

**IN THE
SUPREME COURT OF THE UNITED STATES**

UNITED STATES OF AMERICA,

Petitioner,

v.

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

Respondents.

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

BRIEF OF RESPONDENTS

Team No. 10
Attorneys for Respondents

QUESTION PRESENTED

- I. Does the Respondent, the Colonial Football League, have standing to sue on behalf of its players for the return of illegally seized property under Federal Rule of Criminal Procedure 41(g)?

- II. 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)?

- III. 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.?

TABLE OF CONTENTS

QUESTIONS PRESENTED.....	i
TABLE OF CONTENTS.....	ii
TABLE OF AUTHORITIES	iii
OPINIONS BELOW.....	1
CONSTITUTIONAL PROVISIONS	1
STATEMENT OF THE CASE.....	2
SUMMARY OF THE ARGUMENT	6
ARGUMENT	9
I. UNDER FEDERAL RULE OF CRIMINAL PROCEDURE 41(G), THE CFL HAS STANDING BECAUSE THE SEARCH WAS DIRECTED AGAINST IT AND IT MEETS ALL PRONGS OF THE <i>PENNELL</i> TEST.....	9
A. <u>The CFL has standing because a search was directed against it when the FBI seized the databases in which the CFL has a proprietary interest and the government copied the information the CFL was contractually obligated to protect.....</u>	9
B. <u>The CFL has standing because it satisfies all three prongs of the <i>Pennell</i> test because the players are able to sue individually and it is contractually bound to protect the privacy interests of the players who are not necessary parties.....</u>	10
II. THE PARTICULARITY REQUIREMENT FOR ISSUING WARRANTS IS CLARIFIED IN THE DIGITAL EVIDENCE CONTEXT UNDER THE GUIDELINES ANNOUNCED BY THE NINTH AND FOURTEENTH CIRCUITS.....	12
III. THE GOVERNMENT MAY NOT RELY ON THE PLAIN VIEW EXCEPTION TO THE FOURTH AMENDMENT’S WARRANT REQUIREMENT IN SEARCHES OF ELECTRONICALLY STORED INFORMATION.....	15
CONCLUSION.....	20

TABLE OF AUTHORITES

Cases

Coolidge v. New Hampshire,
403 U.S. 443 (1971).....15, 16, 18

Horton v. California,
496 U.S. 128 (1990).....15

Massachusetts v. EPA,
549 U.S. 497 (2007).....10

Pennell v. City of San Jose,
485 U.S. 1 (1988).....6, 10, 11, 12

Rakas v. Illinois,
439 U.S. 128 (1978).....9

Trupiano v. United States,
334 U.S. 699 (1948).....16, 17

United States v. Abrams,
615 F.2d 541 (1st Cir. 1980).....17

United States v. Adjani,
452 F.3d 1140 (9th Cir. 2006).....19

United States v. Carey,
172 F.3d 1268 (10th Cir. 1999).....14, 16

United States v. Comprehensive Drug Testing, Inc.,
579 F.3d 989 (9th Cir. 2009).....*passim*

United States v. Elycio-Montoya,
18 F.3d 845 (10th Cir. 1994).....1

United States v. Giberson,
527 F.3d 882 (9th Cir. 2008).....17, 19

United States v. Hill,
459 F.3d 966 (9th Cir. 2006).....12, 19

United States v. Hillyard,
677 F.2d 1336 (9th Cir. 1982).....17

<i>United States v. Raney</i> , 342 F.3d 551 (7th Cir. 2003).....	16
<i>United States v. Tamura</i> , 694 F.2d 591 (9th Cir. 1982).....	17
<i>United States v. Turner</i> , 169 F.3d 84 (1st Cir. 1999).....	16
<i>Warth v. Seldin</i> , 422 U.S. 490 (1975).....	11
<u>Regulations</u>	
Fed. R. Crim. P. 41(g).....	<i>passim</i>

