

No. 2010-W20

IN THE SUPREME COURT OF THE UNITED STATES

UNITED STATES OF AMERICA,
Petitioners,
v.
STARTESTS, INC. AND THE COLONIAL FOOTBALL LEAGUE,
Respondents.

On Writ of Certiorari to the
Supreme Court of the United States

BRIEF FOR RESPONDENTS

Spong Competition Number: 6

QUESTIONS PRESENTED

1. Whether a professional football organization has standing to bring a Motion for Return of Property under FED. R. CRIM. P. 41(g) for databases that the FBI seized when conducting an investigation into illegal steroid use within professional football?
2. Whether government can use the plain view doctrine to justify seizing digital evidence not listed in the warrant that comes into the officers' view during the search?
3. Whether the Fourth Amendment mandates heightened particularity in digital evidence seizure cases, thus prohibiting magistrates from authorizing the government to seize all computer files for later sorting?

TABLE OF CONTENTS

QUESTION PRESENTED.....	ii
TABLE OF CONTENTS.....	iii
TABLE OF AUTHORITIES.....	vii
OPINIONS BELOW.....	1
CONSTITUTIONAL PROVISIONS, STATUTES, AND REGULATIONS INVOLVED.....	1
STATEMENT OF THE CASE.....	2
I. <u>THE FBI’S UNLAWFUL SEIZURE OF RESPONDENTS’ PROPERTY</u>	2
II. <u>DECISIONS AND ARGUMENTS BELOW</u>	4
SUMMARY OF THE ARGUMENT.....	5
ARGUMENT.....	7
I. <u>THIS COURT SHOULD AFFIRM THE FOURTEENTH CIRCUIT’S HOLDING THAT RESPONDENTS HAVE STANDING TO BRING A MOTION FOR RETURN OF PROPERTY PURSUANT TO FED. R. CRIM. P. 41</u>	7
A. <u>The CFL Has Associational Standing To Bring The Motion On Behalf Of Its Players</u>	7
1. <u>The CFL has associational standing because the players could sue in their own right</u>	8
2. <u>The CFL has associational standing because its litigation interest is germane to its organizational purpose</u>	9
3. <u>The CFL has associational standing because its players do not need to be present for this Court to resolve the dispute</u>	9

B.	<u>The CFL Has Standing To Bring The Motion Because The Government’s Actions Made It An Aggrieved Party</u>	10
1.	<u>The CFL meets the traditional constitutional requirements for standing</u>	11
a.	<u>The CFL satisfies the prudential standing requirements</u>	12
b.	<u>Even if this Court finds that the CFL is standing in for the players, the CFL meets the <i>Singleton</i> exception to the ban on third party standing</u>	13
2.	<u>The CFL has standing to challenge the FBI’s actions because it had a legitimate expectation of privacy in the things seized and the place searched</u>	14
C.	<u>Rule 41(g) Is An Appropriate Remedy</u>	16
II.	<u>THE GOVERNMENT MAY NOT USE THE PLAIN VIEW DOCTRINE TO RIFFLE THROUGH PRIVATE INFORMATION IN DIGITAL EVIDENCE SEARCHES TO DEVELOP A CASE AGAINST ATTRACTIVE DEFENDANTS</u>	17
A.	<u>The Plain View Doctrine Cannot Apply To Digital Evidence Seizures Because Executing Officers Misuse The Doctrine And Digital Evidence Requires A Unique Solution That Cannot Be Crafted From Traditional Criminal Procedure Exceptions To The Warrant Requirement</u>	17
1.	<u>Allowing the government to seize everything that comes into view during a digital evidence search gives officers unfettered discretion to seize anything they wish</u>	18
2.	<u>The plain view doctrine has no practical application in digital evidence cases because digital data is distinct from the physical evidence that informed the plain view doctrine</u>	20

B.	<u>Even If This Court Allows The Government To Rely On The Plain View Doctrine In Digital Evidence Seizures, The Government Cannot Meet The Doctrine’s Requirements</u>	22
1.	<u>The FBI cannot rely on the plain view doctrine because it did not view the players’ test results from a lawful vantage point</u>	22
2.	<u>The FBI has not met its burden under the plain view exception because the incriminating nature of the players’ test results was not immediately apparent</u>	24
3.	<u>The FBI has not met the plain view exception’s requirements because it did not have lawful access to seize the remaining players’ test results</u>	25
C.	<u>This Court Should Not Allow The Government To Rely On The Plain View Doctrine When It Blatantly Disregarded Respondents’ Fourth Amendment Rights</u>	26
III.	<u>THIS COURT SHOULD EMBRACE THE GUIDELINES THAT BOTH THE NINTH AND FOURTEENTH CIRCUITS ADOPTED TO HEIGHTEN THE PARTICULARITY REQUIREMENT FOR DIGITAL EVIDENCE WARRANTS</u>	26
A.	<u>Heightening The Particularity Requirement For Digital Evidence Warrants Is Consistent With The Framers’ Intent</u>	26
1.	<u>The framers’ primary concern when drafting the Fourth Amendment was to prevent the issuance of general warrants</u>	27
2.	<u>Judge Leon’s warrant runs afoul of the framers’ particularity requirement</u>	28
3.	<u>This Court heightens Fourth Amendment protection when necessary to protect American citizens from unreasonable searches and seizures</u>	29

B. <u>The Test For Digital Evidence Warrants From Comprehensive Drug Testing And Its Progeny Is Consistent With The Fourth Amendment’s Particularity Requirement</u>	30
1. <u>The Comprehensive guidelines uphold the sanctity of the Fourth Amendment</u>	31
2. <u>Courts validating broad warrants face distinguishable facts from the case at bar and did not give enough credence to the particularity requirement</u>	31
C. <u>The Particularity Requirement’s Role In Digital Evidence Warrants Is Not a Job For The Legislature</u>	34
1. <u>This Court may properly heighten the particularity requirement in digital evidence cases because it is the definitive interpreter of the constitution</u>	34
2. <u>The legislature’s recent amendments to the Federal Rules of Criminal Procedure do not adequately address the unique problems inherent in digital evidence seizures</u>	35
D. <u>The Government Has Not Met The Five Requirements Of The Comprehensive Test</u>	35
CONCLUSION.....	37

TABLE OF AUTHORITIES

United States Supreme Court

<i>Allen v. Wright</i> , 468 U.S. 737 (1984).....	11, 12
<i>Arizona v. Hicks</i> , 480 U.S. 321 (1987).....	24
<i>Carroll v. United States</i> , 267 U.S. 132 (1925).....	34
<i>Coolidge v. New Hampshire</i> , 403 U.S. 433 (1971).....	18, 24, 25, 28, 33
<i>County of Riverside v. McLaughlin</i> , 500 U.S. 44 (1991).....	8
<i>Fed. Election Comm’n v. Akins</i> , 524 U.S. 11 (1998).....	11, 12
<i>Ferguson v. City of Charleston</i> , 532 U.S. 67 (2001).....	8
<i>Flast v. Cohen</i> , 392 U.S. 83 (1968).....	13
<i>Gerstein v. Pugh</i> , 420 U.S. 103 (1975).....	25
<i>Groh v. Ramirez</i> , 540 U.S. 551 (2004).....	22, 23
<i>Havens Realty Corp. v. Coleman</i> , 455 U.S. 363 (1982).....	11
<i>Hein v. Freedom From Religion Foundation, Inc.</i> , 551 U.S. 587 (2007).....	13
<i>Horton v. California</i> , 496 U.S. 128 (1990).....	18, 22, 23, 24, 25, 34
<i>Hunt v. Wash. State Apple Adver. Comm’n</i> , 432 U.S. 333 (1977).....	8, 9, 10
<i>Illinois v. Rodriguez</i> , 497 U.S. 177 (1990).....	34
<i>International Union, United Automobile Workers v. Brock</i> , 477 U.S. 274 (1986).....	8
<i>Johnson v. United States</i> , 333 U.S. 10 (1971).....	18, 25, 27, 30
<i>Katz v. United States</i> , 389 U.S. 347 (1967).....	9, 14, 15, 16, 28
<i>Lujan v. Defenders of Wildlife</i> , 504 U.S. 555 (1992).....	10, 12
<i>Maryland v. Garrison</i> , 480 U.S. 79 (1987).....	28,
<i>Marron v. United States</i> , 274 U.S. 192 (1927).....	22, 28
<i>Minnesota v. Olson</i> , 495 U.S. 91 (1990).....	14, 16, 18
<i>NAACP v. Alabama</i> , 357 U.S. 449 (1958).....	8, 9
<i>Pennell v. City of San Jose</i> , 485 U.S. 1 (1988).....	8, 10
<i>Rakas v. Illinois</i> , 439 U.S. 128 (1978).....	14, 16
<i>Rawlings v. Kentucky</i> , 448 U.S. 98 (1980).....	14
<i>Schmerber v. California</i> , 384 U.S. 757 (1996).....	30
<i>Shadwick v. City of Tampa</i> , 407 U.S. 345 (1972).....	25
<i>South Dakota v. Opperman</i> , 428 U.S. 364 (1976).....	25
<i>Simon v. E. Ky. Welfare Rights Org.</i> , 426 U.S. 26, 41-42 (1975).....	10
<i>Singleton v. Wulff</i> , 428 U.S. 106 (1976).....	13
<i>Steagald v. United States</i> , 451 U.S. 204 (1981).....	27, 30
<i>Steele v. United States</i> , U.S. 498 (1925).....	27
<i>Tennessee v. Gardner</i> , 471 U.S. 1 (1985).....	29, 34
<i>United States v. Chadwick</i> , 433 U.S. 1 (1977).....	27
<i>United States v. Dunn</i> , 480 U.S. 294 (1987).....	15
<i>United States v. Leon</i> , 468 U.S. 897 (1984).....	23, 25
<i>United States v. Richardson</i> , 418 U.S. 166 (1974).....	13
<i>United States v. Salvucci</i> , 448 U.S. 83 (1980).....	14
<i>Vale v. Louisiana</i> , 399 U.S. 30 (1969).....	29
<i>Warth v. Seldin</i> , 422 U.S. 490 (1975).....	10, 11, 14

