

2. The government had a lawful right of access to the evidence seized from StarTests.

The government had a lawful right of access to StarTests’s databases. The warrant permitted the FBI to search the databases containing the drug-test results. The warrant was also sufficiently narrow because it clearly stated the objects sought. During the search, the government did not deviate from its warranted search path. Therefore, the search was legal because the government had a lawful right of access to StarTests’s digital databases during the search.

a. The FBI’s warrant granted access to the database containing the contested evidence.

The FBI’s warrant gave the agents a lawful right of access to the particular StarTests databases in which they found the contested evidence. An investigator has a lawful right of access to databases that are likely to include items specified by the warrant. See Wong, 334 F.3d at 838 (accepting into evidence images of child pornography found while searching for image files, specified by the warrant, relating to a murder). The government’s search warrant permitted investigators to “search computer equipment, storage devices, and—where an on-site search

would be impracticable—seize either a copy of all data or the computer equipment itself.” R. 8. The government satisfies the second prong of the plain view test because the FBI agents had a lawful right of access to the particular database in which the drug-test results were found.

b. The government’s warrant was not overbroad.

The government’s warrant was appropriately tailored to the search of StarTests’s facility. The warrant was limited in scope and clearly stated the objects of the search. Additionally, a neutral and detached magistrate judge issued the warrant. For these reasons, the government’s warrant to search the StarTests facility was adequately narrow.

i. The government’s warrant satisfied the particularity requirement

The government’s warrant was not overbroad because it satisfied the particularity requirement. The Supreme Court imposes a “particularity” requirement on search warrants. U.S. CONST. amend. IV (“No warrants shall issue except [those] particularly describing the . . . things to be seized.”). To satisfy the particularity requirement, warrants must clearly state what is sought and be limited to the items for which probable cause has been shown. Hill, 459 F.3d at 973, citing United States v. Towne, 997 F.3d 537, 544 (9th Cir. 1993); see also United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009) (limiting warrants for computer searches to evidence of specific federal crimes). The warrant in this case clearly stated what was sought: “all computer records, files, and equipment” pertaining to the illegal drug use of five named players. R. 1-2. Further, there was probable cause to investigate these five players’ drug use and the warrant was limited to information reasonably related to that end. R. 1-2. Therefore, the government’s warrant was sufficiently particular.

ii. A neutral and detached magistrate judge approved the government's warrant.

This Court should defer to Magistrate Judge Leon's discretion in approving a warrant for the government that was reasonably tailored to the circumstances. Courts defer to issuing magistrates when deciding whether a warrant is sufficiently limited in scope so long as the magistrate is "neutral and detached." United States v. Leon, 468 U.S. 897, 914-16 (1984) (finding that magistrates have no reason to ignore or subvert the Fourth Amendment). Magistrate Judge Leon, determined to be neutral and detached, authorized the warrant with several restrictions in a fashion similar to others that have been upheld. R. 2, 4, 8. Therefore, this Court should defer to Magistrate Judge Leon's discretion in authorizing the warrant.

c. The FBI did not deviate from its warranted search path.

The FBI also had a lawful right of access to the drug-test information because the evidence was found while conducting the warranted search. Investigators have a lawful right of access to the information they find so long as they do not deviate from their warranted search path. See Giberson, 527 F.3d at 890 (admitting digital evidence of child pornography found while lawfully scanning thumbnail images for evidence related to production of false I.D.s); see also Carey, 172 F.3d at 1273 (finding no lawful right of access when officer began additional, unauthorized search for unrelated information). The government was searching for the five named players' test results by cross-referencing the identification numbers with the results file when it stumbled upon other positive test results and corresponding names. R. 5. The government never strayed from the search warrant; rather, it came across the test results of unnamed CFL players while conducting its lawful search. R. 5, 9. Thus, the government satisfies the second prong of the plain view test because the FBI did not deviate from its warranted search path.

3. The government immediately discerned the incriminating character of the drug-test results.

The government satisfies the third prong of the plain view test because the incriminating character of the drug-test results was immediately apparent to the investigating officers. The incriminating character of evidence is immediately apparent if investigators are able to instantly recognize it as evidence of a crime. See Minnesota v. Dickerson, 508 U.S. 366, 375 (1993); see also Arizona v. Hicks, 480 U.S. 321, 336 (1987) (stating that the incriminating character of evidence is immediately apparent when officers have probable cause to believe they have encountered evidence of crime). The FBI agents recognized criminal activity instantly when they observed positive test results alongside various illegal substances, such as “anabolic steroids” or “cocaine.” R. 6. Thus, the government satisfies the third prong of the plain view test because the incriminating character of the contested evidence was immediately apparent to the investigating officers.