OPINIONS BELOW

The Respondents, StarTests and the CFL filed a motion per Federal Rule of Criminal Procedure 41(g) to reclaim all illegally seized property. (R. at 1, 3, 9.) The United States District Court for the District of Wythe decided that the CFL had standing to seek the return of the information it paid StarTests to collect and store. (R. at 3, 10.) However, it concluded that the evidence was not illegally seized by the United States government and denied the motion to return the property. (R. at 1, 6, 9.) However, the court did decide that the CFL had standing to seek the return of their information. (R. at 7, 9.) Additionally, the CFL appealed claiming it was reversible error to deny the motion for the return of the property seized by the government. (R. at 7, 9.) The United States Circuit Court of Appeals for the Fourteenth Circuit reversed the district court’s opinion by adopting new standards for drafting warrants and the use of the plain view exception in computer search cases. (R. at 7, 17.) The case was remanded with instructions that all property be returned to StarTests. (R. at 17.) The United States government petitioned the Supreme Court of the United States and a Writ of Certiorari was granted. (R. at 20.) As this case involves denial of a 41(g) motion, the decision is reviewed de novo. *See United States v. Elycio-Montoya*, 18 F.3d 845, 848 (10th Cir. 1994).

CONSTITUTIONAL PROVISIONS

Constitutional Provisions

U.S. Const. amend. IV.....*passim*

STATEMENT OF THE CASE

To ensure compliance with its own athletic performance standards, the Colonial Football League (“CFL”) began requiring its franchises to submit players for drug screening tests (conducted either by blood or urine sample) as a term of membership. (R. at 1, 8.) The CFL subsequently hired StarTests, Inc. (“StarTests”) to conduct the tests and store the information. (R. at 1, 8.) StarTests is an independent business specializing in conducting drug tests for professional sports franchises, corporations, school districts and other organizations. (R. at 1, 8.) The CFL and StarTests contractually represented to the franchises and their respective players that the information gathered would remain confidential and anonymous, with StarTests only disclosing whether five percent or more of CFL’s players tested positive for illegal steroid use. (R. at 1, 8.) The CFL has required the drug test every year since 2005. (R. at 8.)

In July 2008, due to intense media scrutiny, the Federal Bureau of Investigation (“FBI”) began an investigation into the use and distribution of illegal steroids by professional athletes. (R. at 7.) The investigation implicated five well-known football players who play for two of the most famous American professional football franchises, as major users and distributors. (*Id.*) Both the Wythe City Lightning and Marshall Phoenixes are team franchise members of the CFL. (R. at 1.) From the Lightning, the FBI collected transactional evidence implicating quarterback John Reynolds and wide receiver John Reeves. (R. at 1, 7.) Three newly drafted rookies from the Phoenixes, Danny Rodriguez, Michael Fleming and Ace Hall were also implicated as cooperating in the steroid ring. (R. at 1, 7.)

During the course of its investigation, the FBI assembled information that each of the five players was involved with illegal steroids. (R. at 1.) According to evidence ascertained at the motions hearing, the evidence included numerous eyewitness reports and taped conversations.

(R. at 7.) After securing these conversations and documents, the FBI hoped to prove that the players had actually used the illegal steroids as performance enhancers. (R. at 8.) It was during this inquest that the FBI discovered the drug testing program administered by the CFL. (*Id.*)

As a result, the FBI presented its case for probable cause to a magistrate and applied for a search warrant to seize material related to the alleged steroid use from the StarTests facility in Millersville, Wythe. (R. at 1, 8.) In the supporting affidavit, the FBI requested permission to seize “all computer records, files, and equipment” related to the StarTests-administered test. (R. at 1–2, 8.) To justify such a broad request, the FBI relied on difficulties common to all computer searches: the massive quantity of data at issue, the technical difficulty of locating, identifying, and retrieving files that may be mislabeled or deceptively hidden in various drives, and the fact that viewing and decoding the data might require software not available at the StarTests facility. (R. at 2, 8.)

The magistrate judge issued the warrant which 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, 8.) The only restrictions imposed included the caveat that the search be limited to information “reasonably related to the investigation into the five named players’ steroid use.” (R. at 2, 8.) Additionally, “law enforcement personnel trained in searching and seizing computer data” were to decide when the seizure and removal of computer equipment was necessary.” (R. at 2, 8.) Lastly, “appropriately trained personnel” were to review the data, retain the relevant information, and designate the remainder for return. (R. at 2, 8.)