<i>Weeks v. United States</i> , 232 U.S. 383 (1914).....	27
<i>Whitmore v. Arkansas</i> , 495 U.S. 149 (1990).....	10
<i>Williams v. United States</i> , 401 U.S. 667 (1971).....	34
<i>Wilson v. Layne</i> , 526 U.S. 603 (1999).....	23
<i>Winston v. Lee</i> , 470 U.S. 753 (1985).....	30
<i>Ybarra v. Illinois</i> , 444 U.S. 85 (1979).....	29

Constitution

U.S. Const. amend. IV.....	26, 31, 34
----------------------------	------------

Statutes

FED. R. CRIM. P. 41(e)(2)(B).....	35
FED. R. CRIM. P. 41(g).....	11

United States Court of Appeals Cases

<i>In re Search Warrant for K-Sports Imports, Inc.</i> , 163 F.R.D. 594 (C.D. Cal. 1995).....	28, 29
<i>J.B. Manning Corp. v. United States</i> , 86 F.3d 926 (9th Cir. 1996).....	16, 17
<i>Ramsden v. United States</i> , 2 F.3d 322 (9th Cir. 1993).....	17
<i>Richey v. Smith</i> , 515 F.2d 1239 (5th Cir. 1975).....	17
<i>Trulock v. Freeh</i> , 275 F.3d 391 (4th Cir. 2001).....	16
<i>United States v. Adjani</i> , 452 F. 3d 1140 (9th Cir. 2006).....	19, 33
<i>United States v. Alexander</i> , 574 F.3d 484 (8th Cir. 2009).....	33
<i>United States v. Carey</i> , 172 F.3d 1268 (10th Cir. 1999).....	19, 21
<i>United States v. Comprehensive Drug Testing, Inc.</i> , 579 F.3d 989 (9th Cir. 2009).....	9, 18, 21, 23, 24, 26, 29, 30, 31, 33, 36, 37
<i>United States v. Johnson</i> , 584 F.3d 995 (10th Cir. 2009).....	15
<i>United States v. Lacy</i> , 119 F.3d 742 (9th Cir. 1997).....	31, 32
<i>United States v. Lamb</i> , 945 F. Supp. 441 (N.D.N.Y. 1996).....	31, 32
<i>United States v. Raney</i> , 342 F.3d 551 (7th Cir. 2003).....	33
<i>United States v. Spilotro</i> , 800 F.2d 959 (9th Cir. 1986).....	15
<i>United States v. Tamara</i> , 694 F.2d 591 (9th Cir. 1982).....	19
<i>United States v. Turner</i> , 169 F.3d 84 (1st Cir. 1999).....	18
<i>United States v. Vitek Supply Corp.</i> , 144 F.2d 476 (7th Cir. 1998).....	28, 31
<i>United States v. Walser</i> , 275 F.3d 981 (10th Cir. 2001).....	21

Law Review Articles

Donald A. Dripps, <i>Criminal Procedure, Footnote Four, and the Theory of Public Choice; Or Why Don't Legislatures Give a Damn About the Rights of the Accused?</i> , 44 Syracuse L. Rev. 1079 (1993).....	35
Orin S. Kerr, <i>Digital Evidence and the New Criminal Procedure</i> . 105 Colum. L. Rev. 279 (2005).....	20, 21
Orin S. Kerr, <i>Searches and Seizures in a Digital Evidence World</i> , 119 Harv. L. Rev. 531 (2005).....	29, 33
Osmond K. Fraenkel, <i>Concerning Searches and Seizures</i> , 34 Harv. L. Rev. 361 (1920).....	27

Ray Chang, <i>Why the Plain View Doctrine Should Not Apply to Digital Evidence</i> , 12 Suffolk J. Trial & App. Advoc. 31 (2007).....	20, 21, 22
Samantha Trepel, <i>Digital Searches, General Warrants, and the Case for the Courts</i> , 10 Yale J. L. & Tech. 120 (2007).....	27

OPINIONS BELOW

The United States District Court for the District of Wythe's decision is included in the record. (R. at 1.) The United States Fourteenth Circuit Court's decision is also contained in the record. (R. at 7.)

CONSTITUTIONAL STATUTES AND PROVISIONS INVOLVED

The Fourth Amendment to the United States Constitution provides as follows:

“[t]he 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.”

Federal Rule of Criminal Procedure Rule 41(g) Motion To Return Property provides as follows:

“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 Rule 41(e)(2)(B) Warrant Seeking Electronically Stored Information provides as follows:

“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.”

STATEMENT OF THE CASE

I. THE FBI'S UNLAWFUL SEIZURE OF RESPONDENTS' PROPERTY

The Colonial Football League (“CFL”) is a federation of professional football franchises. (R. at 1.) StarTests, Inc. (“StarTests”) is a private business that administers drug tests and stores results for sports organizations, businesses, schools, and other entities. (R. at 1, 8.) The CFL began requiring its franchises to test players for drugs in 2005. (R. at 8.) In 2005, the CFL hired StarTests to administer drug tests to all CFL franchise players. (R. at 8.) The CFL players had to submit to testing as a term of their membership. (R. at 8.) The CFL implemented this program to comply with its own performance standards and federal law, as well as to alleviate a media blitz on steroid use in professional sports. (R. at 1, 8.)

StarTests stored the results in its Millerville facility. (R. at 2.) The CFL and StarTests explicitly communicated to the players that the tests were “strictly to determine whether five percent or more of the CFL’s players would test positive for illegal steroids.” (R. at 1.) If the initial tests revealed more than five percent of the CFL’s players used illegal steroids, the CFL would implement a more frequent testing program. (R. at 1.) The CFL and StarTests agreed that StarTests would make the percentage public. (R. at 1.) However, StarTests and the CFL told the players that StarTests would keep the names and results confidential. (R. at 1.)

In July 2008, the FBI began investigating the following CFL players for alleged illegal steroid use: Barry Reynolds, Danny Rodriguez, John Reeves, Michael Fleming, and Ace Hall. (R. at 1.) The FBI already had evidence that these five players acted illegally, including numerous eyewitness reports and taped conversations where the players discussed obtaining steroids. (R. at 7.) In an effort to strengthen its case, the FBI applied for a warrant to search StarTests’ facilities and seize information relating to these five players. (R. at 8.) The affidavit

supporting the warrant request sought authorization to seize documents, urine samples, and “all records, files and equipment” pertaining to the CFL’s tests. (R. at 1-2.) The FBI requested permission to seize files for a later “off-site” search, asserting that an on-site search was impracticable since StarTests likely misleadingly labeled some files to protect the players’ privacy, and the FBI did not have the software to decrypt on-site. (R. at 2.)

Magistrate Judge Leon issued a warrant authorizing agents to search StarTests’ Millerville facility for computer equipment and storage devices. (R. at 2.) The warrant allowed agents to either seize the equipment or copy it for a later “off-site” search if they determined an “on-site” search was impractical. (R. at 2.) Judge Leon placed merely one limitation on the executing agents’ discretion: only law enforcement personnel specifically trained in searching and seizing computer data could decide whether data needed to be seized and subsequently searched. (R. at 2.) These specially trained personnel could only seize information “reasonably related to the investigation into the five named players’ steroid use.” (R. at 8.) Judge Leon explicitly directed the government to return all property to StarTests that the warrant did not authorize its agents to seize. (R. at 2.)

The FBI executed the search warrant on November 1, 2008. (R. at 2.) StarTests employees quickly informed FBI agents that CFL data was on almost every computer in the facility because the CFL was one of StarTests’ biggest clients. (R. at 2.) Agents soon learned that StarTests utilized a “computer-hopping” procedure to ensure client confidentiality. (R. at 2.) StarTests “hopped” information among several computers so that one computer had the players’ personal health information, one contained the players’ anonymous numbers, and a final computer had the players’ test results identifiable only by their anonymous numbers. (R. at 2.)

The head FBI agent ordered the other agents to seize or copy *all* of the computers and equipment so that agents could search each at the FBI's office in Wythe City. (R. at 2, 8.)

The FBI ultimately found the test results for the five players named in the warrant. (R. at 9.) However, while broadly searching through the databases, investigators came across the names of other CFL players, not under investigation, who tested positive for illegal steroids and other substances. (R. at 2.) The FBI expanded its investigation to include all illegal drug possession and sale within professional football, and it retained all of the CFL's test results to use in its broadened investigation. (R. at 2.) StarTests and the CFL filed a timely motion for return of the copied discs and other electronic data because the FBI insisted on keeping evidence on players other than those named in the warrant. (R. at 3, 8.)

