

No. 2009-H20

IN THE
Supreme Court of the United States

UNITED STATES OF AMERICA,
Petitioners,

v.

STARTESTS, INC.,
AND THE COLONIAL FOOTBALL LEAGUE,
Respondent.

*ON WRIT OF CERTIORARI TO THE
U.S. CIRCUIT COURT OF APPEALS FOR THE FOURTEENTH CIRCUIT*

BRIEF FOR PETITIONER

SPONG COMPETITION NUMBER: 11

QUESTION PRESENTED

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

TABLE OF CONTENTS

QUESTION PRESENTED..... ii

TABLE OF CONTENTS..... iii

TABLE OF AUTHORITIES v

OPINIONS BELOW 2

CONSTITUTIONAL PROVISIONS, STATUTES, AND FEDERAL RULES INVOLVED 2

STATEMENT OF THE CASE..... 2

 I. The Search of StarTests’s Facility 3

 II. The Lower Courts’ Decisions 4

SUMMARY OF THE ARGUMENT 5

ARGUMENT 10

 I. The CFL lacks standing to file a FED. R. CRIM. P. 41(g) motion on behalf of its players because the CFL was not a "person aggrieved" by the search and seizure of individual football players’ drug testing records and none of its members, the franchises, would have standing to sue individually 10

 a. The CFL was not the victim of the search of StarTests’s facility or the seizure of the individual players’ records 10

 b. The CFL’s members, the franchises, did not suffer an injury that would allow them to bring suit in their own right..... 12

 II. Federal magistrates may issue warrants authorizing the government to seize all computer equipment and files for an off-site search when such warrants are sufficiently particular and an on-site search of the digital evidence is impractical and overly intrusive..... 14

 a. The warrant in this case was sufficiently particular because the warrant contained instruction that focused the FBI agents’ search on information regarding the five players’ illegal use of steroids 15

 b. The seizure of all computer records, data, and equipment followed by an off-site search was necessary for the government to find the data for which it had probable cause and to avoid a more intrusive and lengthy on-site search .. 19

 i. The massive amount of data, risk of deceptive file labeling, and lack of necessary software on-site to search StarTests’s databases necessitated the seizure of all computer records, files, and equipment to cover the material for which the government had probable cause 20

ii.	<u>The off-site search was reasonable because StarTests’s files relating to the drug-testing program were massive and its “computer-hopping” file storage procedure made an on-site search nearly impossible</u>	24
III.	<u>Applying the plain view doctrine in a digital search context satisfies the Fourth Amendment’s reasonableness test where the searching officer saw the test results targeted by the warrant in the same file as positive test results for illegal substances</u>	28
a.	<u>The FBI satisfied the plain view doctrine’s requirements when it retained records showing illegal drug use where those records were from a database Magistrate Judge Leon’s warrant authorized the FBI to seize and search</u>	28
b.	<u>The District Court correctly found that the plain view doctrine applied where the incriminating data seized and the data targeted by the warrant were located immediately next to each other in the same database</u>	29
IV.	<u>Contrary to Fourth Amendment precedent, the Court of Appeals’ rules grant magistrate judges the power to prevent searches justified by probable cause and require the government to spend additional time and money on each electronic search case, and therefore such restrictions are best left to the Federal Rules of Criminal Procedure</u>	31
	CONCLUSION.....	34

TABLE OF AUTHORITIES

United States Supreme Court Cases

<u>Alderman v. United States,</u> 394 U.S. 165 (1969).....	11
<u>Andresen v. Maryland,</u> 427 U.S. 463 (1976).....	15
<u>Brigham City v. Stuart,</u> 547 U.S. 398 (2006).....	29
<u>Cady v. Dombrowski,</u> 413 U.S. 433 (1973).....	19
<u>Coolidge v. New Hampshire,</u> 403 U.S. 443 (1971).....	14, 15
<u>Dalia v. United States,</u> 441 U.S. 238 (1979).....	31, 32
<u>Ex Parte United States,</u> 287 U.S. 241 (1932).....	32
<u>Horton v. California,</u> 496 U.S. 128 (1990).....	22, 27, 28, 30
<u>Hunt v. Wash. State Apple Adver. Comm’n,</u> 432 U.S. 333 (1977).....	12
<u>Illinois v. Gates,</u> 462 U.S. 213 (1983).....	14, 16
<u>Jones v. United States,</u> 362 U.S. 257 (1960).....	11
<u>Lujan v. Defenders of Wildlife,</u> 504 U.S. 555 (1999).....	13
<u>Ohio v. Robinette,</u> 519 U.S. 33 (1996).....	29
<u>Rakas v. Illinois,</u> 439 U.S. 128 (1978).....	10, 11, 12
<u>Singleton v. Wulff,</u> 428 U.S. 106 (1976).....	10
<u>Steel Co. v. Citizens for a Better Env’t,</u> 523 U.S. 83 (1998).....	34
<u>United States v. Grubbs,</u> 547 U.S. 90 (2006).....	32
<u>United States v. Ross,</u> 456 U.S. 798 (1982).....	20
<u>United States v. Sharpe,</u> 470 U.S. 675 (1985).....	19
<u>United States v. Ventresca,</u> 380 U.S. 102 (1965).....	16
<u>Vernonia Sch. Dist. 47J v. Acton,</u> 515 U.S. 646 (1995).....	32
<u>Warth v. Seldin,</u> 422 U.S. 490 (1975).....	10

United States Court of Appeals Cases

<u>Davis v. Gracey,</u> 111 F.3d 1472 (10th Cir.1997)	22
<u>Guest v. Leis,</u> 255 F.3d 325 (6th Cir. 2001)	15, 21, 24
<u>United States v. Abrams,</u> 615 F.2d 541 (1st Cir.1980).....	18, 22
<u>United States v. Adjani,</u> 452 F.3d 1140 (9th Cir. 2006)	16, 18, 20, 21, 29
<u>United States v. Beusch,</u> 596 F.2d 871 (9th Cir. 1979)	29, 31
<u>United States v. Carey,</u> 172 F.3d 1268 (10th Cir. 1999)	16, 22, 28, 30
<u>United States v. Comprehensive Drug Testing, Inc.,</u> 513 F.3d 1085 (9th Cir. 2008)	12, 13
<u>United States v. Comprehensive Drug Testing, Inc.,</u> 579 F.3d 989 (9th Cir. 2009)	12, 24, 27, 31
<u>United States v. Dichiarinte,</u> 445 F.2d 126 (7th Cir. 1971)	28
<u>United States v. Frost,</u> 125 F.3d 346 (6th Cir. 1997)	18
<u>United States v. Giberson,</u> 527 F.3d 882 (9th Cir. 2008)	29
<u>United States v. Gracey,</u> 111 F.3d 1472 (10th Cir. 1997)	17, 18
<u>United States v. Hargus,</u> 128 F.3d 1358 (10th Cir. 1997)	20, 26
<u>United States v. Hay,</u> 231 F.3d 630 (9th Cir. 2000)	22
<u>United States v. Henson,</u> 848 F.2d 1374 (6th Cir. 1988)	19, 25
<u>United States v. Hill,</u> 459 F.3d 966 (9th Cir.)	16, 21, 25, 26, 30
<u>United States v. Kimbrough,</u> 69 F.3d 723 (5th Cir. 1995)	16, 17, 22, 26
<u>United States v. Kow,</u> 58 F.3d 423 (9th Cir.1995)	22
<u>United States v. Mann,</u> 389 F.3d 869 (9th Cir. 2004)	16
<u>United States v. Raney,</u> 342 F.3d 551 (7th Cir. 2003)	28
<u>United States v. Schandl,</u> 947 F.3d 462 (11th Cir. 1991)	16, 26
<u>United States v. Spilotro,</u> 800 F.2d 959 (9th Cir. 1986)	16
<u>United States v. Summage,</u> 481 F.3d 1075 (8th Cir. 2007)	15, 16, 22, 25, 26
<u>United States v. Tamura,</u> 694 F.2d 591 (9th Cir. 1982)	16, 22, 30, 32