The FBI executed the search warrant on the StarTests facility on the morning of

November 1, 2008 and discovered that the computer system configuration was far more complex than originally anticipated. (R. at 2, 8.) When the agents inquired about the location of the CFL drug test results, StarTests personnel pointed out that most of the computers in the facility included at least one database on the CFL drug test. (R. at 2.) The manager of the Millerville office described the “computer-hopping” procedure employed by the company to maintain client confidentiality as involving three separate databases for each drug test. (R. at 8.)

Testimonial evidence demonstrated at the motions hearing that one computer contained a database recording the players’ names and personal health information. (R. at 2, 8.) Another contained a database listing the assigned numbers given to the players prior to the test date. (R. at 2, 8.) The final computer held the test results with the assigned identification number given to each participant. (R. at 2, 8.) The databases were then saved on different computers in the facility under different names. (R. at 2, 8.) The league was one of StarTests largest clients and the tests had been conducted for the past four years. (R. at 2.) The “computer-hopping” procedure was repeated for every year in which the drug test was administered and no one computer at the StarTests facility had two databases from any one test administered in any one year. (R. at 2, 8.) Additionally, many of these files were encrypted while others were hidden in various computer drives. (R. at 2.) The purpose of this procedure was to maintain the integrity of the plaintiff’s business and constituted a part of StarTests’s and CFL’s confidentiality commitment to the players. (R. at 2.)

Realizing that the search for the information could take a few days, the head agent decided to seize all of the computer equipment at the facility and copy the hard drives of computers that were stationary or difficult to move for further review. (R. at 2, 8–9.) The computers and other digital media were taken to the FBI computer forensics laboratory in Wythe

City. (R. at 2, 8–9.) Computer forensics agents were able to eventually view the databases and match the test results to the five players in question. (R. at 2, 9.) However, while conducting the search the FBI computer personnel discovered positive test results for illegal steroid use by other CFL players who were not included in the warrant. (R. at 2, 9.) The tests also revealed positive test results for a myriad of other illegal substances such as cocaine, marijuana and various hallucinogens. (R. at 2.)

Following this discovery, the FBI decided to expand its investigation to include all illegal drug possession and sale within professional football. (R. at 2, 9.) Toward this new objective and without seeking additional warrants, the FBI decided to retain StarTests' databases. (R. at 2, 9.) After thoroughly copying and inventorying the computer hard drives, the FBI returned the unneeded equipment. (R. at 2, 9.)

SUMMARY OF THE ARGUMENT

Under Federal Rule of Criminal Procedure 41(g), the CFL has standing because the search was directed against it when the FBI sought to seize the databases in which it has a proprietary interest and when the government copied the information it was contractually obligated to protect. This view is supported by the fact that the government searched the StarTests facility to acquire the “CFL drug test databases.” The CFL does qualify as one against whom the search was directed because it has a proprietary interest in the databases and the FBI targeted its drug test databases. Additionally, the CFL has standing because it satisfies all three prongs of the *Pennell* test because the players are able to sue individually, it is contractually bound to protect the privacy interests of the athletes and the players are not necessary parties to the action.

Under the guidelines announced in the Ninth and Fourteenth Circuits, the warrant was invalid because it lacked particularity in allowing for the seizure of all computer equipment with only a cursory inspection for relevance by trained personnel. In order to clarify the particularity requirement for issuing federal warrants in the digital evidence context, the Ninth Circuit announced a four pronged set of guidelines in *United States v. Comprehensive Drug Testing*. The warrant failed to adequately require that the segregation and redaction of information from computer documents be done either “by specialized personnel or an independent third party” in order to protect private data from government encroachment. The warrant was overbroad because it failed to warn of the risk that its encryption process would result in the seizure of all its databases and exposure of its entire clientele. The warrant failed to ensure that the government’s search protocol was designed to uncover “only the information for which it has

probable cause and only that information may be examined by the case agents” because the computer personnel turned over related and unrelated information. Finally, the warrant did satisfy the last condition by requiring the return of property irrelevant to the search. However, application of the four prongs of the Ninth Circuit’s test shows that the warrant was invalid because it lacked particularity when it allowed for the seizure of all computer equipment with only a cursory inspection for relevance by trained personnel.