II. DECISIONS AND ARGUMENTS BELOW

StarTests and the CFL filed a motion for return of property pursuant FED. R. CRIM. P. 41(g) in the United States District Court for the District of Wythe, contending that the FBI's warrant and subsequent search and seizure violated their Fourth Amendment rights. (R. at 1, 4.) Specifically, StarTests and the CFL argued that the warrant was overly broad because it allowed agents to seize computer equipment after only a hasty initial relevance determination. (R. at 4.) Additionally, StarTests and the CFL contended that the FBI agents acted outside the warrant's scope when they seized information unrelated to the original five players who sparked the investigation. (R. at 4.) The United States conceded that it did not have probable cause to hold the information on the other players, but that the "plain view" exception to the warrant requirement made its seizure of the information lawful. (R. at 4.) Finally, the United States challenged the CFL's standing to bring the Motion. (R. at 3.)

The District Court quickly disregarded the United States’ standing challenge, holding that the CFL has associational standing to sue on behalf of its players and seek the return of its property being stored at StarTests when the seizure occurred. (R. at 3.) The District Court did not address whether the warrant was sufficiently particular. (R. at 4.) The District Court held that the “plain view” doctrine extends to the search and seizure of digital evidence. (R. at 4-5.) The District Court denied StarTests and the CFL’s 41(g) Motion and validated the FBI’s conduct using the “plain view” rationale. (R. at 6.) StarTests and the CFL filed a timely appeal to the U.S. Circuit Court of Appeals for the Fourteenth Circuit. (R. at 7.)

The U.S. Circuit Court of Appeals for the Fourteenth Circuit reversed the District Court’s decision and held that the initial warrant and subsequent seizure violated StarTests and the CFL’s Fourth Amendment rights. (R. at 7, 14.) The Court of Appeals quickly disregarded the United States’ standing challenge, and it adopted the Ninth Circuit’s standard for evaluating search warrants in digital evidence cases. (R. at 10, 17.) The Court, after applying the Ninth Circuit’s practical five-prong test, determined that the FBI’s warrant was overbroad. (R. at 15.) The Court of Appeals did not need to address whether the government’s actions fell within the “plain view” exception to the warrant requirement because the Ninth Circuit’s test requires that the government waive reliance upon the plain view doctrine in any warrant application to search and seize digital evidence. (R. at 14.) The Court also ordered the FBI to return the property to StarTests’ facilities pursuant to FED. R. CRIM. P. 41(g). (R. at 16.)

SUMMARY OF THE ARGUMENT

The CFL has standing to challenge the government’s actions as an association and in its own right. The CFL meets all three of this Court’s requirements for associational standing: the players could bring suit themselves, the CFL’s litigation interest is germane to its organizational

purpose, and the players do not need to be present for this Court to adjudicate Respondents' Motion. Even if this Court does not think that the CFL has associational standing, the CFL may also bring the 41(g) Motion on its own because it has suffered an injury, the government's actions caused its injury, and a favorable court decision will remedy its injury. The CFL likewise meets the prudential requirements for standing because it is not asserting a generalized grievance or the rights of a third party. Even if this Court thinks that the CFL is standing in for a third party, the CFL fits within the recognized exception to the ban on third party standing. The CFL also has standing to sue on its own behalf because it has a legitimate expectation of privacy in the test results, and it may lawfully challenge the place searched under the Fourth Amendment. Rule 41(g) is an appropriate remedy for the CFL's injury.

The government wishes to shoehorn the FBI's unlawful conduct into the plain view exception to the warrant requirement, but courts cannot logically apply the plain view doctrine to digital evidence seizures without profound negative consequences. First, if law enforcement officials can rely on the plain view exception during digital evidence searches, then officers would have unfettered discretion to comb through responsive as well as non-responsive, constitutionally protected data. Second, such unfettered discretion violates American citizens' right to be free from unreasonable searches and seizures under the Fourth Amendment. Third, traditional criminal procedure rules, such as the plain view doctrine, are illogical in the digital evidence context because digital evidence is unlike physical evidence where warrants can place specific limitations on law enforcement's search techniques. Even if this Court thinks that the government can rely on the plain view exception for digital evidence searches, the government has not proven it fulfills the plain view doctrine's three requirements that it lawfully viewed all

of the players test results, that the test results' incriminating nature was immediately apparent, or that the agents lawfully obtained the results.

This Court should heighten the particularity requirement for digital evidence warrants by adopting the Fourteenth Circuit's well-reasoned guidelines. The framers intended to prevent magistrates from issuing general warrants by requiring law enforcement officials to particularly describe the places they will search and the items they will seize. If this Court heightens the particularity requirement for digital evidence searches, it will be acting consistently with its previous decisions expanding Fourth Amendment protection. Lower court cases that have failed to heighten Fourth Amendment protection for digital evidence seizures do not give enough credence to the particularity requirement. The Ninth Circuit's test for digital evidence warrants ensures that the particularity requirement remains more than just a truism. This Court should adopt the Ninth Circuit's test rather than leaving the important question of the particularity requirement's role in digital evidence cases unanswered because this Court is the sole interpreter of the constitution. If this Court adopts the Ninth Circuit's well-reasoned test for digital evidence warrants, the government cannot satisfy that test's guidelines and must return Respondent's property.

ARGUMENT

- I. THIS COURT SHOULD AFFIRM THE FOURTEENTH CIRCUIT'S HOLDING THAT RESPONDENTS HAVE STANDING TO BRING A MOTION FOR RETURN OF PROPERTY PURSUANT TO FED. R. CRIM. P. 41(g)
 - A. The CFL Has Associational Standing To Bring The Motion On Behalf Of Its Players

The CFL has associational standing to challenge the government's conduct. An association may have standing to sue both as an entity as well as on behalf of its members. *See International Union, United Automobile Workers v. Brock*, 477 U.S. 274, 286-87 (1986) (holding that the Union could sue on its own for injuries suffered and on behalf of its members even though the members could have sued individually). Associational standing allows an association to represent its members' interests in court. *NAACP v. Alabama*, 357 U.S. 449, 459 (1958). The three-prong test this Court uses to determine whether an organization has standing to sue on behalf of its members is as follows: "(1) its members would otherwise have standing to sue in their own right; (2) the interests it seeks to protect are germane to the organization's purpose; and (3) neither the claim asserted nor the relief requested requires the participation in the lawsuit of the individual members." *Hunt v. Wash. State Apple Adver. Comm'n*, 432 U.S. 333, 343 (1977); *see also Pennell v. City of San Jose*, 485 U.S. 1, 7 n.3 (1988).

1. The CFL has associational standing because the players could sue in their own right

The CFL may properly challenge the FBI's actions on behalf of its members under the doctrine of associational standing. *See NAACP*, 357 U.S. at 459. Under *Hunt's* first prong, the CFL may sue on behalf of its members because the players would be able to sue in their own right. 432 U.S. at 343. The government concedes that it lacked probable cause to hold information on players other than the five specifically named in the warrant. (R. at 9.) This fact alone gives the players standing to challenge the seizure of their test results. *See County of Riverside v. McLaughlin*, 500 U.S. 44, 51 (1991) (holding that the plaintiffs had standing to challenge their arrest since officers incarcerated them without a probable cause determination). Moreover, the players could seek the return of their own test results because this Court

recognizes that an individual has a legitimate expectation of privacy in his or her bodily fluids. *See Ferguson v. City of Charleston*, 532 U.S. 67, 70-73 (2001) (holding that patients have a reasonable expectation of privacy that medical personnel will not share their urine samples “nonmedical personnel without [their] consent”). The players expected that StarTests would keep the results private. (R. at 1.) Under *Katz v. United States*, this expectation is one that society accepts as reasonable because objectively speaking, the medical community and facilities supporting it go to extraordinary lengths to keep records private. 389 U.S. 347, 361 (1967) (Harlan, J., concurring). Thus, the CFL meets the first-prong of the *Hunt* test for associational standing because the players could sue in their own right. 432 U.S. at 343.

2. The CFL has associational standing because its litigation interest is germane to its organizational purpose

The CFL’s litigation interest is germane to its organizational purpose of safeguarding the moneymaking potential of the sport of football. *See Hunt*, 432 U.S. at 343. To be successful in this endeavor, the CFL must protect the players from tarnish. In *Pennell*, this Court determined that the plaintiff, a homeowners’ association, had a litigation interest that was germane to its organizational purpose of protecting lessor’s rights. 485 U.S. at 1. Like the homeowners’ association, the CFL “is protecting the well-being of its members, which could easily be impaired if the government were to release the test results swept up in the [investigatory] dragnet.” *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 1001 (9th Cir. 2009). The CFL procured StarTests’ services to protect its public image, which includes the players’ public impression. (R. at 3.) Therefore, since the CFL’s profit motive is inextricably linked with the players’ images, the CFL’s litigation interest is germane to its organizational purpose.