<u>United States v. Upham</u> , 168 F.3d 532 (1st Cir. 1999).....	15, 17, 20, 24
--	----------------

United States District Court Cases

<u>Gutman v. Klein</u> , No. 03 Civ. 1570, 2008 U.S. Dist. LEXIS 92398 (E.D.N.Y. Oct. 15, 2008)	33
<u>Gutman v. Klein</u> , No. 03 Civ. 1570, 2008 U.S. Dist. LEXIS 97707 (E.D.N.Y. Dec. 1, 2008).....	33
<u>United States v. Hill</u> , 322 F. Supp. 2d 1081 (C.D. Cal. 2004)	30

Federal Rules

FED. R. CRIM. PRO. 41	11, 19, 24, 33
FED. R. EVID. 1001	31
FED. R. EVID. 1002	31
FED. R. EVID. 1003	31

Federal Statutes

21 U.S.C. § 812 (2009)	29
21 U.S.C. § 844 (2009)	29

Other Authorities

Letter from Karen L. Strombom, Chief United States Magistrate Judge, W.D. Wash., to Robert Westinghouse, Assistant U.S. Attorney (Oct. 1, 2009).....	33
Mark Conrad, <u>The Business of Sports: A Primer for Journalists</u> (Lawrence Erlbaum Associates, Inc., 2005)	13
Orin S. Kerr, <u>Searches and Seizures in a Digital World</u> , 119 Harv. L. Rev. 531, 543-47 (2005)	33

IN THE
Supreme Court of the United States

UNITED STATES OF AMERICA,
Petitioners,

v.

STARTESTS, INC.,
AND THE COLONIAL FOOTBALL LEAGUE,
Respondent.

*ON WRIT OF CERTIORARI TO THE
U.S. CIRCUIT COURT OF APPEALS FOR THE FOURTEENTH CIRCUIT*

BRIEF FOR PETITIONER

OPINIONS BELOW

The decision of the U.S. Circuit Court of Appeals for the Fourteenth Circuit is contained in the record. (R. at 7.) The decision of the U.S. District Court for the District of Wythe is also contained in the record. (R. at 1.)

CONSTITUTIONAL PROVISIONS, STATUTES, AND FEDERAL RULES INVOLVED

Rule 41 of the Federal Rules of Criminal Procedure provides in pertinent part:

(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.

The Fourth Amendment to the United States Constitution provides:

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.

STATEMENT OF THE CASE

Respondents StarTests, Inc. (“StarTests”) and the Colonial Football League (“CFL”) instituted this action by filing a motion under FED. R. CRIM. P. 41(g), requesting that the Federal Bureau of Investigation (“FBI”) return all copied records of CFL players’ drug test results as well as all seized computer equipment that was used to store those test results, except for the records of the five players the FBI had probable cause to believe were using illegal steroids. (R. at 1-3.) The U.S. District Court for the District of Wythe (“District Court”) held that the FBI had a valid warrant to search for the drug testing records of the five players and that the plain view

doctrine justified the FBI's seizure of drug testing records of athletes not named in the affidavit. (R. at 6.) Respondents appealed to the U.S. Circuit Court of Appeals for the Fourteenth Circuit ("Circuit Court"), which reversed the District Court. (R. at 7.) The Circuit Court adopted new standards for the issuance of warrants in digital evidence cases based on United States v. Comprehensive Drug Testing, 579 F.3d 989 (9th Cir. 2009) (en banc). (R. at 14-15.) The Circuit Court also banned the government from relying on the plain view doctrine in digital evidence cases, requiring it to submit any intermingled digital files to a court-supervised third party for sorting. (R. at 13.) The main issues in this case are whether the government may use the plain view doctrine in digital evidence cases and whether the Circuit Court's guidelines for warrants in digital evidence cases comport with the Fourth Amendment.

I. The Search of StarTests's Facility.

The CFL began to require its players to submit to drug testing in 2005. (R. at 8.) The testing was instituted to ensure that the CFL was complying with federal and state laws, as well as its own athletic performance standards. (R. at 1.) The CFL hired StarTests, an independent drug-testing agency, to administer the drug tests to the CFL players. (R. at 1.) To encourage participation in the drug-testing program, the CFL and StarTests represented to the CFL players that the drug tests were solely to determine if five percent or more of CFL's players would test positive for illegal steroids. (R. at 1.) If the five percent threshold were exceeded, more drug testing would be done in the future. (R. at 1.) The CFL players were assured that their names and test results would remain confidential and that only the percentage would be released to the public. (R. at 1.)

In 2008, intense media scrutiny began to build around the usage of steroids in the CFL. (R. at 7.) This scrutiny prompted the FBI to open an investigation in July of 2008 into the

distribution and usage of steroids amongst professional athletes. (R. at 7.) After months of investigation, the FBI probe began to focus on five CFL players who it believed were major distributors and users of illegal steroids. (R. at 7.) After collecting eyewitness reports and taped conversations, the FBI developed probable cause to believe that the five players had tested positive for steroid usage in the StarTests administered drug-testing program. (R. at 1, 7.)

The FBI applied for a search warrant to seize the test results of the five players from the StarTests facility in Millersville, Wythe along with “all computer records, files, and equipment” located at the Millersville facility that were related to the CFL’s StarTests-administered drug testing program. (R. at 8.) The FBI filed a supporting affidavit that gave three reasons to justify the request: (1) the data to be retrieved is massive in quantity, (2) some file names may be deceptively labeled, and (3) the software required to read the test results may not be installed on StarTests’s computers. (R. at 2.) Magistrate Judge Leon issued a warrant that authorized the FBI to search “computer equipment, storage devices, and, where an on-site search would be impracticable, seizure of either a copy of all data or the computer equipment itself.” (R. at 2.)

Magistrate Judge Leon placed three restrictions on the search: (1) “law enforcement personnel trained in searching and seizing computer data” were to determine whether a computer or other equipment needed to be seized; (2) if computers or other equipment were seized, “appropriately trained personnel” were to then review the data, retaining the information authorized by the warrant and returning information not authorized by the warrant; and (3) only information “reasonably related to the investigation into the five named players’ illegal steroid use” was to be retained. (R. at 2.)

On November 1, 2008, the FBI executed the search warrant on StarTests’s Millersville facility. (R. at 2.) The StarTests personnel informed the FBI that since the CFL was such a

major client and since the CFL drug-testing program had been conducted for the past four years, the vast majority of the computers in the facility had at least one database pertaining to CFL drug-testing program. (R. at 2.) To increase confidentiality of test results, StarTests used a computer-hopping procedure which consists of dividing each database's information among multiple computers using different names or encrypted files; no one database contained enough information to read the players' test results. (R. at 2.) Due to these impediments, the head FBI agent ordered all computer equipment to be either seized or copied depending on ease of movement of the piece of equipment. (R. at 2.)

At the FBI facility in Wythe, FBI computer forensic agents were able to view the databases and determine which test result correlated with which player. (R. at 2.) While viewing the databases, the agents also came across test results that indicated that multiple CFL players had tested positive for other illegal drugs. (R. at 2.) The FBI subsequently expanded its investigation to include all illegal drug possession and sale within professional football. (R. at 2.) In light of this new objective, the FBI decided to keep all of StarTests's databases. (R. at 2.) The FBI copied all the hard drives and returned any unneeded equipment. (R. at 2.)

II. The Lower Courts' Decisions.

Respondents filed a motion pursuant to FED. R. CRIM. P. 41(g) requesting that the FBI return all information and equipment unrelated to the five CFL players under investigation. (R. at 2-3.) The District Court held that the CFL had standing to file the 41(g) motion. (R. at 3.) The District Court further held that the warrant issued by Magistrate Judge Leon was valid and that the plain view doctrine authorized the FBI's seizure of all evidence not marked for seizure in the warrant. (R. at 6.)