Even if the warrant were sufficiently particular, the FBI violated the Fourth Amendment by relying on the plain view exception and retaining digital information about players other than the five for which it had probable cause. The plain view exception may not be used as an excuse to engage in a fishing expedition until something incriminating at last emerges. As an exception to the warrant requirement, the Supreme Court has warned the circuits about allowing plain view doctrine to become an end run around the Fourth Amendment. It is therefore important for the federal courts to be cautious in the application of search warrant exceptions, and to either forbid its application or severely restrict it in instances when the government can use it to completely negate the need for a warrant and seize a wide array of evidence. The wholesale seizure for later detailed examination of records not described in a warrant has been characterized as the kind of investigatory dragnet that the fourth amendment was designed to prevent.

In the comparatively rare instances where documents are so intermingled that they cannot feasibly be sorted on site, we suggest that the government and law enforcement officials generally can avoid violating fourth amendment rights by sealing and holding the documents pending approval by a magistrate of a further search, in accordance with the procedures set forth in the American Law Institute's Model Code of Pre-Arrest Procedure. If the need for transporting the documents is known to the officers prior to the search, they may apply for

specific authorization for large-scale removal of material, which should be granted by the magistrate issuing the warrant only where on-site sorting is infeasible and no other practical alternative exists. The essential safeguard required is that wholesale removal must be monitored by the judgment of a neutral, detached magistrate.

After a number of computer search cases, the Ninth Circuit recently eschewed the plain view exception altogether in *Comprehensive Drug Testing*. It stated that the government should, in future warrant applications, forswear reliance on the plain view doctrine or any similar doctrine that would allow it to retain data to which it has gained access only because it was required to segregate data that may be seized from that which may not. If the government refuses, the magistrate judge must order that the data be sorted by an “independent third party” under the court’s supervision. The court also imposed a duty on the government to disclose the actual risks of concealment and destruction of evidence in any given computer search, and that the search protocol must be designed to root out only the documents for which the government has probable cause.

Given the fact that computers are simultaneously file cabinets and locked desk drawers, the negation of plain view does little more than harmonize current technological complexity with the Fourth Amendment’s reasonableness requirement. As the FBI has conceded a lack of probable cause to seize the additional drug test information, then its seizure and retention was an illegal search and seizure under the Fourth Amendment because the government erroneously relied on the plain view doctrine.

ARGUMENT

I. UNDER FEDERAL RULE OF CRIMINAL PROCEDURE 41(G), THE CFL HAS STANDING BECAUSE THE SEARCH WAS DIRECTED AGAINST IT AND IT MEETS ALL PRONGS OF THE *PENNELL* TEST.

A. The CFL has standing because a search was directed against it when the FBI seized the databases in which the CFL has a proprietary interest and the government copied the information the CFL was contractually obligated to protect.

The CFL has standing because it has a proprietary interest in the databases seized and a contractual obligation to the players. A Rule 41(g) motion requires that the moving party is one who has been “aggrieved by an unlawful search and seizure of property or by the deprivation of property.” Fed. R. Crim. P. 41(g). Furthermore, “a person aggrieved by an unlawful search and seizure” is either a “victim [or] *one against whom the search was directed*, as distinguished from one who claims prejudice only through the use of evidence gathered as a consequence of a search or seizure directed at someone else.” *Rakas v. Illinois*, 439 U.S. 128, 134–35 (1978).

Arguably, the CFL has a stronger ownership interest in the databases than StarTests does because it paid the facility to administer the tests and to store the results in its computer databases for reasons of anonymity. (R. at 10.) The CFL has a good claim that the databases are indeed its property and that they are simply stored at another facility. (*Id.*) This view is supported by the fact that the government searched the StarTests facility to acquire the “CFL drug test databases.” (*Id.*) The CFL does qualify as one against whom the search was directed because it has a proprietary interest in the databases and the FBI targeted its drug test databases. (R. at 3, 10.)

This interest outweighs any vicarious representation of the players’ privacy interests that CFL could maintain. (R. at 10.) However, the contract between the CFL and each individual player whose results are at issue grants the CFL the right to represent their interests as

professional athletes. (R. at 3, 10.) The CFL does qualify as one against whom the search was directed because it has a contractual obligation to protect the privacy interests of its player, especially when involving bodily fluids. (R. at 10.) Therefore, the CFL has standing because it has a proprietary interest in the databases seized and a contractual obligation to the players.

B. The CFL has standing because it satisfies all three prongs of the *Pennell* test because the players are able to sue individually and it is contractually bound to protect the privacy interests of the players who are not necessary parties.