3. The CFL has associational standing because its players do not need to be present for this Court to resolve the dispute

“[N]either the claim asserted nor the relief requested requires the participation in the lawsuit of the individual members.” *Hunt*, 432 U.S. at 343. Petitioners may argue that the players are necessary to manage the lawsuit. However, the CFL wants to protect *all* of the players’ test results, while individual players would only be interested in protecting their individual positive results. Thus, the CFL is the best party to litigate on behalf of all the players. Moreover, this Court recognizes associational standing more freely if an “association seeks a declaration, injunction, or some other form of prospective relief” because it is likely judicial relief “will inure to the benefit of those members of the association actually injured.” *Warth v. Seldin*, 422 U.S. 490, 515 (1975). Respondents seek the return of copied disks and other digital evidence pursuant to FED. R. CRIM. P. 41(g). (R. at 3.) Thus, the players do not need to be present because Respondents seek injunctive relief rather than damages. Therefore, under *Hunt*, this Court should find that Respondents can assert the players’ rights because the players do not need to be present to litigate whether the government must return Respondents’ property.

B. The CFL Has Standing To Bring The Motion Because The Government’s Actions Made It An Aggrieved Party

The CFL meets the traditional constitutional requirements for standing. The issue of standing “is whether the litigant is entitled to have the court decide the merits of the dispute or of particular issues.” *Warth*, 422 U.S. at 498. Article III confers on federal courts jurisdiction to hear only “‘cases and controversies,’ and the doctrine of standing serves to identify those disputes which are appropriately resolved through the judicial process.” *Whitmore v. Arkansas*, 495 U.S. 149, 154-55 (1990). The plaintiff must allege that he suffered an “injury in fact,” and the injury must be “concrete and particularized” and “actual or imminent, not

conjectural or hypothetical.” *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992).

Additionally, a court may hear a case only if it can trace the plaintiff’s injury to “the challenged action of the defendant.” *Simon v. E. Ky. Welfare Rights Org.*, 426 U.S. 26, 41-42 (1975).

Finally, the plaintiff’s “relief from the injury must be ‘likely’ to follow from a favorable [court] decision.” *Allen v. Wright*, 468 U.S. 737, 751 (1984).

1. The CFL meets the traditional constitutional requirements for standing

Respondents have properly alleged and suffered an economic “injury in fact.” *See Fed. Election Comm’n v. Akins*, 524 U.S. 11, 24 (1998) (explaining that “where a harm is concrete . . . the Court has found ‘injury in fact’”). This Court recognizes that an organization has standing where it is injured as a whole unit, where the organization suffers a “concrete and demonstrable injury to [its] activities—with the consequent drain on [its] resources,” and the injuries are “far more than simply a setback to the organization’s abstract social interests.” *Havens Realty Corp. v. Coleman*, 455 U.S. 363, 379 (1982). The FBI deprived the CFL and StarTests of their property, and Respondents’ economic loss constitutes an abundant “injury in fact” to satisfy Article III. *See id.* StarTests cannot conduct its normal business activities because it is missing equipment. (R. at 2.) Likewise, the CFL is losing money because it cannot use the test results in accordance with its corporate model—namely, to determine how many CFL players use steroids. (R. at 3.) As a result, the FBI’s actions interfered with the CFL’s business model, constituting Respondents’ “injury in fact.”

Respondents also suffer from a non-economic injury. *See Havens*, 455 U.S. at 363. In *Havens*, this Court determined that HOME, a nonprofit organization committed to ensuring equal housing opportunities, had standing even though HOME’s injury stemmed from a non-economic

interest in providing open-housing. *Id.* at 363, 379. HOME alleged that Havens Realty Corporation discriminated against African-American renters, and thus Havens' actions impeded HOME's ability to counsel and refer low-income housing seekers. *Id.* at 379. Like HOME, Respondents have suffered a demonstrable injury, draining to Respondents' resources. *See id.* The CFL and StarTests told the players that their names and results would remain confidential and safely stored in StarTests' facilities. (R. at 1.) As a result of the government's intrusion, the CFL may be subject to subsequent suits, and those suits may cause discord within its organization, resulting in an unquantifiable injury to its operational harmony and good name in the media. As this Court articulated in *Lujan*, a litigant's interest can be as simple as a "desire to use or observe an animal species, even for purely aesthetic purposes." 504 U.S. at 562-63. Certainly if infringement on aesthetic interests constitutes an injury, the Respondents' property loss, exposure to liability, and the resulting friction between the organization and its players is a sufficient "injury in fact."

Additionally, the FBI's search and seizure caused Respondents' injury, and judicial adjudication can remedy the harm. For standing purposes, a plaintiff's injury must be "fairly traceable to the defendant's allegedly unlawful conduct and likely to be redressed by the requested relief." *Allen*, 468 U.S. at 751. In addition, the plaintiff's injury must be curable through judicial determination. *Id.* at 753 n.19. Here, the FBI's broad investigatory sweep into Respondents' databases caused Respondents' injury, thus undermining their agreement to keep the players' information confidential. (R. at 1.) Should the Court grant Respondents' Motion for Return of Property, it will lessen Respondents' injury because the results will return to StarTests' facilities where Respondents told the players the results would remain safely stored. (R. at 1.)

Thus, Respondents meet the Article III causation and redressibility requirements for standing.

See *Allen*, 468 U.S. at 751, 753 n.19.

a. The CFL satisfies the prudential standing requirements

Moreover, Respondents satisfy the prudential requirements for standing. See *Akins*, 524 U.S. at 20. This Court requires that in addition to the constitutional requirements of injury, causation, and redressibility, “the plaintiff . . . cannot rest his claim to relief on the legal rights or interests of third parties,” and individuals cannot assert a “generalized grievance shared in a substantially equal measure by all or a large class of citizens” as their injury for standing purposes. *Warth*, 422 U.S. at 499. Respondents’ injury is not a generalized grievance because the injury is particular to the Respondents and their players, and this Court only addresses the prohibition against generalized grievances in taxpayer standing cases. See *United States v. Richardson*, 418 U.S. 166 (1974); *Flast v. Cohen*, 392 U.S. 83 (1968); *Hein v. Freedom From Religion Foundation, Inc.*, 551 U.S. 587 (2007). Likewise, the CFL is not asserting the rights of the players by bringing this 41(g) Motion since the test results are its property. (R. at 10.)

b. Even if this Court finds that the CFL is standing in for the players, the CFL meets the *Singleton* exception to the ban on third party standing

However, even if this Court believes that the CFL is resting its case on the players’ rights, it still meets the requirements under the *Singleton v. Wulff* exception to the ban on third party standing. 428 U.S. 106, 114-16 (1976). Two factors weigh in favor of allowing third party standing: the closeness of the relationship between the litigant and the third party, and the third party’s ability to assert his or her own right. *Id.* In *Singleton*, even though doctors asserted their female abortion patients’ rights, this Court held that the doctors had standing because they suffered an economic loss when the government refused to pay the doctors’ bills. *Id.* at 117-18.

The doctors appropriately stood in for the patients because the women were unlikely to challenge the statute on their own due to privacy concerns. *Id.*

The CFL players are in a similar position as the female patients in *Singleton*, and the CFL is appropriately acting as their proxy. Like the patients who did not want to disclose their private medical information for fear of embarrassment or harassment, the players who tested positive for drug use will not want to reveal their identities to challenge the FBI's actions because to do so could jeopardize their careers and reputations. Moreover, the CFL shares a close relationship with its players like that seen in *Singleton*. In 2005, negative press coverage of the "steroid controversy" plagued professional sports. (R. at 8.) The players submitted to drug testing knowing that the CFL would use the percentage to determine whether it needed to conduct further testing. (R. at 1.) The CFL worked diligently to maintain its players privacy, and it hired StarTests to achieve this goal. Similar to the physicians in *Singleton*, the CFL will continue to suffer injury if the FBI does not return the property to StarTests, including a decrease in the players' willingness to play for the CFL. The CFL is the best party to advocate for the players because it has a financial and public relations interest in the return of the databases.

2. The CFL has standing to challenge the FBI's actions because it had a legitimate expectation of privacy in the things seized and the place searched

The CFL has standing to bring the Rule 41(g) Motion because the FBI's actions violated its rights under the Fourth Amendment. Fourth Amendment protection extends only to those with a legitimate expectation of privacy in both the area searched and the property seized. *Rakas v. Illinois*, 439 U.S. 128, 148-49 (1978); *see also United States v. Salvucci*, 448 U.S. 83, 93 (1980); *see also Rawlings v. Kentucky*, 448 U.S. 98, 104 (1980). Under this Court's jurisprudence, an individual with a legitimate expectation of privacy is one who exhibits an

actual subjective expectation of privacy that society objectively accepts as reasonable. *See Katz*, 389 U.S. at 361 (Harlan, J., concurring). When challenging the place searched, a party may have a “legally sufficient interest in a place other than his own home so that the Fourth Amendment protects him from unreasonable governmental intrusion into that place.” *Minnesota v. Olson*, 495 U.S. 91, 97-98 (1990).

The CFL had a subjective expectation of privacy in the test results. *See Katz*, 389 U.S. at 361 (Harlan, J., concurring). What one “seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.” *Katz*, 389 U.S. at 351. Respondents’ subjective expectation of privacy is similar to that which one has in a safety deposit box or public storage facility. *See United States v. Spilotro*, 800 F.2d 959, 962 (9th Cir. 1986) (holding that there is no question as to whether the defendant had standing to challenge the search of his safety deposit box); *see also United States v. Johnson*, 584 F.3d 995, 1001 (10th Cir. 2009) (explaining that “[p]eople generally have a reasonable expectation of privacy in a storage unit . . . because storage units are secure areas that command a high degree of privacy”) (quotations omitted). The CFL contracted with StarTests to store the results and maintain its players’ confidentiality, communicating its expectation that StarTests would keep the results private. (R. at 10.) Therefore, the CFL displayed a subjective expectation of privacy when it entrusted the test results to StarTests, a company specializing in sorting and storing this type of information, for safekeeping.