Respondents appealed to the Circuit Court, arguing that the District Court erred by upholding Magistrate Judge Leon’s search warrant because of its lack of particularity and by applying the plain view doctrine in a digital evidence search and seizure case. (R. at 7.) The Circuit Court affirmed the District Court’s ruling that the CFL had standing to file the 41(g) motion. (R. at 10.) A divided Circuit Court adopted the standards for issuing warrants in digital evidence cases recently announced by the Ninth Circuit in United States v. Comprehensive Drug Testing, which require the magistrate judge to place limitations on the scope of the warrant to guard against unauthorized exploratory searches. The standards also require the government to waive reliance on the plain view doctrine in digital evidence cases. Judged against the Comprehensive standards, the Circuit Court found the FBI’s search to be illegal and granted Respondents’ 41(g) motion to return all seized property to StarTests’s Millersville facility. (R. at 15-16.)

SUMMARY OF THE ARGUMENT

The Fourth Amendment allows law enforcement agents to engage in searches and seizures as long as they are reasonable. The Circuit Court incorrectly reversed the District Court’s decision to uphold the FBI’s search of StarTests’s Millersville facility and erred in adopting the standards for digital evidence searches recently announced in the Ninth Circuit case United States v. Comprehensive Drug Testing, 579 F.3d 989 (9th Cir. 2009) (en banc). First, the Circuit Court incorrectly ruled that, because Magistrate Judge Leon’s warrant authorized the seizure of “all computer records, files, and equipment” related to a StarTests’s steroid testing of CFL players, it was not sufficiently particular. Second, the Circuit Court erred in forbidding the government to rely on the plain view doctrine in digital evidence cases.

This Court's Fourth Amendment jurisprudence reveals the error in the Circuit Court's ruling. Under Fourth Amendment, a valid search warrant must only meet three requirements: 1) it is issued by a neutral and disinterested magistrate, 2) it is supported by probable cause, and 3) it describes, with particularity, the places to be searched and items to be seized. In digital evidence cases, generic language is permissible in the warrant when detailed particularity is impossible as long as the warrant specifies the types of items to be seized.

Magistrate Judge Leon's warrant only allowed the FBI agents to search for and seize information reasonably related to the investigation into the five CFL for which the FBI had probable cause to believe had engaged in illegal steroid usage and distribution. The warrant specified the types of items to be seized as computer records, files, and equipment, and only allowed an off-site search where an on-site search would be impracticable. The FBI had to act quickly to put together as accurate an affidavit as it could under time constraints, as it began its investigation in July of 2008 and executed the search on November 1, 2008. Upon the FBI agents' arrival, StarTests personnel informed them that the results of the drug tests, which were conducted over the course of four years, were spread out over multiple computers in encrypted and hidden files. At that point, it was reasonable for the agents to seize the computer equipment so that computer forensics agents could view and match the test results to the suspected players off-site because there was no way to quickly segregate and seize only the evidence they needed. Throughout the execution of the search, the FBI acted in good faith, seeking to conduct the least intrusive and most practical search and seizure possible.

This Court's Fourth Amendment jurisprudence also allows for warrantless searches and seizures as long as they are reasonable under the circumstances. The plain view doctrine, an exception to the warrant requirement, allows for seizure of items without a warrant if (1) a law-

enforcement officer is lawfully present, (2) an item not named in the warrant is in the plain view of the officer, and (3) the incriminating nature of the item is immediately apparent.

The FBI had searched for and seized the data on StarTests's computers pursuant to a valid warrant. During the off-site search of the StarTests databases, FBI agents saw other evidence of illegal drug use in plain view. The FBI only viewed these databases because they had probable cause to believe the databases contained evidence of steroid use by the five CFL players. When the agents opened the database containing the sought-after test results, data concerning other players immediately presented itself before them, satisfying the plain view requirement. The numerous positive results next to "cocaine, marijuana, and various other hallucinogens" indicated to the officers that other CFL players had tested positive for illegal drugs.

Fourth Amendment principles do not change with the technology involved in a given search or seizure. The main concern in the context of electronic media searches is that a search for certain information on a computer will turn into a general search of the type the Fourth Amendment was intended to prevent. Based on the government's affidavit, the magistrate can appropriately limit the search's scope and the items to be seized to prevent an overexpansive search. Though such a warrant may require dealing with issues of data security, mislabeled files, and hidden documents, whether the end result violates the Fourth Amendment, i.e., is unreasonable, can be answered only after considering the facts of the particular situation. Moreover, since evidence discovered in plain view within the scope of a magistrate-approved search warrant is by definition the fruit of constitutionally protected activity, excluding such evidence is not reasonable.

In the present case, the evidence seized was not in a separate folder or file, but in the same database as the evidence sought by the warrant. Even if the FBI had utilized a search protocol to prevent it from reading documents unrelated to the warrant, the agents still would have found, opened, and read the document containing test results because that is exactly what the warrant authorized them to do. Having a third party copy and paste only the relevant part of the database into another file would leave the government without the original evidence in its original context and format, thus opening the door to allegations by defendants that the government has tampered with evidence or taken it out of context. While a magistrate judge may require a high level of particularity as part of a warrant, reasonableness does not require dividing individual files into smaller and smaller pieces only because it is theoretically possible. It is completely reasonable for the government to seize all the incriminating evidence.

Although warrants must both establish probable cause and particularly describe the place to be searched and the property to be seized, this Court has rejected the idea that warrants must include the precise manner in which they are to be executed. In fact, this Court has affirmed that it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant, although subject to later judicial review for reasonableness. After the government has established probable cause, a magistrate judge's duty is merely ministerial; the Fourth Amendment does not require warrants to specify the manner of their execution. Guidance concerning how electronic searches should be performed belongs in the Federal Rules of Criminal Procedure, not in jurisprudence concerning the issuance of warrants. Like all searches, electronic searches are still subject to post-search judicial review for reasonableness. But having courts create detailed execution requirements as preconditions to issuing warrants is far beyond the cases and controversies

Article III lists as the realm of federal courts. The Constitution empowers the Executive Branch, not the Judicial Branch, to execute searches and seizures, subject to the limits of the warrant and judicial review for reasonableness.

ARGUMENT

- I. The CFL lacks standing to file a FED. R. CRIM. P. 41(g) motion on behalf of its players because the CFL was not a "person aggrieved" by the search and seizure of individual football players' drug testing records and none of its members, the franchises, would have standing to sue individually.

For a party to have standing to challenge a search and seizure, it must show two things: 1) the litigant must demonstrate an injury in fact that is concrete in nature, and 2) the litigant must prove that he is asserting his own legal rights and interests and not the rights of a third party. Rakas v. Illinois, 439 U.S. 128, 139 (1978); see also Singleton v. Wulff, 428 U.S. 106, 112 (1976). When an association is the party invoking federal jurisdiction to challenge a search or seizure, it can establish standing in two ways. An association can allege that the association itself suffered a harm sufficient to confer standing under the Rakas test. The association can also satisfy the standing requirement by alleging that one or more of its members suffered a legally cognizable harm that satisfies the Rakas test and the association has an interest in seeking legal redress on behalf of those injured members. E.g., Warth v. Seldin, 422 U.S. 490, 511 (1975). As the record demonstrates, neither the CFL nor the individual members of the CFL have standing under the Rakas test because neither suffered an injury in fact to a legally protected interest.

- a. The CFL was not the victim of the search of StarTests's facility or the seizure of the individual players' records.

Central to the standing issue is "whether the plaintiff has alleged such a personal stake in the outcome of the controversy as to warrant his invocation of federal court jurisdiction and to justify exercise of the court's remedial powers on his behalf." Warth, 422 U.S. at 498-99. The

way in which the plaintiff demonstrates his or her personal stake will vary according to the facts of the case. To have standing to bring a Rule 41(g) motion, the plaintiff must be “[a] person aggrieved by an unlawful search and seizure of property or by the deprivation of property.” FED. R. CRIM. P. 41(g).