The CFL has standing because it satisfies all three prongs of the *Pennell* test because the players are able to sue individually, it is contractually bound to protect the privacy interests of the athletes and the players are not necessary parties to the action. An association has standing to sue on behalf of its members when each individual would otherwise have independent standing to sue, the interests sought to be protected are germane to the organization's purpose, and the claim asserted does not require the participation of the individual members of the lawsuit.

Pennell v. City of San Jose, 485 U.S. 1, 7 n.3 (1988).

The CFL satisfies the first element of associational standing because each player could individually sue because he meets the three required elements of injury, causation and redressability for independent standing. The first element requires the individual members to have independent standing in order for the association to be able to sue on behalf of its members.

Id. There are three elements that must be met for individual standing, which are injury, causation and redressability. *Massachusetts v. EPA*, 549 U.S. 497, 515 (2007).

The injuries each player suffered were an invasion of their private medical records without consent and the continued withholding of copies of that information. The FBI seized this information and continues to keep copies of the test results. (R. at 2, 9.) Therefore, the cause of the harm is fairly traceable to the United States government. Finally, the harm is easily

redressed by granting the order to return the illegally seized property. Each player would have the right to seek the return of his own drug testing record (R. at 3.), and to hold otherwise would be contrary to the basic respect society has for one's privacy and possessory interest in medically related records. Therefore, the CFL satisfies the first element of associational standing because each player could individually sue because he meets the three required elements of injury, causation and redressability for independent standing.

The players' privacy interests in the drug test results are related to the CFL's organizational function which is to represent the athletes. (R. at 3.) The second element of associational standing requires that the interests to be protected are germane to the organization's purpose in order to sue on behalf of its members. *Pennell*, 485 U.S. at 7 n.3. Under their contracts, the CFL is obligated with protecting the players' interests, especially in an instance where their privacy was intruded upon under the CFL's prerogative. (R. at 3.) Therefore, the second element of associational standing is met because it is germane to the purpose of the CFL to defend the privacy interests of the individual players that it has contracted to protect.

Finally, the CFL may sue on behalf of the players because they are not required parties to the cause of action when only seeking prospective relief. The third element of associational standing requires that the participation of the individual members not be necessary in order for the organization to sue on behalf of its members. *Pennell*, 485 U.S. at 7 n.3. For prospective relief, the individual players need not be parties to the action. *See Warth v. Seldin*, 422 U.S. 490, 515 (1975) (holding that an association lacked standing where it sought damages on members' behalf rather than "a declaration, injunction, or some other form of prospective relief"). The CFL seeks only the return of the drug testing information on StarTests's computers (R. at 3.), which is a form of prospective relief. The final element of associational standing is satisfied

because only prospective relief is being sought and that does not require the participation of the individual players.

Consequently, the CFL has standing because it satisfies all three prongs of the *Pennell* test because the players are able to sue individually, it is contractually bound to protect the privacy interests of the athletes and the players are not necessary parties to the action.

II. THE PARTICULARITY REQUIREMENT FOR ISSUING WARRANTS IS CLARIFIED IN THE DIGITAL EVIDENCE CONTEXT UNDER THE GUIDELINES ANNOUNCED BY THE NINTH AND FOURTEENTH CIRCUITS.

The warrant was invalid because it lacked particularity when it allowed for the seizure of all computer equipment with only a cursory inspection for relevance by trained personnel. (R. at 4, 9.) Search warrants must be specific. *United States v. Hill*, 459 F.3d 966, 973 (9th Cir. 2006). Specificity has two aspects: particularity and breadth. *Id.* Particularity is the requirement that the warrant must clearly state what is sought. *Id.* Breadth deals with the requirement that the scope of the warrant be limited by the probable cause on which the warrant is based. *Id.* (internal quotation marks and citations omitted). The level of specificity required “varies depending on the circumstances of the case and the type of items involved.” *Id.* In order to clarify the particularity requirement for issuing federal warrants in the digital evidence context, the Ninth Circuit announced a four pronged set of guidelines. *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 1006 (9th Cir. 2009). First, the segregation and redaction of information from computer documents “must be either done by specialized personnel or an independent third party.” *Id.* Second, warrants must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other courts. *Id.* Third, the government’s search protocol must be designed to uncover “only the information for which it has probable cause and only that information may be examined by the case agents.” *Id.* Finally, the