III. FEDERAL MAGISTRATES MAY CONTINUE TO ISSUE WARRANTS FOR SEIZURE OF COMPUTER EQUIPMENT AND FILES FOR LATER OFFSITE REVIEW AND WARRANT ISSUANCE SHOULD NOT BE CONDITIONED ON COMPLIANCE WITH THE DIGITAL SEARCH GUIDELINES ANNOUNCED BY THE FOURTEENTH CIRCUIT.

This Court should find that magistrate judges may issue warrants authorizing seizure of computer equipment and files for offsite sorting, as they are currently permitted to do. The Fourth Amendment requires that warrants “particularly” describe the place to be searched and the items to be seized. U.S. CONST. amend IV. Courts adhere to a reasonableness standard looking at the type of targeted evidence and the totality of the circumstances to determine if a warrant meets the particularity requirement. United States v. Peters, 92 F.3d 768, 769-70 (8th Cir. 1996). The intricacies of digital forensic analysis make warrants authorizing seizure of computer equipment for offsite review a necessity. Moreover, Federal Rule of Criminal

Procedure 41(e)(2)(B) as well as circuits that have addressed the issue uniformly approve such warrants as reasonable. Therefore, warrants that permit the seizure of computer equipment and files for offsite review are reasonably particular and this Court should continue to allow magistrate judges to issue them.

Federal Rule of Criminal Procedure 41(e)(2)(B) as well as circuits that have addressed the issue uniformly approve of such warrants. Moreover, the intricacies of digital forensic analysis make warrants authorizing seizure of computer equipment for offsite review a necessity.

This Court should also hold that the government's warrant was not overbroad for its failure to comport with the new guidelines imposed on digital searches by the United States Court of Appeals for the Fourteenth Circuit. Under the guise of heightening warrant particularity in the digital search context, the Fourteenth Circuit adopted five guidelines restricting the manner in which digital searches may be executed. However, this Court has never held that the Fourth Amendment's warrant particularity requirement may limit the manner of search execution. Dalia v. United States, 441 U.S. 238, 258 (1979). This Court has consistently held that the manner of search execution is best left to law enforcement's discretion, subject to a later reasonableness review. United States v. Grubbs, 547 U.S. 90, 97-98 (2006).

This Court should reject the Fourteenth Circuit's adoption of the guidelines set forth in United States v. Comprehensive Drug Testing as unworkable and thus inapplicable to the government's warrant. 579 F.3d 989, 1006 (9th Cir. 2009). These guidelines require magistrates to insist that: 1) the government waive reliance upon the plain view doctrine; 2) specialized personnel or independent third parties segregate and redact seized nonresponsive data with no discussion or assistance from investigators; 3) warrants disclose the actual risks of destruction or concealment of the data sought; 4) all warrants for computer searches include a search protocol,

detailing the type of digital forensic analysis and software to be used; and 5) the government destroy or return data not responsive to the warrant. These guidelines pertain to the way in which digital searches are executed and do nothing to heighten warrant particularity. Thus this Court should determine that the government's warrant was valid and reject the Fourteenth Circuit's restrictions on search execution in the digital context.

To determine whether a search violated the Fourth Amendment, courts review findings of fact for clear error and conclusions of law de novo. See United States v. Cavazos, 288 F.3d 706, 709 (5th Cir. 2002).

A. Magistrates May Continue To Issue Warrants Authorizing Seizure Of Computer Equipment And Files For Later Sorting.

Magistrates are permitted to issue warrants authorizing the seizure of computer equipment and files for subsequent offsite review. Warrants routinely authorize this practice because it is the most practicable way to search for digital evidence. Both Congress and the majority of circuits to have addressed this practice endorse warrants that authorize seizure of computer equipment and files for offsite search. Therefore, this Court should hold that magistrates may continue to issue warrants allowing the seizure and offsite search of computer equipment and other digital media.

1. Warrants routinely authorize seizure of computer files and equipment for later sorting because it is the most feasible way to search for digital evidence.