In order to qualify as a person aggrieved by an unlawful search and seizure, one must have been a victim of a search or seizure, one against whom the search was directed, as distinguished from one who claims prejudice only through the use of evidence gathered as a consequence of a search or seizure directed at someone else. Rakas, 439 U.S. at 134-35. In Rakas, police searched a vehicle after a traffic stop and found a sawed-off shotgun and shells underneath the seat. Id. at 129. Nevertheless, the passengers challenged the lawfulness of the search at trial by alleging that Jones v. United States, 362 U.S. 257, 261 (1960), granted standing to victims of a search or seizure *or* one against whom the search was directed. Rakas, 439 U.S. 128, 132. The Court held that the phrase “one against whom the search was directed” was not an alternate test for standing, rather, it was the parenthetical equivalent of the previous phrase “a victim of a search or seizure.” Id. at 135. The Court rejected the petitioners’ argument and held that, since they did not assert a property or possessory interest in either the vehicle or the items seized from the vehicle, they had no standing to challenge the search. Id. at 148.¹

The CFL did not have a sufficient interest in the players’ test results to qualify as a victim of the FBI search. At no time did the CFL have access, control, or ownership of the test results. The players’ test results that the FBI seized, along with the computer equipment they were stored on, were the property and in the possession of StarTests. The computers were owned and maintained by StarTests. Furthermore, the computers were housed in StarTests's facility.

¹ Although Rakas and Jones were both Fourth Amendment cases, the Supreme Court has held that Rule 41(g) conforms to the general Fourth Amendment standard. Alderman v. United States, 394 U.S. 165, 173, n. 6 (1969).

Nowhere in the record does the CFL claim that they had property or possessory interests in the players' test results. The CFL is not trying to vindicate its own rights. Rather, the CFL is attempting to vicariously assert the rights of another because the seized evidence has the potential to interfere with the financial success of the league. This court has previously rejected such a vicarious assertion. See Rakas, 439 U.S. at 133-34. Since the CFL claims no possessory or property interest in the test results, nor can it prove such an interest, the CFL fails to qualify as a victim of the FBI search.

- b. The CFL's members, the franchises, did not suffer an injury that would allow them to bring suit in their own right.

An association has standing to bring suit on behalf of its members when (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 of individual members in the lawsuit. Hunt v. Wash. State Apple Adver. Comm'n, 432 U.S. 333, 343 (1977) (finding a state agency comprised of apple growers and dealers elected by their peers had associational standing to challenge a North Carolina statute); see also United States v. Comprehensive Drug Testing, Inc., 513 F.3d 1085, 1096 (9th Cir. 2008), aff'd in part, rev'd in part, dismissed in part, 579 F.3d 989 (9th Cir. 2009) (en banc). In Comprehensive, the Ninth Circuit applied the Hunt test to a set of facts remarkably similar to the instant case. The Major League Baseball Players Association (Players Association) filed a Rule 41(g) motion after the federal government seized dozens of baseball players' drug testing records and computer equipment from a company hired by Major League Baseball to test the players for steroid usage. 513 F.3d at 1093. The court observed that the individual players had standing to sue on their own, and since the only remedy sought was return of property, the involvement of the players was unnecessary. Also, the Players Association was organized for

the sole purpose of protecting the players' interests. The court held that the Hunt test was satisfied and the Players Association had standing to challenge the seizure of records and equipment. Id. at 1096.

The CFL fails the first prong of the Hunt test because its individual members do not have standing to sue on their own. In Comprehensive, the Players Association, not the league, filed the 41(g) motion requesting that the players' test results be returned. As the Ninth Circuit recognized in Comprehensive, the Players Association was organized for the sole purpose of representing the interests of major league baseball players. Id. at 1096. Many individual baseball players, all of them members of the Players Association, were harmed by the seizure and therefore had standing to bring suit on their own. Id. Here, the CFL filed the 41(g) motion. However, the CFL does not execute the same mission as the Players Association. The CFL is more properly recognized as the trade association of the franchise owners. See Mark Conrad, The Business of Sports: A Primer for Journalists 4-6 (Lawrence Erlbaum Associates, Inc., 2005). The franchise owners were not harmed by the FBI's search of StarTests's facility, the individual football players were. Since the franchise owners were not harmed, they do not have an "injury in fact" to satisfy the constitutional requirement of a case or controversy and therefore could not bring a lawsuit on their own. See Lujan v. Defenders of Wildlife, 504 U.S. 555, 560-61 (1999). Therefore, the CFL fails the first prong of the Hunt test for associational standing.

The CFL also fails the second prong of the Hunt test because the privacy interests of the players are not germane to the purposes of the CFL. The CFL is organized to represent the interests of its members; its members are the owners of the individual franchises. The interests of the franchise owners revolve around the business aspects of the CFL: organizing games, regulating franchise creation, setting the rules of the game, negotiating with the players' union,

etc. The CFL's attempt to represent the players' interests contrasts to the situation in Comprehensive where the baseball players' union, the Players Association, filed the 41(g) motion. The Players Association is an organization created with the permission of the players, and its purpose is to represent the interests of the players. Filing a lawsuit to protect the players' privacy interests was well within the purpose of the Players Association. However, the CFL was not created by the players, is not made up of the players, and does not represent their interests. The privacy interests of the individual players are not germane to the purpose of the CFL. Thus the CFL has no standing to file a 41(g) motion. StarTests, the only remaining party, does not have a privacy interest in the test results. Therefore, no party has standing to complain that the FBI's retention of copies of the players' test results violates the players' privacy.

II. Federal magistrates may issue warrants authorizing the government to seize all computer equipment and files for an off-site search when such warrants are sufficiently particular and an on-site search of the digital evidence is impractical and overly intrusive.

The Fourth Amendment requires that a valid search warrant meet three basic requirements: 1) it is issued by a neutral and disinterested magistrate, Illinois v. Gates, 462 U.S. 213, 239-40 (1983); 2) it is supported by probable cause, id.; and 3) it describes, with particularity, the places to be searched and items to be seized, Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971). Here, Magistrate Judge Leon's neutrality is not at issue nor is the probable cause to search the computers for the five football players' drug test results. Thus, this section focuses on the particularity of warrants allowing for the search and seizure of computer equipment and files, and why the government's seizure for later review in this particular case is permissible.

Courts concerned with the particularity of a warrant primarily examine whether the warrant contained enough information to guide and control the agent's judgment in selecting

what to take and whether the category as specified prevents officers from seizing items that should not be seized, to the extent possible. United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999.) Here, Magistrate Judge Leon issued a warrant for a search of data relating to StarTests’s drug tests of the five players under investigation. (R. at 1-2.) The search resulted in FBI agents seizing all computer records, files, and equipment that could reasonably contain information relating to those five players. (R. at 1-2.) The warrant authorized the seizure of either a copy of all data or the computer equipment itself that related to the investigation as long as “an on-site search would be impracticable.” (R. at 2.) Then, an off-site search was conducted by computer personnel, who came across test results indicating illegal substance use by other CFL players. (R. at 2.) The warrant issued by Magistrate Judge Leon was sufficiently particular because 1) it contained instructions limiting the scope of what an agent may initially search and 2) it restricted officers from seizing items not to be seized, to the extent possible. Even prior to the recent amendment to the Rules of Criminal Procedure concerning electronically stored information, seizure for an off-site search was permitted when, as in this case, it would be more intrusive and impractical to conduct on-site sorting. See, e.g., United States v. Summage, 481 F.3d 1075, 1079 (8th Cir. 2007); Guest v. Leis, 255 F.3d 325, 335 (6th Cir. 2001). Thus, Magistrate Judge Leon’s warrant allowing for the initial search for the computers storing the CFL data, seizure of those computers, and a later off-site search, was not overbroad.

- a. The warrant in this case was sufficiently particular because the warrant contained instruction that focused the FBI agents’ search on information regarding the five players’ illegal use of steroids.