Moreover, society is prepared to accept the CFL’s expectation of privacy in the test results as reasonable. *Katz*, 389 U.S. at 361 (1967) (Harlan, J., concurring). StarTests repeated the “computer-hopping” procedure for every year it administered drug tests to the CFL players. (R. at 2.) Since the CFL hired StarTests in 2005, and the FBI did not execute its warrant until

2008, the CFL presumably knew and trusted StarTests' extensive confidentiality procedures. (R. at 7-8.) In *United States v. Dunn*, this Court determined that a defendant did not take reasonable precautions to protect his privacy interest in his barn because the barn was sixty feet away from his home, not surrounded by a fence, and officers could view inside the barn from an outside position. 480 U.S. 294, 303-05 (1987). Unlike *Dunn*, Respondents buried the test results in harddrives housed in a secure facility. (R. at 8.) The CFL and StarTests had a clear objective expectation of privacy that society is prepared to accept as reasonable because they took extensive measures consistent with protecting that expectation. See *Trulock v. Freeh*, 275 F.3d 391, 403 (4th Cir. 2001) (holding that the defendant's simple precaution of password-protecting his computer files sufficiently exhibited his legitimate expectation of privacy in the files).

In addition to having both a subjective and objective expectation of privacy in the items seized, the CFL has standing to challenge the place searched. *Rakas v. Illinois*, 439 U.S. 128, 148-49 (1978). Here, the CFL has more than a "legally sufficient" interest in StarTests' facilities. See *Olson*, 495 U.S. at 97-98. The CFL contracted with StarTests to safely store the results, and it only authorized StarTests to disclose the results for the very limited purpose of answering the media frenzy over drug use in professional football. (R. at 1.) The very nature of the StarTests and CFL contract displays the CFL's subjective expectation of privacy that StarTests would privately store its property. (R. at 1.) Moreover, certainly if society accepts that shutting the door behind oneself in a telephone booth is a reasonable precaution to prevent one's words from being broadcast to the world, *Katz*, 389 U.S. at 392, contracting with a company specializing in drug-testing and data storage to prevent dissemination of sensitive information is objectively reasonable. Thus, the CFL has a "legally sufficient" interest in StarTests' facilities to challenge the seizure of its own test results from that facility. See *Olson*, 495 U.S. at 97-98.

C. Rule 41(g) Is An Appropriate Remedy

Since the CFL has standing to bring the Rule 41(g) Motion, this Court must determine whether the return of property under 41(g) is “reasonable under all the circumstances.” *J.B. Manning Corp. v. United States*, 86 F.3d 926, 928 (9th Cir. 1996). The Ninth Circuit’s test, which the Fourteenth Circuit Court of Appeals applied below, weighs four factors to determine whether the 41(g) motion should be granted: “1) whether the government displayed a conscious disregard for the constitutional rights of the movant; 2) whether the movant has an individual interest in and need for the property he wants returned; 3) whether the movant would be irreparably injured by denying return of the property; and 4) whether the movant has an adequate remedy at law for the redress of his grievance.” *Ramsden v. United States*, 2 F.3d 322, 324-25 (9th Cir. 1993) (citing *Richey v. Smith*, 515 F.2d 1239, 1243-44 (5th Cir. 1975)). Additionally, the proper inquiry is not “whether the officers acted in good faith, but whether returning the illegally seized documents would be reasonable[] under the circumstances.” *J.B. Manning*, 86 F.3d at 928.

Respondents’ motion should be granted because the facts of this case all weigh in favor of return. First, the FBI displayed a conscious disregard for Respondents’ constitutional rights by affirmatively keeping information for which it admittedly lacked probable cause. (R. at 4.) The FBI now seeks to use that information in an investigation it conceived of only after it executed the warrant. (R. at 16.) Second, StarTests needs its equipment to run its business, and the CFL needs the results to assess the safety and state of its organization. Third, the CFL and StarTests will both be irreparably harmed if the information is not returned because both organizations’ reputations are at stake and both are subject to future litigation because of this

matter. (R. at 16.) Fourth, this Court can redress Respondents' harm by requiring the FBI to return the databases and computers. Thus, the Court should grant Respondents 41(g) Motion.

II. THE GOVERNMENT MAY NOT USE THE PLAIN VIEW DOCTRINE TO RIFFLE THROUGH PRIVATE INFORMATION IN DIGITAL EVIDENCE SEARCHES TO DEVELOP A CASE AGAINST ATTRACTIVE DEFENDANTS

A. The Plain View Doctrine Cannot Apply To Digital Evidence Seizures Because Executing Officers Misuse The Doctrine And Digital Evidence Requires A Unique Solution That Cannot Be Crafted From Traditional Criminal Procedure Exceptions To The Warrant Requirement

The plain view doctrine's application to digital evidence is an issue of first impression. (R. at 11.) As this Court's time-tested jurisprudence dictates, searches conducted without a warrant are *per se* unreasonable. *See Johnson v. United States*, 333 U.S. 10, 13-14 (1971). Under the warrant requirement, probable cause determinations must be made by a neutral and detached magistrate "instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime." *Id.* The plain view doctrine allows officers to seize fruits of a crime without a warrant. *Horton v. California*, 496 U.S. 128, 129 (1990). To properly invoke the plain view doctrine, the government must prove that the executing officer (1) was lawfully in a position from which to view the object seized in plain view; (2) the object's incriminating character was immediately apparent, meaning that the officer had probable cause to believe that the object was contraband or evidence of a crime; and (3) the officer had a lawful right of access to the object itself. *Coolidge v. New Hampshire*, 403 U.S. 433, 465 (1971).

1. Allowing the government to seize everything that comes into plain view during a digital evidence search gives officers unfettered discretion to seize everything they wish

If this Court allows law enforcement to rely on the plain view exception, private information that is “intermingled with seizable materials” is subjected to illegal government intrusion. *Comprehensive*, 579 F.3d at 998. As a consequence, law enforcement agencies would have the misappropriated discretion to transform a limited search for particular information into an overbroad search of office file systems and computer databases. *See id.* at 998. Accordingly, some circuits decline extending the plain view doctrine to digital evidence cases. *See United States v. Turner*, 169 F.3d 84, 88 (1st Cir. 1999) (rejecting the government’s claim that sexually explicit pictures on a computer were “fair game” because they were in “plain view” during a consensual search simply because the government suspected the defendant of a sex crime); *see also United States v. Carey*, 172 F.3d 1268, 1273 (10th Cir. 1999) (holding that child pornography on the defendant’s computer was not in plain view during a consensual search because officers had to open the files to determine whether each was relevant). Though access to computers is inane without access to the files therein, *United States v. Adjani*, 452 F. 3d 1140, 1152 (9th Cir. 2006), the government should not be able to penetrate the Fourth Amendment’s safeguards simply because it designed a search protocol where all information comes into plain view. Thus, this Court should find that the FBI cannot use the plain view doctrine to justify its actions because to do so would allow agents to circumvent the warrant requirement and access information that it does not otherwise have probable cause to search.

The agents’ actions in this case demonstrate why the plain view doctrine leaves too much discretion to executing officers. Here, the FBI expanded its investigation only after it “came across the test results of other CFL players who had tested positive for steroid use” while looking for information on the five players named in the warrant. (R. at 2.) However, because StarTests’ employees informed government agents that the company used a “computer hopping procedure”

as an additional and intentional means of protecting their clients' privacy, (R. at 2.) the agents were on notice that on-site inspection and isolation of the items listed in the warrant was impracticable. The government can "generally avoid violating fourth amendment rights by sealing and holding the documents pending approval by a magistrate of further search." *United States v. Tamara*, 694 F.2d 591, 595-96 (9th Cir. 1982). Rather than sealing and holding the items until further approval from a detached magistrate, government agents copied and viewed all of the private data. Nonetheless, the government now seeks to justify its unlawful behavior by shoehorning the illegally seized items under an exception to the warrant requirement that is incompatible with modern digital information.

2. The plain view doctrine has no practical application in digital evidence cases because digital data is distinct from the physical evidence that informed the plain view doctrine

Modern digital evidence is ubiquitous and cannot be searched and seized in the same way as traditional physical evidence. The Fourth Amendment framers did not contemplate the complexities of computers and digital evidence data. See Ray Chang, *Why the Plain View Doctrine Should Not Apply to Digital Evidence*, 12 Suffolk J. Trial & App. Advoc. 31, 32-33 (2007). Digital items are not the same "paper[s]" and "effects" that the framers considered, and digital storage media contain unending amounts of data. *Id.* For instance "[t]he School of Information Management and Systems at the University of California, Berkley, estimates that about five exabytes of new information, which is equivalent to 37,000 times the amount of information in the Library of Congress book collections, was created in 2002 alone. Of the five exabytes of new information created in 2002, 92% were created and stored on magnetic media, primarily computer hard disks." *Id.* Thus, digital evidence presents a unique problem with no

historical corollary, and this Court should consider innovative solutions that can encompass digital evidence's vast nature.