Ninth Circuit required the government to “destroy or, if the recipient may lawfully possess it, return non-responsive data.” *Id.*

In order protect private data from government encroachment, federal warrants must require that the segregation and redaction of information from computer documents “be either done by specialized personnel or an independent third party.” *Id.* The employees can be either government employees or independent third parties, but all such personnel must not communicate any information outside the scope of the warrant that they find during the segregation process without separate court approval. *Id.* at 1000. The magistrate judge touched on this condition when the warrant required computer personnel to make the initial decision to seize and that “appropriately trained personnel” perform the segregation. (R. at 14.) However, the fact that the computer personnel who decided to seize all the computer equipment collaborated with the FBI agents in conducting the actual database search only lends credence to the accusation that “government agents obviously were counting on the search to bring constitutionally protected data into the plain view of the investigating agents.” *Comprehensive Drug Testing, Inc.*, 579 F.3d at 999. Therefore, the warrant failed to adequately require that the segregation and redaction of information from computer documents be done either “by specialized personnel or an independent third party” in order to protect private data from government encroachment. *Id.* at 1006.

The actual risks of destruction of information as well as prior efforts to seize that information in other courts must be disclosed in warrants involving digital evidence. *Id.* at 1006. According to the record, the FBI was not required to give any information about the risks of destruction or concealment other than what it volunteered for the affidavit. (R. at 14.) StarTests had a contractual duty to protect its clients’ drug test information, and so it encrypted the data.

(*Id.*) Instead of seizing the computer equipment and files, the computer personnel could have simply located the database with the identification numbers, then locate the databases with the test results, match the numbers to the results, and then perform a cut-and-paste function of the drug test results into another document. (R. at 14–15.) This simple procedure would have ensured that they would only view information regarding the five players for which there was probable cause. *Comprehensive Drug Testing*, 579 F. 3d at 1016 n.2 (Bea, J., concurring in part, dissenting in part) (describing a cut-and-paste procedure in Microsoft Excel to prevent random scrolling by computer forensics analysts). The warrant was impermissibly broad because it failed to warn of the risk that its encryption process would result in the seizure of all its databases and exposure of its entire clientele list. *Id.* at 1006.

Additionally, the warrant must ensure that the government’s search protocol is designed to uncover “only the information for which it has probable cause and only that information may be examined by the case agents.” *Comprehensive Drug Testing*, 579 F. 3d at 1006. If the government is going to use sophisticated tools to discover well-known illegal files without opening the files, it must be disclosed in the warrant. *Id.* at 999. Law enforcement must engage in the intermediate step of sorting various types of documents and then only search the ones specified in a warrant. *United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999). To give effect to this requirement, the computer personnel must act as an effective barrier and turn over only the relevant database information while leaving out anything found which was not covered by the search warrant. (R. at 15.) The warrant at issue here fails in that respect because the computer personnel turned over related and unrelated information, no doubt causing the FBI’s decision to expand its investigation from mere illegal steroid use to that of all illegal substances. (*Id.*) The record is also devoid of any decryption equipment or special equipment used to detect

the databases and ascertain the information, and the warrant prescribes none. (*Id.*) Such unchecked search protocols do not meet the constitutional requirement of a narrowly tailored, particular search warrant. (*Id.*)

Finally, the Ninth Circuit required the government to “destroy or, if the recipient may lawfully possess it, return non-responsive data.” *Comprehensive Drug Testing*, 579 F. 3d at 1006. However, Federal Rule of Criminal Procedure 41(g) already provides a remedy for return of property and it is the one sued under in this matter. (R. at 15.) Although the warrant to search and seize StarTests’ databases failed under all the other prongs of the *Comprehensive Drug Testing* test, it did actually satisfy this condition by requiring the return of property irrelevant to the search. (*Id.*)

Application of the four prongs of the Ninth Circuit’s test shows that the warrant was invalid because it lacked particularity when it allowed for the seizure of all computer equipment with only a cursory inspection for relevance by trained personnel.

III. THE GOVERNMENT MAY NOT RELY ON THE PLAIN VIEW EXCEPTION TO THE FOURTH AMENDMENT’S WARRANT REQUIREMENT IN SEARCHES OF ELECTRONICALLY STORED INFORMATION.