The particularity requirement for warrants prevents the government from engaging in a “general exploratory rummaging in a person’s belongings.” Coolidge, 403 U.S. at 467; see also Andresen v. Maryland, 427 U.S. 463, 480 (1976) (prohibiting “general warrants”). At the same

time, warrants are intended to be practical and commonsense tools, “drafted by nonlawyers in the midst and haste of a criminal investigation.” United States v. Ventresca, 380 U.S. 102, 108 (1965). This Court has recognized that warrants are not held to high “[t]echnical requirements of elaborate specificity.” Id. Rather, courts generally defer to the issuing magistrate. United States v. Hill, 459 F.3d 966, 973-75 (9th Cir. 2006); United States v. Carey, 172 F.3d 1268, 1272-73 (10th Cir. 1999); see also Gates, 103 U.S. at 288 (emphasizing this Court’s history of substantial deference to magistrates).

A court should look to whether an executing officer would reasonably know what items should be seized. United States v. Summage, 481 F.3d 1075, 1079 (8th Cir. 2007); United States v. Kimbrough, 69 F.3d 723, 727 (5th Cir. 1995); United States v. Tamura, 694 F.2d 591, 595 (9th Cir. 1982). Courts generally focus on whether it was reasonable to expect a more detailed warrant and whether the search of the documents could have been further narrowed, either by specifying the types of documents needed or the documents’ relation to the alleged crime. See United States v. Schandl, 947 F.3d 462, 465-66 (11th Cir. 1991) (emphasizing that the “crucial inquiry” is always whether the search and seizure is “reasonable under all the circumstances,” which includes the behavior of the searching officers, the scope of the warrant, the facts of the case, and the nature of the evidence being sought); United States v. Spilotro, 800 F.2d 959, 963 (9th Cir. 1986) (disapproving a warrant because it could have better tied the documents sought to the crimes and it failed to identify their type or contents). Prior to Comprehensive Drug Testing, even the Ninth Circuit had a history of finding search warrants sufficiently particular if the “government described the items to be searched and seized as particularly as could be reasonably expected given the nature of the crime and the evidence it then possessed.” United States v. Adjani, 452 F.3d 1140, 1149 (9th Cir. 2006); see also United States v. Mann, 389 F.3d 869, 877

(9th Cir. 2004) (holding that a warrant does not need to be elaborately detailed, but simply “reasonably specific”).

With respect to electronic data, if courts specify the types of items to be seized, “generic language is permissible” when “detailed particularity is impossible.” United States v. Kimbrough, 69 F.3d 723, 727 (5th Cir. 1995). A warrant that permits the seizure of computer software, drives, hardware, and equipment will satisfy the particularity requirement if it correlates the equipment and data to be seized with the alleged crime. In Kimbrough, for example, the court upheld a warrant authorizing the seizure of “commercial software and manuals, hardware, computer disks, disk drives, monitors, computer printers, modems . . . other computer related operational equipment, and other similar materials . . . used to visually depict a minor engaging in sexually explicit conduct.” Id. Similarly, in United States v. Upham, the court upheld a warrant allowing the seizure and an off-site search of “any and all computer software and hardware . . . computer disks, disk drives” because it was limited by the alleged crime of child pornography. 168 F.3d 532, 535-536 (1st Cir. 1999).

In United States v. Gracey, the Tenth Circuit upheld a warrant that did not specify what type of “equipment” officers could seize from the suspect’s business premises. 111 F.3d 1472, 1475-76 (10th Cir. 1997). In Gracey, the warrant authorized officers to seize “equipment, order materials, papers, membership lists, and other paraphernalia” relating to the distribution of pornography in violation of state laws. Id. During the search, officers seized computer equipment belonging to the suspect, including two computers, monitors, keyboards, modems, and CD-ROM drives. Id. at 1476. The court held that the warrant’s failure to explicitly state what type of “equipment” officers could seize did not make the warrant overbroad because it guided officers toward the relevant items to be seized by limiting the search to equipment

“pertaining to the distribution or display of pornographic material in violation of state obscenity laws.” Id. at 1478-79.

In United States v. Abrams, the First Circuit found that a general description in the warrant calling for officers to seize fraudulent records was a general exploratory search that required the officers to make a legal distinction between fraudulent and non-fraudulent records. 615 F.2d 541, 542-43 (1st Cir. 1980). The court highlighted that the warrant could have limited the search by requiring the seizure of only Medicare and Medicaid patient records, as the case concerned alleged Medicare and Medicaid fraud. Id. at 543; see also Adjani, 452 F.3d at 1148 (focusing on whether a warrant tied the documents sought to the crimes alleged). Instead, the officers had “no guidance” and seized records of non-Medicare and non-Medicaid patients, making the search and seizure unconstitutional. Id. at 543-545; cf. United States v. Frost, 125 F.3d 346, 388 (6th Cir. 1997) (“[T]he agents did not ‘flagrantly’ exceed the scope of the warrant, which appropriately authorized the extensive seizure of paper and computer documents in this complicated mail fraud case.”).

In this case, the warrant issued by Magistrate Judge Leon was sufficiently particular because it guided agents to search only for information “reasonably related to the investigation into the five named players’ illegal steroid use,” thereby restricting the search and seizure to investigation-related data. (R. at 2.) First, the warrant specified the types of items to be seized as “computer records, files, and equipment,” and only allowed an off-site search “where an on-site search would be impracticable,” modeling the warrant after the valid warrants in Kimrough and Upham. (R. at 2.) In fact, the warrant was more specific than the valid warrant in Gracey, limiting the search to only computer equipment and not allowing a broad search of any possible non-computer equipment StarTests had on its premises. Second, Magistrate Judge Leon

restricted the search and seizure to information “reasonably related to the investigation into the five named players’ illegal steroid use,” following established law requiring some correlation between the objects of the warrants and the alleged crime. (R. at 2.) For example, if agents opened a file containing no data pertaining to steroid use or if the file contained the results of another organization’s drug tests, the warrant would have required them to close the file. Thus, unlike in Abrams, the warrant guided agents to look only for evidence that could be used in the current investigation.

- b. The seizure of all computer records, data, and equipment followed by an off-site search was necessary for the government to find the data for which it had probable cause and to avoid a more intrusive and lengthy on-site search.

The government’s seizure of items within the scope of the warrant should not be invalidated solely because some items seized were outside of the warrant’s scope. United States v. Henson, 848 F.2d 1374, 1383 (6th Cir. 1988). This Court has admonished courts “not [to] indulge in unrealistic second-guessing” of a search or seizure. United States v. Sharpe, 470 U.S. 675, 686-87. A “creative judge engaged in *post hoc* evaluation of police conduct can almost always imagine some alternative means by which the objectives of police might have been accomplished,” but simply because there may have been “less intrusive means does not, itself, render the search unreasonable.” Id. (quoting Cady v. Dombrowski, 413 U.S. 433, 447 (1973)) (“The question is not simply whether some other alternative was available, but whether the police acted unreasonably in failing to recognize or pursue it.”). The most recent version of Rule 41 specifically authorizes later review of electronically stored information and allows the executing officer to “retain a copy of the electronically stored information that was seized or copied.” See FED. R. CRIM P. 41(e)(2)(B). Moreover, the seizure for off-site sorting is an

accepted method by many courts when it is impractical and more intrusive to sort the data at the time of the search.

- i. The massive amount of data, risk of deceptive file labeling, and lack of necessary software on-site to search StarTests’s databases necessitated the seizure of all computer records, files, and equipment to cover the material for which the government had probable cause.