Moreover, the traditional criminal procedure rules do not work for digital evidence seizures. Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 Colum. L. Rev. 279, 300 (2005). Digital evidence seizures are unique because “[i]n many cases, computer hardware is merely a storage device for evidence rather than evidence itself.” *Id.* Here, the players’ positive urine samples were the actual evidence, yet the FBI had to seize the databases storing the results to get the evidence it wanted. (R. at 2.) Under traditional criminal procedure rules, seizing a container to obtain the information inside would seem overbroad— “[i]t’s roughly analogous to seizing an entire house and carting off its contents to mine them for evidence of a crime.” Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 Colum. L. Rev. 279, 300 (2005). The current rules on search and seizure, including the plain view doctrine, are appropriate for physical evidence seizures, but these rules leave officers with the strong temptation to conduct over-broad, off-site searches in digital evidence cases. *Id.* Rules such as the plain view doctrine do not adequately address digital evidence concerns, because “[i]f the government can’t be sure whether data may be concealed, compressed, erased or booby-trapped without carefully examining the contents of *every file . . . then everything* the government chooses to seize will automatically come into plain view.” *Comprehensive*, 579 F. 3d at 998 (emphasis added). Hence, digital evidence requires a new rule that is not dependant on physical evidence seizure principles.

In addition, arguments equating physical evidence to digital evidence are nonsensical because a computer search is in no way “tantamount to looking for documents in a file cabinet pursuant to a valid search warrant.” *See United States v. Carey*, 172 F.3d at 1273. “An object in

the physical world is discrete and is easily separable from the object's physical location, whereas digital data must be interpreted through machines because one bit looks much like another bit until a machine organizes it into something useful." Ray Chang, *Why the Plain View Doctrine Should Not Apply to Digital Evidence*, 12 Suffolk J. Trial & App. Advoc. 31, 35-36 (2007). For this reason, "[a]nalogies to other physical objects, such as dressers or file cabinets, do not often inform the situations [facing courts] . . . when applying search and seizure law." *United States v. Walser*, 275 F.3d 981, 986 (10th Cir. 2001). If this Court allows the government to rely on the plain view doctrine to justify its actions, then digital property warrants will be "transfor[med] into a species of de facto general warrants." Ray Chang, *Why the Plain View Doctrine Should Not Apply to Digital Evidence*, 12 Suffolk J. Trial & App. Advoc. 31, 32 (2007). Since digital evidence has no physical evidence equivalent, this Court should affirm the Fourteenth Circuit's determination that the plain view doctrine in digital searches and seizures "becomes an end around the Fourth Amendment warrant requirement." (R. at 12.)

B. Even If This Court Allows The Government To Rely On The Plain View Doctrine In Digital Evidence Seizures, The Government Cannot Meet The Doctrine's Requirements

Even if this Court finds that the plain view doctrine should apply in the digital evidence context, the government cannot make the requisite showing necessary to shoehorn its unlawful conduct into the plain view exception. *See Horton*, 496 U.S. at 144-45 (explaining that this Court will not use the plain view doctrine to "excuse officers from the general requirement of a warrant to seize if the officers know the location of the evidence, have probable cause to seize it, intend to seize it, and yet do not bother to obtain a warrant particularly describing that evidence"). Thus, "the problem with the 'plain view' doctrine has been to identify the circumstances in which plain view has legal significance rather than being simply the normal

concomitant of search, legal, or illegal.” *Id.* The government has not met the plain view doctrine’s three requirements.

1. The FBI cannot rely on the plain view doctrine because it did not view the players’ test results from a lawful vantage point

First, the agents did not lawfully view all of the players’ test results because the warrant was overbroad. The warrant has to be so specific so as “[prevent] the seizure of one thing under a warrant describing another,” and as to what officers may take “nothing is left to the discretion of the officer executing the warrant.” *Marron v. United States*, 275 U.S. 192, 196 (1927). A warrant is facially invalid if it fails to particularly describe the things to be seized, and a warrant executed that does not meet the particularity requirement violates the Fourth Amendment. *Groh v. Ramirez*, 540 U.S. 551, 552-60 (2004). The warrant in this case was overbroad and invalid because it authorized agents to seize “all” files relating to the CFL testing. (R. at 2.) Thus, the warrant did not particularly describing the place to be searched and the things to be seized. *Id.* at 552-60.

Second, the FBI exceeded the scope of Judge Leon’s warrant at the execution stage. *See Horton*, 496 U.S. at 140 (explaining that “[if] the scope of the search exceeds that permitted by the terms of a validly issued warrant . . . the subsequent seizure is unconstitutional without more”). The FBI’s objectives changed once its agents rummaged through all the players’ test results, after which they expanded their investigation into “all illegal drug possession and sale within professional football.” (R. at 2.) As such, the FBI exceeded the warrant’s scope because the agents’ actions were not related to the “objectives of the authorized intrusion.” *Wilson v. Layne*, 526 U.S. 603, 611 (1999). Additionally, although the agents entered StarTests’ Millerville facilities with a warrant, they did not limit their search to data “‘reasonably related to

the investigation into the five named players' illegal steroid use.'" (R. at 2.) As a result, the government cannot assert that it viewed the players' test results from a "lawful vantage point" when it discovered the other players' positive test results because its agents exceeded the discretion given to them in the warrant. *Comprehensive*, 579 F.3d at 998. Petitioners may argue that even if this Court finds that the warrant was facially invalid, the agents still viewed the players' test results from a lawful vantage point because of the good faith exception to the warrant requirement. *See United States v. Leon*, 468 U.S. 897, 922 (1984) (explaining that the government has not necessarily violated the Fourth Amendment when the executing officer relies in objective good faith "on the magistrate's probable cause determination and on the technical sufficiency of the warrant"). However, this Court applies the good faith doctrine as an exception to the exclusionary rule. *See id.* It follows that the government may not rely on the good faith exception here because a Rule 41(g) Motion is narrower than the exclusionary rule. *See Comprehensive*, 579 F.3d at 1001. Therefore, the government did not view all the CFL players' results from a lawful vantage point as this Court requires. *Horton*, 496 U.S. at 136.

2. The FBI has not met its burden under the plain view exception because the incriminating nature of the players' test results was not immediately apparent

The second plain view requirement that the incriminating nature of the evidence be "immediately apparent" is not met here. *See Coolidge*, 403 U.S. at 465. In *Arizona v. Hicks*, police officers lawfully entered the defendant's apartment. 480 U.S. 321, 321 (1987). Once inside, an officer noticed what appeared to be stolen stereo equipment, so he moved the stereo to see the serial number even though he was in the apartment investigating a crime unrelated to the stereo. *Id.* This Court held that the search of the stereo was unreasonable because the

investigating officer did not have probable cause to believe the equipment was evidence of a crime when he physically manipulated the stereo's position. *Id.* at 326-27.

Like the investigating officer in *Hicks* who had to move the stereo before he found incriminating information, the incriminating nature of the players' test results could not have been immediately apparent to the agents until they opened the files. StarTests utilized a "computer-hopping" system that separated the players' test results from their names and anonymous identification numbers. (R. at 8.) The FBI developed probable cause to investigate the remaining players only after agents rummaged through all of the databases in the weeks following the seizure. (R. at 9.) If the FBI came across a positive test result, agents would have no way of knowing whether that result made it "immediately apparent" that someone other than one of the original five players used drugs. In sum, the clear extra steps agents had to take to view the players' results make it impossible that the results' incriminating nature was immediately apparent. Furthermore, the agents extended their search only after riffling through all the results, (R. at 3.) which truly weighs in favor of this Court finding that the results' incriminating nature was not immediately apparent.

3. The FBI has not met the plain view exception's requirements because it did not have lawful access to seize the remaining players' test results

The investigating agents similarly did not have lawful access to the seizable objects. *See Coolidge*, 403 U.S. at 465. The warrant mandated that agents specially trained in searching computer data had to mark non-seizable materials for return to StarTests. (R. at 4.) The warrant directed agents trained in searching computer data to designate for return information that the warrant did not authorize the agents to seize. (R. at 2.) Here, the agents possessed the test results for over a week. (R. at 9.) In that time, the agents could have easily obtained a warrant after they

realized the number of positive tests exceeded the number of players for whom they had probable cause. This Court clearly prefers that a neutral and detached magistrate make probable cause determinations whenever practicable. See *Horton*, 496 U.S. at 143; *Leon*, 468 U.S. at 944; *Johnson*, 333 U.S. at 68; *South Dakota v. Opperman*, 428 U.S. 364, 384 (1976) (Powell, J., concurring); *Gerstein v. Pugh*, 420 U.S. 103, 112 (1975); *Shadwick v. City of Tampa*, 407 U.S. 345, 350 (1972); *Coolidge*, 403 U.S. at 450 (explaining that prosecutors and policemen simply cannot maintain neutrality with regard to their own investigations). The agents did not lawfully seize the remaining players' results because they retained the results without a warrant authorizing them to do so. (R. at 9.) Thus, this Court should find that the agents' search was unreasonable because the government has not met its burden under the plain view exception to the warrant requirement and since the agents should have sought a second warrant.