The scope of the warrant authorizing the FBI to comprehensively search StarTests's computer equipment was reasonably related to the objective of the investigation. A warrant authorizing the search of entire computers or digital storage media may represent the narrowest definable search reasonably likely to obtain the targeted evidence. United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999). This is especially true where law enforcement must search for

information stored in complex computer programs that may or may not include encrypted files. See United States v. Brooks, 427 F.3d 1246, 1252 (10th Cir. 2005). The FBI sought information regarding the five players' drug-test results. R. 1. To obtain the information, the agents applied for a warrant to search StarTests's computer equipment and files. R. 1. The government expected that the files containing results might be encrypted or otherwise hidden for confidentiality purposes. R. 2. Further, the FBI did not know ahead of time which of StarTests's computers held the targeted evidence. To meet the government's objective, Magistrate Judge Leon issued a warrant permitting the agents to search StarTests's computer equipment and storage devices. R. 2. When the FBI agents executed the search, they learned that nearly every computer in the facility contained some information about the CFL players' drug-test results. R. 2. Due to the computer-hopping procedure, they could not determine which computers contained the relevant data. R. 2. The only way for the FBI to locate the five players' drug-test results was to search all of StarTests's computer databases because the facility stored a vast quantity of intricately configured data.

The time and expertise required to search StarTests's databases made on-site review unfeasible and offsite review necessary. Performing extensive digital forensic searches on-site are impracticable because they require time, expertise, and a controlled environment. United States v. Hay, 231 F.3d 630, 637 (9th Cir. 2000). In their warrant application, the FBI asked to seize StarTests's databases for offsite review because they anticipated having to sort through vast quantities of data that might be hidden or encrypted. R. 2. Accordingly, the Magistrate Judge issued a warrant allowing for an offsite search where necessary. R. 2. Indeed, upon arrival at the StarTests facility, the agents encountered the computer-hopping program and many encrypted or hidden files. R. 2. The agents thus concluded the search would take several days. R. 2, 8. The

warrant appropriately authorized the seizure of equipment for offsite review given the technical complexities in carrying out the search.

Moreover, the warrant reasonably addressed the practical concerns of performing a lengthy on-site search. The intrusiveness of a search is a valid factor for this Court to consider when assessing the reasonableness of a warrant. An on-site search may be more intrusive than an offsite search where it requires law enforcement to spend more than several hours on the premises. United States v. Alexander, 574 F.3d 484, 490 (8th Cir. 2009); see also United States v. Wuagneux, 683 F.2d 1343, 1353 (11th Cir. 1982). The FBI anticipated, and the Magistrate Judge agreed, that the search could at a minimum take several days. R. 2. Thus, the warrant authorized the agents to seize StarTests's computer equipment for offsite review where an on-site search would be impracticable. R. 2. The FBI could not have conducted the search for the drug-test results within several hours. The warrant thus reasonably authorized seizure of StarTests's computer files and equipment where an on-site search would have been more intrusive.

2. Congress and the majority of circuits permit warrants to authorize seizure of computer equipment and files for later offsite review.

This Court should look to recent Congressional enactments for guidance in determining whether magistrates may issue warrants authorizing the seizure of computer equipment and files for offsite review. A common law practice that has been codified into law deserves deference as it carries Congressional endorsement. CoStar Group, Inc. v. LoopNet, Inc., 373 F.3d 544, 553 (4th Cir. 2004) (finding codified common law to be a "valuable touchstone" for judicial interpretation). The circuits facing the issue at bar have uniformly held that magistrate judges may issue warrants authorizing the seizure of digital storage devices for later offsite review. See Alexander, 574 F.3d at 490 (upholding warrant authorizing seizure of all suspect's electronic

storage media for later review because on-site search would be unfeasible); United States v. Hill, 459 F.3d 966, 974-75 (9th Cir. 2006); Guest v. Leis, 255 F.3d 325, 335 (6th Cir. 2001); United States v. Campos, 221 F.3d 1143, 1147 (10th Cir. 2000); Upham, 168 F.3d at 537 (1st Cir. 1999). Federal Rule of Criminal Procedure 41(e)(2)(B) provides that a warrant may authorize the seizure of electronic storage media or files for later offsite review. Congress amended Rule 41(e)(2)(B) with the intent to remove burdens arising from on-site digital searches. See Fed. R. Crim. P. 41(e)(2)(B) advisory committee's note. This Court should afford deference to express Congressional intent and uphold warrants like the one at issue here.

B. The digital search guidelines announced by the Fourteenth Circuit place unnecessary restrictions on search warrant execution and are unworkable.

This Court should reject the new restrictions on digital searches imposed by the Fourteenth Circuit, which are without any precedential support from this Court. These guidelines purport to heighten warrant particularity, but in fact place restrictions on the manner of search execution. Moreover, these five restrictions are overly burdensome and will seriously impede law enforcement's ability to obtain critical digital evidence. This Court should thus decline to adopt these new warrant requirements and reverse the Fourteenth Circuit's decision.