The level of detail required in a warrant is specific to the nature of the evidence sought. Adjani, 452 F.3d at 1147-48. Probable cause may apply to an entire computer just as it may apply to an entire file cabinet, and thus, a magistrate is not required to specify in the warrant every file that may be seized. For example, when a specific document is sought in a business office, a warrant may authorize the search and seizure of an entire file cabinet if it is unclear in which specific file the evidence is located. United States v. Hargus, 128 F.3d 1358, 1363 (10th Cir. 1997). For computer searches, it is particularly difficult to specify the exact location of sought-after data; thus, generic categories of items may be seized if a more specific description is not possible. Adjani, 452 F.3d at 1147-48. If a “sufficient chance of finding some needles in the computer haystack [is] established by the probable-cause showing in the warrant application . . . [then] a search of a computer and co-located disks is not inherently more intrusive than the physical search of an entire house for a weapon or drugs.” Upham, 168 F.3d at 535; see also United States v. Ross, 456 U.S. 798, 820-21 (1982) (“[A] warrant that authorizes an officer to search a home for illegal weapons also provides authority to open closets, chests, drawers, and containers in which the weapon might be found [N]ice distinctions between closets, drawers, and containers . . . must give way to the interest in the prompt and efficient completion of the task at hand.”).

Computers, like file cabinets, contain an unwieldy amount of documents that may require the entire container to be seized because it is “impossible to tell what a computer storage medium

contains just by looking at it.” Hill, 459 F.3d at 973. Computers are like containers, with the data on a computer’s hard drive or disk being the “inside” of the computer. Adjani, 452 F.3d at 1152 (equating computers to “file cabinets (with millions of files) and locked desk drawers”). In Adjani, the warrant authorized the search of a suspect’s residence, vehicle, and person, along with the seizure of both “records, documents, and materials” relating to the alleged extortion and communications with others suspected of involvement in the extortion scheme. Id. at 1144. It also authorized the seizure of Adjani’s “[c]omputer, hard drives, computer disks, CD’s, and other computer storage devices,” describing the seizure as necessary to find evidence of the alleged crime. Id. The warrant further allowed for off-site sorting, stating computer personnel could examine “all of the data contained in the computer equipment and storage devices.” Id. The Ninth Circuit first found that warrant was valid because it provided the “precise identity and nature of the items to be seized” and described the alleged criminal activity. Id. at 1148-49 (citations omitted). The court then emphasized the effortless task of disguising or renaming files. Id. at 1150. Thus, it held that the warrant’s level of specificity was reasonable under the circumstances because requiring “such a pinpointed computer search, restricting the search to an email program or to specific search terms, would have likely failed to cast a sufficiently wide net to capture the evidence sought.” Id. at 1149.

Courts recognize that warrants cannot predict where incriminating evidence may be found when information can be misfiled, mislabeled, or hidden to shield it from a search. Guest v. Leis, 255 F.3d 325, 335 (6th Cir. 2001). In Kimbrough, the Fifth Circuit upheld the seizure of “virtually every record, document and paper found at the premises . . . [and] every video and audio cassette tape” because whether each contained child pornography “could not be determined by a cursory examination on the premises” and the tapes’ labels were “not dispositive

of their content.” 69 F.3d at 728. In United States v. Summage, the Eighth Circuit permitted the search and seizure of “all video tapes and DVDs, pornographic pictures, video and digital recording devices and equipment, all equipment that is used to develop, upload, or download movies, computers, and any indicia of occupancy.” 481 F.3d at 1079. The court deemed an extensive search and seizure necessary because officers knew only that a video and photographs of alleged child pornography existed, but not the format in which they were being kept. Id.; see also United States v. Hay, 231 F.3d 630, 637-38 (9th Cir. 2000) (upholding a warrant for the search and seizure of an entire computer system in a child pornography investigation).

Accordingly, not everything seized must be specifically listed in the warrant. See Davis v. Gracey, 111 F.3d 1472, 1481 (10th Cir. 1997) (finding no Fourth Amendment violation when defendants seized a bulletin board computer system that included personal communications unrelated to the alleged crime). Even when the Tenth Circuit held that a warrant was overbroad, it was “quick to note” that the results were “predicated only upon the particular facts of this case,” in which the officer searching through the defendant’s computer looked through files he knew he was not authorized to see. See United States v. Carey, 172 F.3d 1268, 1274-75 (10th Cir. 1999) (recognizing, however, that computers could contain ‘intermingled documents’ and officers may engage in off-site sorting of all documents (quoting United States v. Tamura, 694 F.2d 591, 595-96 (9th Cir. 1982))). But see Horton v. California, 496 U.S. 128, 138-39 (finding the motive of an officer to be irrelevant). Moreover, in some cases in which the warrant was held overbroad, the court found the government to be at fault because the investigation lasted years, showing that the delay of the additional investigation required to request a more precise search would not have been unreasonable. Abrams, 615 F.2d at 543 n.5; United States v. Kow, 58 F.3d 423, 427, 428 n.2 (9th Cir. 1995).

The warrant here, allowing for the search and seizure of computer records, files, and equipment regarding an alleged crime pertaining to five individuals, is not inherently less specific than a warrant allowing for the physical search of an entire file cabinet for paper records regarding certain individuals. The District Court adhered to the well-established limits of the particularity requirement, stating, “Given the difficulty of searching through thousands of computer files and the special technical knowledge required, it is not unreasonable for a neutral and detached magistrate to provide for the . . . seizure of all computer equipment for further review.” (R. at 4-5) (holding the warrant to be facially valid because restricting the search further would “too greatly hamper the government’s ability to find incriminating evidence in the digital universe”).

Unlike cases in which the court held the government could have made a more specific request, here the government acted under time constraints. It commenced its investigation in July 2008 and quickly put together as accurate an affidavit as it could, conducting the search on November 1, 2008. (R. at 1-2.) Like in Adjani, Magistrate Judge Leon was not required to specify every file that might be seized in the warrant. Instead, similar to a warrant for the search and seizure of a file cabinet containing relevant documents, the warrant allowed for the seizure of all computer equipment and files that reasonably related to the investigation only if “an on-site search would be impracticable.” (R. at 2.) The warrant relied upon the difficulties articulated by the government in searching mass quantities of computer files, which include “mislabeled or deceptively hidden [files] in various H-drives or S-drives.” (R. at 8.) Upon the FBI agents’ arrival, StarTests personnel informed them that the results of the drug tests, which were conducted over the course of four years, were spread out over three computers in encrypted and hidden files. (R. at 2.) At that point, it was reasonable for the agents to seize the computer

equipment for computer forensics agents to view and match the test results to the suspected players because there was no way to quickly segregate and seize only the evidence they needed. (R. at 2.)

The appellate court relied on the minority view espoused in Comprehensive Drug Testing. However, even in that case, the Ninth Circuit “accept[ed] the reality that such over-seizing is an inherent part of the electronic process and proceed[ed] on the assumption that, when it comes to the seizure of electronic records, this will be far more common than in the days of paper records.” 579 F.3d 989, 1006 (9th Cir. 2009). Indeed, the case conflicts with the Federal Rules of Criminal Procedure, which now allow for the seizure of electronic data for later review. FED. R. CRIM P. 41(e)(2)(B). Here, the seizure of all the computers was necessary to gather the evidence needed for the five suspected players. Because the FBI seized only the computers containing the files and databases where the alleged positive drug tests for the five players were located, the seizure was reasonable under the Fourth Amendment.

- ii. The off-site search was reasonable because StarTests’s files relating to the drug-testing program were massive and its “computer-hopping” file storage procedure made an on-site search nearly impossible.

Courts across the country recognize the near impossibility in sifting and separating large amounts of both computer-related and non-computer-related evidence on-site, and therefore they allow the seizure of documents when on-site sorting is impractical. For example, in Guest v. Leis, the court found it unreasonable for the warrant to require officers to separate relevant files from unrelated files at the time of the search due to the “technical difficulties of conducting a computer search in a suspect’s home.” 255 F.3d at 335. Furthermore, computers contain hidden and deleted files, and finding such files “is no easy task.” Upham, 168 F.3d at 535. It is “frequently difficult, and often times more intrusive to an individual’s privacy, to perform an on-

site review of certain items.” Summage, 481 F.3d at 1079. Even if the officers are trained in computer searches, a court will find it unreasonable to require police to sort through extensive files in a suspect’s office in order to separate out items outside the warrant’s scope. United States v. Henson, 848 F.2d 1374, 1363 (6th Cir. 1988).