C. This Court Should Not Allow The Government To Rely On The Plain View Doctrine When It Blatantly Disregarded Respondents' Fourth Amendment Rights

The government should not be able to use the plain view doctrine as a justification for their actions. Judge Leon's warrant only authorized agents to search for the test results of the five named players. (R. at 1-4.) Nonetheless, the government unilaterally and without the permission of a detached and neutral magistrate, decided to expand its investigation, and it based this decision on evidence it obtained in violation of Judge Leon's warrant. (R. at 2.) Hence, the FBI twisted "authorization to search *some* computer files" into "authorization to search *all* files in the same subdirectory, and all files in an enveloping directory, a neighboring hard drive nearby computer or nearby storage media." *Comprehensive*, 579 F.3d at 1005 (emphasis added). This court should not allow officers to rely on the plain view doctrine for evidence "inadvertently" discovered when the agents so flagrantly ignored Judge Leon's directions.

III. THIS COURT SHOULD EMBRACE THE GUIDELINES THAT BOTH THE NINTH AND FOURTEENTH CIRCUITS ADOPTED TO HEIGHTEN THE PARTICULARITY REQUIREMENT FOR DIGITAL EVIDENCE WARRANTS

A. Heightening The Particularity Requirement For Digital Evidence Warrants Is Consistent With The Framers' Intent

The Fourth Amendment to the United States Constitution provides that the people have a right to be “secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” U.S. Const. amend. IV. This right “shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and *particularly* describing the *place to searched*, and the *persons or things to be seized*.” U.S. Const. amend. IV (emphasis added). Accordingly, “[t]he point of the Fourth Amendment” warrant requirement is not to “deny law enforcement the support of the usual inferences which reasonable men draw from evidence,” but rather to protect individuals by “insist[ing] that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.” *Johnson*, 333 U.S. at 13-14.

1. The framers' primary concern when drafting the Fourth Amendment was to prevent the issuance of general warrants

In the broadest sense, “the Fourth Amendment’s commands grew in large measure out of the colonists’ experience with the writs of assistance and their memories of the general warrants formerly in use in England.” *United States v. Chadwick*, 433 U.S. 1, 7-8 (1977). Agents of the Crown used general warrants to forcibly enter homes and search for evidence relating to seditious activities. Osmond K. Fraenkel, *Concerning Searches and Seizures*, 34 Harv. L. Rev. 361, 362-63 (1921). While the framers enacted the Fourth Amendment to guard against more than just such specific abuses, the framers mostly pushed for the Fourth Amendment to prevent magistrates from issuing general warrants. *See Weeks v. United States*, 232 U.S. 383, 391-92

(1914) (asserting that the “[Fourth] Amendment put the courts of the United States and Federal officials in the exercise of their power and authority, under limitations and restraints”); *see also Steagald v. United States*, 451 U.S. 204, 220 (1981) (explaining that the framers strongly objected to colonial writs of assistance and general warrants that “provided no judicial check on the determination of the executing officials that the evidence available justified an intrusion into any particular home”). Consequently, the framers reacted to the outrages and abuses they experienced under British rule by drafting the Fourth Amendment and expressly incorporating the particularity requirement therein. Samantha Trepel, *Digital Searches, General Warrants, and the Case for the Courts*, 10 Yale J. L. & Tech. 120, 123 (2007).

Warrants must sufficiently describe the “place to be searched” so that executing officers can reasonably identify any seizable item’s location through reasonable efforts. *Steele v. United States*, U.S. 498, 503 (1925). The warrant must describe the “things to be seized” with enough particularity that “seizure of one thing under a warrant describing another” cannot arise, and so that “[a]s to what is to be taken, nothing is left to the discretion of the officer executing the warrant.” *Marron*, 275 U.S. at 196. As such, “searches conducted outside the judicial process, without prior approval by judge or magistrate are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.” *Katz*, 389 U.S. at 357. The particularity requirement, by limiting where law enforcement can search, “ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.” *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

2. Judge Leon’s warrant runs afoul of the framers’ particularity requirement

Judge Leon's warrant closely resembles the general warrants that the framers abhorred because it left too much discretion to the government agents executing the search. *See Johnson*, 333 U.S. at 13-14; *see also United States v. Vitek Supply Corp.*, 144 F.2d 476, 481 (7th Cir. 1998) (quoting *Coolidge*, 403 U.S. at 467 (explaining that "[t]he particularity requirement precludes the issuance of a warrant that permits a 'general exploratory rummaging in a person's belongings'")). The warrant must "name the particular property that the police have probable cause to believe will be located in the particular place to be searched." *Garrison*, 480 U.S. at 84. The warrant in this instance was overbroad because it authorized the lead agent to make a decision, *after* the search began, to have the agents remove all transportable equipment. (R. at 2, 8.) Moreover, Judge Leon's warrant resembles a general warrant because it authorized agents to seize "all computer records, files, and equipment" related to the CFL testing. (R. at 1, 2.) A warrant is overbroad with the use of the word "all" because it encourages officers to seize "all computer records/data without regard to the . . . subject matter." *See In re Search Warrant for K-Sports Imports, Inc.*, 163 F.R.D. 594, 596 (C.D. Cal. 1995). Thus, Judge Leon's warrant is the epitome of a general warrant because it left too much discretion to the executing officers and allowed for the wholesale seizure of "all" the testing data rather than particularly describing the items to be seized.

Warrants that leave officers broad discretion to search and seize unspecified items of digital data diminish the "regulatory effect of the particularity requirement." Orin S. Kerr, *Searches and Seizures in a Digital Evidence World*, 119 Harv. L. Rev. 531, 568 (2005). Broad digital evidence warrants create a "serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." *Comprehensive*, 579 F. 3d at 1004. While general warrants certainly make it easier for officers

to search for evidence of a crime, Fourth Amendment jurisprudence does not allow using the difficulty of executing a search warrant as a justification for loosening the warrant requirement. *See Vale v. Louisiana*, 399 U.S. 30, 34-35 (1969) (holding that the government cannot justify a warrantless search by arguing it is too time consuming to obtain a warrant). Thus, this Court should not allow federal magistrates to issue warrants authorizing the government to seize all files for later searching in digital evidence cases because to do so could “swallow the warrant requirement itself.” *Ybarra v. Illinois*, 444 U.S. 85, 104 (1979) (Rehnquist dissenting).

3. This Court heightens Fourth Amendment protection when necessary to protect American citizens from unreasonable searches and seizures

This Court heightens Fourth Amendment protection and places specific limitations on law enforcement officials when necessary to protect American citizens’ rights. *See Tennessee v. Gardner*, 471 U.S. 1, 11 (1985) (holding that the use of excessive force to stop a fleeing felon is constitutionally unreasonable). Particularly, this Court articulated that a higher than normal justification may be necessary in especially intrusive situations. *See Schmerber v. California*, 384 U.S. 757, 769-70 (1966) (holding that officers needed a clear indication that they would find evidence of an alleged crime to justify extracting blood from a suspect). For instance, when the government sought permission to use an invasive surgery to extract a bullet from a suspect, this Court held that the government must provide a “more substantial” than ordinary justification to “intrude upon an area in which our society recognizes a significantly heightened privacy interest.” *Winston v. Lee*, 470 U.S. 753, 760 (1985). Thus, heightening the particularity requirement in digital evidence searches is a natural progression from this Court’s previous holdings applying heightened scrutiny to a litigant’s interest in his or her bodily fluids.

B. The Test For Digital Evidence Warrants From *Comprehensive Drug Testing* And Its Progeny Is Consistent With The Fourth Amendment's Particularity Requirement

The Ninth Circuit laid out guidelines in *Comprehensive Drug Testing* for district courts to follow when evaluating digital evidence warrants. 579 F.3d at 1009. First, “magistrates should insist that the government waive reliance upon the plain view doctrine in digital evidence cases.” *Id.* at 1006. Second, either “specialized personnel or an independent third party” must segregate and redact the responsive and non-responsive data. *Id.* If the government wants to use its own personnel to segregate, “it must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant.” *Id.* Third, “[w]arrants and subpoenas must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other judicial fora.” *Id.* Fourth, “[t]he government’s search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents.” *Id.* Finally, “[t]he government must destroy or, if the recipient may lawfully possess it, return non-responsive data, keeping the issuing magistrate informed about when it has done so and what it has kept.” *Id.*

1. The *Comprehensive* guidelines uphold the sanctity of the Fourth Amendment

The *Comprehensive* test ensures that officers apply for and execute search warrants in a manner that upholds the Fourth Amendment requirement that the government’s warrants particularly list the “things to be seized.” *See* U.S. Const. amend. IV. The Ninth Circuit’s test states that if the warrant requires agents to separate seizable data from non-seizable data when searching, the process used to do so must be designed to achieve that end. *Comprehensive*, 579

F.3d at 999. For instance, the government has at its disposal “sophisticated hashing tools” that allow it to identify the clearly illegal files from the non-illegal. *Id.* The *Comprehensive* test ensures that “[t]hese and similar tools may not be used without specific authorization in the warrant, and such permission may only be given if there is probable cause to believe that such files can be found on the electronic medium to be seized.” *Id.* Thus, the *Comprehensive* test more than satisfies the Fourth Amendment requirement that warrants “particularly describ[e] the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV.