1. The Fourteenth Circuit's digital search guidelines do not heighten warrant particularity but rather place unnecessary limitations on the manner of search execution.

Under the pretext of heightening particularity, the Fourteenth Circuit imposed restrictions on the government's digital search procedures that in fact reach beyond what particularity requires. Specifying the manner in which searches are executed is outside the scope of the particularity requirement. United States v. Grubbs, 547 U.S. 90, 97-98 (2006) (limiting particularity requirement to description of the place to be searched and the person or things to be seized); Dalia, 441 U.S. 238, 258 (1979) (finding "nothing in the language of the Constitution"

to suggest that warrants must specify the precise manner of search execution). The Fourteenth Circuit imposed five restrictions on the manner in which the government must perform digital searches. R. 17. Finding that the government’s warrant did not include these restrictions, the court held the warrant overbroad. R. 17. The Fourteenth Circuit cannot impose these restrictions under the guise of particularity and should not have invalidated the government’s warrant on these grounds.

The Fourteenth Circuit’s digital search restrictions are unnecessary and inappropriate because courts review the reasonableness of a search after the warrant is executed. Reasonableness of search execution is a matter for reviewing courts to decide after a search has been executed, not for magistrate judges to decide before issuing a warrant. Dalia, 441 U.S. at 258 (holding it unnecessary to require a specific manner of warrant execution because it is “subject to later judicial review as to its reasonableness”). Judge Leon did not dictate the precise manner of search execution when issuing the warrant and the reviewing district court determined the search had been conducted reasonably. R. 2, 5-6. The guidelines set forth by the Fourteenth Circuit require magistrate judges to impose specific search procedure restrictions before issuing warrants in digital evidence cases. R. 17. Such restrictions are unnecessary because courts ensure that officers properly execute searches by reviewing their conduct after the warrant is executed.

The Fourteenth Circuit’s search guidelines would improperly interfere with law enforcement judgment in deciding how to execute digital searches like the StarTests search. Details of how to execute a search are best left to the discretion of executing officers. Dalia, 441 U.S. at 257; see also Hill, 459 F.3d 974 (explaining that officers have discretion as to digital search method subject to general Fourth Amendment reasonableness standard). This is

especially true for digital searches, as magistrates do not usually possess the technical expertise to discern the best digital search method. United States v. Graziano, 558 F. Supp. 2d 304, 316 (E.D.N.Y. 2008). The Fourteenth Circuit's guidelines mandate that warrants for digital searches specify the computer analysis steps to be taken, the personnel that will conduct the forensic analysis, and how those personnel may communicate with investigators. R. 14-15. These search guidelines inappropriately encroach upon the discretion that law enforcement needs to conduct effective digital searches.

2. The Fourteenth Circuit's digital search guidelines are unworkable and place an undue burden on law enforcement.

The five guidelines set forth by the court below are impracticable and will excessively hamper law enforcement efforts. First, law enforcement should not be required to waive reliance on the plain view doctrine as a condition of obtaining warrants for digital searches. Second, magistrate judges should not require segregation and redaction of digital evidence to be performed by government personnel or independent screeners who cannot communicate freely with investigating agents. Third, warrants should not be required to disclose the actual risks of destruction or concealment of data. Fourth, the government should not be required include search protocols in digital search warrants. Finally, effective procedures already exist to ensure that the government returns non-responsive evidence. Therefore, this Court should reject the Fourteenth Circuit's digital search guidelines.

a. Law enforcement should not be required to waive reliance on the plain view doctrine.

This Court should not hinder law enforcement by requiring them to waive reliance on plain view as a condition of obtaining warrants. It is an extreme measure to ask law enforcement to willfully ignore incriminating evidence in plain view during a lawful search. See United States

v. Lopez, 777 F.2d 543, 547 (10th Cir. 1985); Farlow, 2009 WL 4728690, at *6 n.3 (“The judicial directive to forswear in advance the plain view doctrine [in the digital context] is equivalent to demanding that a DEA investigative team engaged in the search of a residence for drugs promise to ignore screams from a closet or a victim tied to a chair.”). The FBI opened the database containing the drug-test results for the five players and other positive test results immediately appeared in plain view. R. 5-6. Preventing the FBI from relying on plain view here would shield evidence of illegal drug activity and in future cases could shield evidence of other serious crimes.

b. Warrants should not impose barriers on communication between investigators and computer forensics specialists.