In Hill, the Ninth Circuit repeatedly highlighted the difficulties in conducting an on-site search of computers and related media. First, it emphasized that officers were not required to bring adequate equipment—“far more than an ordinary laptop computer”—to read computer storage media and a competent officer to operate the equipment. 459 F.3d at 974. The court pointed out the complex types of equipment that would be necessary, including computers that were equipped to read the “variety of operating systems—various versions or flavors of Windows, Mac OS and Linux—to name only the most common” as well as “all of the major media types.” Id. The court recognized that to require such on-site searches would “be an insuperable obstacle” and “pose a significant burden” on law enforcement because of the difficulty of determining what a computer contains by simply looking at it. Id. Moreover, there is no assurance that officers are able to bypass security measures to operate any computers on-site. Id. Even if there were proper equipment and a competent agent to sort data, the Hill court recognized that the officers could damage or “compromise the integrity of the evidence,” which is “not trivial.” See id. (“As everyone who has accidentally erased a computer file knows, it is fairly easy to make mistakes . . . especially [with] equipment one is not intimately familiar with.”).

In addition to the complex equipment and possibility of irreparable damage, the Hill court underscored the significant time it might take for officers to “examine every one of what may be

thousands of files on a disk.” Id. at 974-75.² Thus, it is an unnecessary drain on government resources to require officers to learn to navigate software used by each computer they may potentially search simply to avoid off-site sorting by trained personnel. Hill, 459 F.3d at 973-74.

Hill was a case of child pornography on a suspect’s single computer. In contrast, here the FBI was faced with multiple computers and a company skilled at encrypting and hiding data. (R. at 1.) The mechanics of the search for test results later performed off site could not readily have been conducted on the spot. (R. at 8.) Moreover, the FBI agents were simply not trained to search the intentionally complicated database created by StarTests. Like in Guest, it would be unreasonable to expect the government to sort the data on the spot. Requiring the searching agents to be well-versed in conducting an on-site search, without accidentally destroying crucial evidence, would likely take weeks, if not months, of training and would be an enormous drain on public resources.

As Hill recognized, there are a number of hazards in searching electronic storage media: computer files may have misleading names, files may have false extensions, data can be erased or hidden by its owner, and there could be traps to alter or destroy data if exact procedures are not followed. This type of on-site search could, in fact, be more intrusive than seizing the data for a later search of the evidence. Here, such a search, particularly without cooperation, could

² Other courts have emphasized the need for off-site sorting for precisely these reasons. See United States v. Summage, 481 F.3d 1075, 1079-80 (8th Cir. 2007) (finding an off-site search necessary for a wide variety of equipment and media that could be used in for development, uploading, downloading, and storing of child pornography because the officers did not know what format in which it was created or stored, and an on-site search would be practically difficult and time consuming); United States v. Kimbrough, 69 F.3d 723, 728 (5th Cir. 1995) (finding the seizure of all recorded material on premises in a search for child pornography permissible because determining presence of child pornography on the items required more than simply a cursory on-site examination); United States v. Hargus, 128 F.3d 1358, 1363 (10th Cir. 1997) (determining that officers’ seizure of two entire file cabinets was acceptable because the officers were authorized to seize ten broad categories of records and those records were present in every drawer of both cabinets); United States v. Schandl, 947 F.2d 462, 465-66 (11th Cir. 1991) (citations omitted) (seizure of certain unauthorized items was permissible because the IRS agents were searching for complicated evidence of tax evasion, and could not immediately evaluate materials without “aggravating the intrusiveness of the search”).

lead to time-consuming obstacles and could also cause irreversible damage to important evidence. As a result of these difficulties, the search would be more intrusive and lengthy than if the data were seized and sorted off-site, and the long-term presence of FBI agents could significantly disrupt StarTests's business. The warrant controlled for the issues address in Hill and ensured that the most efficient and least invasive off-site search would be conducted by limiting the search to "appropriately trained personnel." (R. at 2.)

Unlike in Comprehensive Drug Testing, Respondents here have presented no evidence that the StarTests personnel were willing to help the agents locate the results of the drug tests for the five players. Cf. 579 F.3d at 996 (pointing out that the agents brush[ed] aside an offer by on-site CDT personnel to provide all information pertaining to the ten identified baseball players"). Additionally, Respondents "have proffered no evidence to show that the government ended the search for the five players' drug test results and subsequently began another, unauthorized search for unrelated information relying on the protection of the plain view doctrine From the evidence presented, the government seems to have been matching the identification numbers . . . and while doing so it came across other positive test results and matching names." (R. at 5;) cf. Comprehensive Drug Testing, 579 F.3d at 999 ("Indeed, the government admitted . . . that 'the idea behind taking [the copy of the Tracey Directory] was to take it and later on briefly peruse it to see if there was anything above and beyond that which was authorized for seizure in the initial warrant.'"). But see Horton, 496 U.S. at 138-39 (finding an officer's motive irrelevant to the validity of a search). Consequently, the seizure of data for off-site sorting was reasonable because the government acted in good faith, seeking to conduct the least intrusive and most practical search and seizure possible.

III. Applying the plain view doctrine in a digital search context satisfies the Fourth Amendment's reasonableness test where the searching officer saw the test results targeted by the warrant in the same file as positive test results for illegal substances.

The Fourth Amendment is not offended when a law enforcement officer who has legitimately invaded an individual's privacy comes across something, immediately recognizes that it is evidence of criminal activity, and seizes it. Horton v. California, 496 U.S. 128, 136 (1990). However, this is only true if the officer has a lawful right of access to the object. Id. at 137. The main concerns when the plain view doctrine is used in conjunction with a warrant are that the warrant is sufficiently particular and has a sufficiently limited scope, Id. at 139-40, but there are no other restrictions on the plain view doctrine's application.

- a. The FBI satisfied the plain view doctrine's requirements when it retained records showing illegal drug use where those records were from a database Magistrate Judge Leon's warrant authorized the FBI to seize and search.

The plain view doctrine allows for seizure if "(1) a law-enforcement officer is lawfully present, (2) an item not named in the warrant . . . is in the plain view of the officer, and (3) the incriminating nature of the item is immediately apparent." United States v. Raney, 342 F.3d 551, 558-59 (7th Cir. 2003).

As discussed earlier, the FBI had seized and searched the data on Startests's computers pursuant to a valid warrant. See supra Part II. Furthermore, in contrast to Carey, 172 F.3d at 1271, and United States v. Dichiarinte, 445 F.2d 126 (7th Cir. 1971), where the government asserted plain view to justify opening and viewing files unrelated to the warrant, here the FBI properly opened the file described in the warrant and only then saw other evidence of illegal drug use in plain view. In fact, this warrant authorized the FBI to search the contents of StarTests's database for evidence of steroid use by five CFL players, and that is what the database contained; the FBI searched the exact database that they had probable cause to believe contained evidence

of illegal drug use. (R. at 2.) Thus, the FBI agents were “lawfully present” in examining the database where they found the additional evidence at issue here.

Furthermore, the data seized was in plain view of the officers. When they opened the database containing the sought-after test results, data concerning other players immediately presented itself before them, (R. at 6,) satisfying the plain view requirement. Finally, the incriminating character of the other tests results was immediately apparent to the FBI officers. The numerous positive results next to “cocaine, marijuana, and various other hallucinogens” indicated to the officers that the individuals tested had used illegal drugs. (R. at 2;) see 21 U.S.C. § 812 (2009) (list of controlled substances); Id. § 844(a) (unlawful possession).

- b. The District Court correctly found that the plain view doctrine applied where the incriminating data seized and the data targeted by the warrant were located immediately next to each other in the same database.