2. Courts validating broad warrants face distinguishable facts from the case at bar and do not give enough credence to the particularity requirement

Some courts with facts seemingly similar to this case uphold broad warrants for digital evidence searches. *See United States v. Lamb*, 945 F. Supp. 441, 463 (N.D.N.Y. 1996) (holding that a warrant authorizing officers to search all stored files on the suspect’s computer for evidence of child pornography satisfied the Fourth Amendment’s particularity requirement); *see also United States v. Lacy*, 119 F.3d 742, 746 (9th Cir. 1997) (upholding a generic warrant that allowed officers to seize the defendant’s entire computer system for a later child pornography search because “a more precise description [was] not possible”). Courts that allow officers to seize and search both responsive and non-responsive data in digital evidence seizures site the proposition that it is “unreasonable” or “impracticable” to require specificity in certain cases. *See Lamb*, 945 F. Supp. at 463; *see also Lacy*, 119 F.3d at 746.

However, this case is distinguishable from cases upholding broad warrants that authorize wholesale seizure of digital evidence for later off-site relevance determinations. First, this case is not analogous to a seizure from a single party’s residence. The FBI seized almost every computer in StarTests’ facilities. (R. at 2.) The sheer enormity of the FBI’s investigation,

coupled with the fact that agents knew they investigated incriminating results beyond the warrant's scope, should persuade this Court to reject the government's argument that it was "unreasonable" or "impracticable" for its agents to act differently. Second, unlike seizing "contraband" from a suspect's home where law enforcement deprives the individual of information he cannot legally possess, the FBI's actions deprived StarTests of its vitality by depleting the infrastructure it uses to run its business and possibly dissuading potential clients from using StarTests' services in the future. Third, an individual possessing pornography has every incentive to destroy the evidence in his possession once he knows that he is under investigation, but StarTests has no such incentive because the evidence itself does not subject StarTests to criminal liability. Thus, this case is distinguishable from digital evidence seizure cases where broad warrants appear reasonable.

Moreover, courts allowing broad warrants for digital evidence seizures do not give enough thought to the particularity requirement. Since an officer with a warrant authorizing him to search for and seize a rifle must cease once he finds a rifle, it corresponds that an officer searching for incriminating evidence in the digital evidence context must cease once he comes across the evidence named in the warrant. *See Coolidge*, 403 U.S. at 517. Courts point out that this is especially difficult given the problems inherent in seizing digital evidence. *See generally United States v. Adjani*, 452 F.3d 1140 (9th Cir. 2006); *United States v. Raney*, 342 F.3d 551, 559 (7th Cir. 2003); *United States v. Alexander*, 574 F.3d 484 (8th Cir. 2009). In this case, there is no way to verify if the unsupervised FBI agents found the information they needed on the five players, but nonetheless continued searching for additional incriminating information, this Court should require the government to follow stricter guidelines such as those in *Comprehensive* when seeking digital evidence warrants.

Additionally, this case's facts elucidate why courts should strictly adhere to the particularity requirement in digital evidence warrant cases. Digital data's complexities significantly increase the temptation for agents to engage in general searches. Orin S. Kerr, *Searches and Seizures in a Digital Evidence World*, 119 Harv. L. Rev. 531, 568 (2005). Once a computer hard-drive is in government custody, the government can easily search all the data within, "com[ing] into possession of evidence by... willfully disregarding limitations in [the] search warrant." *Comprehensive*, 579 F.3d at 1003. Agents here acted on the temptation to disregard the warrant, expanding their investigation to include all drug use in professional football *after* gaining access to the other players' information. (R. at 9.) "When the government comes into possession of evidence by circumventing or willfully disregarding limitations in a search warrant, it must not be allowed to benefit from its own wrongdoing by retaining the wrongfully detained evidence or any fruits thereof." *Comprehensive*, 579 F.3d at 1003. Therefore, given the added enticement for officers to bend Fourth Amendment protections, courts must give credence to the particularity requirement when evaluating digital evidence warrants.

C. The Particularity Requirement's Role In Digital Evidence Warrants Is Not a Job For The Legislature

1. This Court may properly heighten the particularity requirement in digital evidence cases because it is the definitive interpreter of the constitution

This Court is the definitive interpreter of the Constitution. *Williams v. United States*, 401 U.S. 667, 697-98 (1971) (Harlan, J., concurring). This Court must interpret what becomes of the particularity requirement in digital evidence cases just as it constructed rules for criminal procedure situations that the founders did not contemplate. *See Carroll v. United States*, 267

U.S. 132, 153-54 (1925) (creating an exception to the warrant requirement for vehicle searches when the officer has probable cause to believe that the vehicle contains evidence of a crime and the vehicle is stopped on a highway); *see also Illinois v. Rodriguez*, 497 U.S. 177, 181 (1990) (authorizing warrantless entry into a residence when a person with “apparent authority” consents to the entry); *see also Gardner*, 471 U.S. at 12 (holding that “[t]he use of deadly force to prevent the escape of all felony suspects, whatever the circumstances, is constitutionally unreasonable”). Moreover, this Court created the plain view doctrine. *See Horton*, 496 U.S. at 134. It is only natural that this Court revisits the plain view doctrine as it relates to the new area of digital evidence and the particularity requirement for warrants. Thus, this Court should craft the parameters governing warrants for digital evidence searches since it falls within this Court’s expertise—interpreting the Constitution of the United States. In doing so, this Court should follow the Ninth Circuit’s well-reasoned holding and affirm the Fourteenth Circuit’s guide for tailoring search warrants in digital evidence cases. (R. at 17.)

2. The legislature’s recent amendments to the Federal Rules of Criminal Procedure do not adequately address the unique problems inherent in digital evidence seizures

In its December 1st, 2009 amendments to the Federal Rules of Criminal Procedure, the legislature included an inadequate provision governing digital evidence warrants. *See* FED. R. CRIM. P. 41(e)(2)(B). The rule provides that magistrates “may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information.” *Id.* The warrant may “[authorize] a later review of the media or information consistent with the warrant.” *Id.* This rule is incredibly vague because it does not define under what circumstances the government may seize data for a later search, and it places no limitations on what the government may do with the data after the seizure occurs. The ambiguities inherent in Rule

41(e) threaten the Fourth Amendment’s effectiveness and necessitate this Court’s involvement.

Moreover, the judiciary is in a better position than the legislature to establish clear guidelines for officers investigating digital evidence cases. First, the judiciary makes its determinations free from interest groups’ influence. Donald A. Dripps, *Criminal Procedure, Footnote Four, and the Theory of Public Choice; Or Why Don’t Legislatures Give a Damn About the Rights of the Accused?*, 44 Syracuse L. Rev. 1079, 1100 (1993). For instance, “[l]egislators pressed to do something about crime, but constrained by budget priorities, can dilute the rights of the accused without any real inquiry into whether actual crime control benefits will accrue.” *Id.* at 1095. Additionally, courts have a more pronounced role in shaping criminal procedure rules. *Id.* Therefore, this Court, as the definitive interpreter of the constitution, should determine the level of particularity required for digital evidence warrants.

D. The Government Has Not Met The Five Requirements Of The Comprehensive Test

This government did not comply with the *Comprehensive* guidelines adopted for digital evidence warrants. First, the government did not forswear reliance on the plain view doctrine because it used the plain view doctrine to justify its actions to the District Court. (R. at 4.) Second, the government’s computer agents must have disclosed information “other than that which [was] the target of the warrant.” *See Comprehensive*, 579 F.3d at 991. “Computer forensics agents” uncovered the test results for the five players, but also came across the test results for the other players. (R. at 2.) After learning that the “computer forensics agents” found information on more than the five players named in the warrant, the FBI decided to expand its investigation. (R. at 2.) Therefore, the “computer forensics agents” did share the players

constitutionally protected information with the rest of the FBI, so the government cannot meet *Comprehensive's* second prong. See *Comprehensive*, 579 F.3d at 999.

Third, the record does not have enough information to determine whether the FBI's warrant "disclose[d] the actual risks of destruction or concealment of information, as well as prior efforts to seize that information in other courts." *Comprehensive*, 579 F.3d at 1009.

Fourth, the FBI's "search protocol [was not] designed to uncover only the information for which it [had] probable cause, and that information may be examined by non-computer personnel agents." *Id.* The process employed here whereby the agents broadly combed through all the databases, "inadvertently" stumbling upon constitutionally protected information, was not designed to uncover only information for which the government had probable cause. See *id.*

Fifth, "the government [did not] destroy, or, if the [Respondents could] lawfully possess it, return non-responsive data." *Comprehensive*, 579 F.3d 1009. StarTests may lawfully possess the test results since the results in and of themselves are not illegal. The FBI has not returned the non-responsive data to StarTests; indeed, the FBI's failure to return the evidence is the subject of this litigation. (R. at 1.)

In sum, the FBI did not come close to the bar set in *Comprehensive*. 579 F.3d at 1006. Unlike suppression at trial, the primary purpose of Rule 41(g) is to assist "those whose property or privacy interests are impaired by the seizure." *Id.* at 1002. The existence of Rule 41(g) demonstrates society's inherent understanding that individual privacy and property should not be subject to the whims of overzealous officers. Granting Respondent's 41(g) motion for failure to comply with the *Comprehensive* criteria upholds the purpose of the Fourth Amendment and remedies the gap between law and practice that arises in digital evidence cases.

CONCLUSION

Respondents respectfully request that this Court affirm the Fourteenth Circuit's holding by heightening the particularity requirement in digital evidence cases and forbidding the government from relying on the plain view doctrine during digital evidence seizures.