A rule chilling communications between computer forensics specialists and investigating agents will encumber law enforcement efforts. In complex digital investigations, computer personnel must openly communicate with agents who are intimately familiar with the investigation. Brief for the United States in Support of Rehearing en banc by the full court at 16, United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1006 (9th Cir. 2009) (No. CR Misc. 04-234 SI). If they cannot communicate freely, the technicians may not recognize critical evidence because they lack sufficient knowledge of the case. Id. at 6; see also U.S. Department of Justice, Office of the Inspector General, “The Federal Bureau of Investigation’s Efforts to Combat Crimes Against Children Audit Report 09-08,” January 2009 at 25 (noting that in FBI investigations of cyber crimes against children it is routine practice for specialized computer personnel to communicate regularly with the investigators to facilitate the search process). For example, in the District of Arizona, an FBI computer forensics specialist attempting to comply with Comprehensive Drug Testing, and barred from communicating with investigative agents, spent months learning a case to try to properly segregate data on a seized computer. Brief for the

United States at 16, *Comprehensive Drug Testing, Inc.*, (9th Cir. 2009) (No. CR Misc. 04-234 SI). Following *Comprehensive Drug Testing*, the Fourteenth Circuit adopted the same requirement. R. 17. This Court should reject such an unduly restrictive requirement on government personnel seeking to carry out digital investigations.

c. Warrants should not be required to list the actual risks of data concealment and destruction.

It is unreasonable to require law enforcement to list the exact risks of data concealment and destruction in a warrant application. Digital files may be concealed, disguised, or destroyed in a multitude of ways. See *Giberson*, 527 F.3d at 889 (“Computer files are extremely susceptible to tampering, hiding, or destruction, whether deliberate or inadvertent.”). In their warrant application, the FBI agents explained several ways that a facility like StarTests, whose aim it was to maintain customer confidentiality, would likely conceal or disguise data. R. 2. While correct in some of their predictions, they were not able to foresee certain data concealment methods with precision, such as the “computer-hopping” procedure. R. 8. In other criminal investigations, it may be even harder to predict the actual risks of data concealment where law enforcement has little or no knowledge of how the given search target maintains its digital data. Contrary to the Fourteenth Circuit’s opinion, Magistrate Judge Leon need not have required the warrant to disclose the actual risks of digital data destruction or concealment because these risks are extremely difficult to predict.

d. Warrants should not be required to include search protocols.

Requiring the FBI’s warrant to structure a search protocol to encompass every digital search contingency would have been impracticable. Digital search protocols in warrants are unworkable because the complexity and unpredictability of digital forensic analysis requires flexibility. *United States v. Burgess*, 576 F.3d 1078, 1093-94 (10th Cir. 2009) (“it is folly for a

search warrant to attempt to structure the mechanics of the [digital] search and a warrant imposing such limits would unduly restrict legitimate search objectives”); Graziano, 558 F. Supp. 2d at 315 (declining to impose digital search protocol requirement and noting that numerous other courts have done the same). When the FBI agents executed the warrant at the StarTests facility, they came across the computer-hopping procedure—an unexpectedly intricate database configuration. R. 8. It would have been unfeasible for the agents to devise an exact search method that accounted for these contingencies.

e. Procedures already exist to ensure that the government returns nonresponsive data.

A new rule requiring the government to return nonresponsive data is duplicative of effective procedural mechanisms already in place. Federal Rule of Criminal Procedure 41(g) mandates that law enforcement return unnecessary evidence seized pursuant to a warrant. See Fed. R. Crim. P. 41(g) (allowing person aggrieved by seizure of property to move for its return). Indeed, Respondents in the case at bar employed Federal Rule of Criminal Procedure 41(g) to seek the return of allegedly nonresponsive data. R. 1. Where Rule 41(g) provides parties with recourse for the return of seized property, the new rule set forth by the Fourteenth Circuit serves no purpose. Thus, this Court should not impose new restrictions on warrants in the digital evidence context because they are ineffective and excessively burdensome.

CONCLUSION

For the foregoing reasons, this Court should reverse the decision of the Fourteenth Circuit Court of Appeals.

Respectfully Submitted,

/s/ Team Number 5
Team Number 5
Counsel for Petitioner

APPENDIX

Relevant Portions of the U.S. Constitution

U.S. Const. amend. IV.

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

Relevant Portions of Federal Rules

Federal Rule of Criminal Procedure 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.

Federal Rule of Criminal Procedure 41(e)(2)(B):

Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.