The Fourth Amendment is grounded in the requirement of reasonableness, Brigham City v. Stuart, 547 U.S. 398, 403 (2006), and therefore Fourth Amendment principles do not change with the technology involved in a given search or seizure. United States v. Giberson, 527 F.3d 882, 887 (9th Cir. 2008). Thus this Court has rejected bright line rules and embraced tests that determine the reasonableness of the government’s action by considering the totality of the circumstances. See Ohio v. Robinette, 519 U.S. 33, 39 (1996).

Courts have consistently rejected arguments that a single physical file, folder, or volume should be segregated during a search. See, e.g., United States v. Adjani, 452 F.3d 1140, 1151 (9th Cir. 2006); United States v. Beusch, 596 F.2d 871, 877 (9th Cir. 1979) (finding no violation for a search and seizure of “items which, though theoretically separable, in fact constitute one volume or file folder”). Although hindsight may demonstrate that a given file or folder could have been separated because some of its information was not sought by the search warrant, the

Fourth Amendment does not require such foreknowledge or separation. United States v. Hill, 459 F.3d at 976 & n.11 (requiring only justification for the search of each item when only two of 154 disks searched contained images of child pornography).

The main concern in the context of electronic media searches is that a search for certain information on a computer will turn into a general search of the type the Fourth Amendment was intended to prevent. Yet as this Court has already found, scrupulous adherence to the warrant requirements will prevent such problems. See Horton, 496 U.S. at 140. Based on the government's affidavit, the magistrate can craft appropriate limitations to prevent an overexpansive search. Though such a warrant may require dealing with issues of data security, mislabeled files, and hidden documents, see, e.g., United States v. Hill, 322 F. Supp. 2d 1081 (C.D. Cal. 2004) aff'd on other grounds 459 F.3d 966, whether the end result violates the Fourth Amendment, i.e., is unreasonable, can be answered only after considering the facts of the particular situation. Moreover, since evidence discovered in plain view within the scope of a magistrate-approved search warrant is by definition the fruit of constitutionally protected activity, excluding such evidence is not reasonable.

In the present case, application of the plain view doctrine is reasonable. The evidence seized was not in a separate folder or file, but in the same database as the evidence sought by the warrant. The concern that the government would engage in a wholesale seizure of intermingled documents without judicial approval to seize all the documents, as was presented in Tamura, 694 F.2d at 595-96, is not present here because Magistrate Judge Leon authorized the seizure of everything the FBI seized. Even if the FBI had utilized a search protocol to prevent it from reading documents unrelated to the warrant, as suggested in Carey, 172 F.3d at 1276, the agents

still would have found, opened, and read the document containing test results because that is exactly what the warrant authorized them to do.

The only conceivable way for the FBI to have found the evidence identified in the warrant was for them to come across other evidence of illegal drug use, unless maybe a third party copied and pasted only the relevant part of the database into another file. Cf. United States v. Comprehensive Drug Testing, 579 F.3d 989, 1016 n.2 (9th Cir. 2009) (en banc) (Bea, J., concurring in part and dissenting in part) (suggesting a computer technician copy and paste only the relevant excel cells into a new spreadsheet and provide only the new spreadsheet to the police). However, this would leave the government without the original evidence in its original context and format, thus opening the door to allegations by defendants that the government has tampered with evidence or taken it out of context. See FED. R. EVID. 1002 (original document generally required); notes to FED. R. EVID. 1001 (copies produced manually are not admissible under Rule 1003). While a magistrate judge may require a high level of particularity as part of a warrant, reasonableness does not require dividing individual files into smaller and smaller pieces only because it is theoretically possible. Beusch, 596 F.2d at 877. In a situation like this, where the FBI would have seen other incriminating evidence even had it opened only the database containing the evidence sought by the warrant, it is completely reasonable for the government to rely on the plain view doctrine in seizing all the incriminating evidence.

IV. Contrary to Fourth Amendment precedent, the Court of Appeals' rules grant magistrate judges the power to prevent searches justified by probable cause and require the government to spend additional time and money on each electronic search case, and therefore such restrictions are best left to the Federal Rules of Criminal Procedure.

Although warrants must both establish probable cause and particularly describe the place to be searched and the property to be seized, this Court has rejected the idea that warrants must include “a specification of the precise manner in which they are to be executed.” Dalia v. United

States, 441 U.S. 238, 257 (1979) (holding that a warrant did not need to state that it permitted covert entry to install electronic surveillance equipment). In fact, this Court has affirmed that “it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant,” although subject to later judicial review for reasonableness. Id. After the government has established probable cause, a magistrate judge’s duty is merely ministerial; the Fourth Amendment does not require warrants to specify the manner of their execution. United States v. Grubbs, 547 U.S. 90, 98 (2006); see Ex Parte United States, 287 U.S. 241, 250 (1932) (finding no discretion to refuse warrant after indictment because such a refusal “falls little short of a refusal to permit the enforcement of the law”). Thus, the checks required by the Fourth Amendment are the magistrate’s finding of probable cause and inclusion of sufficient particularity.

However, the Court of Appeals’ requirements that a magistrate approve a specific search protocol, (R. at 15,) and define who may view the information the government has probable cause to search and seize, (R. at 14,) place the magistrate in a much more active role. They also contradict this Court’s “repeated[] refus[al] to declare that only the ‘least intrusive’ search practicable can be reasonable under the Fourth Amendment.” Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 663 (1995). The position taken by the Tamura court is closer to what the Fourth Amendment requires. That court complained that the government did not seek judicial approval to seize entire file cabinets for later sorting and searching, not that the search lacked probable cause or with judicial approval would have been unreasonable. 694 F.2d at 595-96. Here, the FBI obtained Magistrate Judge Leon’s approval for the seizure and off-site sorting of all the data seized. (R at. 2.)

The Court of Appeals' requirements are also impractical. The government will have little idea how easy it will be to find information on a given computer until it examines the computer. In some cases folders and files may be well labeled, but in others files may be mislabeled, given false extensions, or even hidden. See, e.g., Gutman v. Klein, No. 03 Civ. 1570, 2008 U.S. Dist. LEXIS 92398 at *7-17 (E.D.N.Y. Oct. 15, 2008) (explaining detailed procedures used by defendant to hide and delete computer data) adopted by 2008 U.S. Dist. LEXIS 97707 (Dec. 1, 2008). Even in the former case, a search may not be straight forward because of the software the government uses to maintain the integrity of the data. See Orin S. Kerr, Searches and Seizures in a Digital World, 119 Harv. L. Rev. 531, 543-47 (2005) (explaining the process used by the FBI to retrieve evidence from a computer). Requiring a specific search protocol be performed by special personnel who are not part of the investigative team will increase the amount of money and time the government will need to spend on electronic searches without providing any additional privacy protection. Indeed, these new personnel will still see all of the data the Court of Appeals sought to protect, but, since they are not the investigators on the case, they will have less familiarity with the case and be less accountable for the results.

Guidance concerning how electronic searches should be performed thus belong in the Federal Rules of Criminal Procedure, not in jurisprudence concerning the issuance of warrants. E.g., FED. R. CRIM. PRO. 41. Like all searches, electronic searches are still subject to post-search judicial review for reasonableness. But having courts create detailed execution requirements as preconditions to issuing warrants is far beyond the cases and controversies Article III lists as the realm of federal courts. E.g., Letter from Karen L. Strombom, Chief United States Magistrate Judge, W.D. Wash., to Robert Westinghouse, Assistant U.S. Attorney (Oct. 1, 2009) (listing eleven requirements for warrants for search and seizure of electronically stored information); see

Steel Co. v. Citizens for a Better Env't, 523 U.S. 83, 101 (1998) (limiting the judiciary's power to actual cases and controversies is "essential" to the separation of powers). The Constitution empowers the Executive Branch, not the Judicial Branch, to execute searches and seizures, subject to the limits of the warrant and judicial review for reasonableness.

CONCLUSION

For the foregoing reasons, Petitioner respectfully requests the Court reverse the ruling of the U.S. Circuit Court of Appeals for the Fourteenth Circuit.

Respectfully submitted,

Spong Competition Number: 11