Even if the warrant were sufficiently particular, the FBI violated the Fourth Amendment by relying on the plain view exception and retaining digital information about players other than the five for which it had probable cause. *See Horton v. California*, 496 U.S. 128 (1990); *Coolidge v. New Hampshire*, 403 U.S. 443 (1971). “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.” *Coolidge*, 403 U.S. at 454–55. The exceptions are “jealously and carefully drawn,” and there must be “a showing by those who seek exemption . . . that the exigencies of the situation made

that course imperative.” *Id.* at 455. The burden is on those seeking the exemption to show the need for it. *Id.* However, “the plain view doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges.” *Carey*, 172 F.3d at 1272 (quoting *Coolidge*, 403 U.S. at 466).

Although some courts have been receptive to applying the plain view exception just as they would in cases involving homes or vehicles, most have been either hesitant or hostile to the notion. *Compare United States v. Raney*, 342 F.3d 551, 559 (7th Cir. 2003) (holding that “the plain view doctrine applies” to a child pornography computer search); *with United States v. Turner*, 169 F.3d 84, 88 (1st Cir. 1999) (refusing to apply the plain view doctrine where a police officer saw a nude photo of an assault victim on the defendant’s desktop during a house search and proceeded to search the computer). The district court erred in finding that the plain view doctrine applies in digital evidence cases to the same extent that it applies in searches of the home or vehicle. (R. at 9.)

The aversion to a plain view exception for digital searches is based on the recognition that it will inevitably pass the test each time it is applied. (R. at 11.) As an exception to the warrant requirement, the Supreme Court has warned the circuits about allowing plain view doctrine to become an end run around the Fourth Amendment. (*Id.*) 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 procedure of any search. *Coolidge*, 403 U.S. at 465. It is therefore important for the federal courts to be cautious in the application of search warrant exceptions, and to either forbid its application or severely restrict it in instances when the government can use it to completely negate the need for a warrant and seize a wide array of evidence. *Trupiano v. United States*, 334 U.S. 699, 700 (1948) (“[T]he Fourth Amendment is a

recognition of the fact that in this nation individual liberty depends in large part upon freedom from unreasonable intrusion by those in authority. It is the duty of this Court to give effect to that freedom”).

Wherever possible, courts should err on the side of granting neutral and detached magistrates the prerogative to decide when searches and seizures are permissible, rather than police officers who have an “understandable zeal to ferret out crime.” *Trupiano*, 334 U.S. at 705. However, the wholesale seizure for later detailed examination of records not described in a warrant is significantly more intrusive, and has been characterized as “the kind of investigatory dragnet that the fourth amendment was designed to prevent.” *United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982) (citing *United States v. Abrams*, 615 F.2d 541, 543 (1st Cir. 1980)). In the comparatively rare instances where documents are so intermingled that they cannot feasibly be sorted on site, the Government and law enforcement officials generally can avoid violating fourth amendment rights by sealing and holding the documents pending approval by a magistrate of a further search, in accordance with the procedures set forth in the American Law Institute's Model Code of Pre-Arrest Procedure. *Tamura*, 694 F.2d at 595–96. If the need for transporting the documents is known to the officers prior to the search, they may apply for specific authorization for large-scale removal of material, which should be granted by the magistrate issuing the warrant only where on-site sorting is infeasible and no other practical alternative exists. *Id.* at 596 (citing *United States v. Hillyard*, 677 F.2d 1336, 1340 (9th Cir. 1982)). The essential safeguard required is that wholesale removal must be monitored by the judgment of a neutral, detached magistrate.

Usually, the pause to apply the doctrine occurs in situations where the court feels that the government had already received a broad search warrant, and sought to use plain view to sweep

up the data and evidence that the warrant did not cover. *See United States v. Giberson*, 527 F.3d 882, 889 (9th Cir. 2008) (refusing to reach the plain view argument because the court found that the seizure was authorized by a broad search warrant). In the case of a computer, gaining access to the desktop is the same as having access to all the files in the My Computer file folder. (R. at 11.) The Supreme Court has given numerous warnings against turning computer warrants, by their application, into authorizations for general exploratory searches. *See, e.g., Coolidge*, 403 U.S. at 466.

Due to the number of computer search cases, the Ninth Circuit recently responded to the situation created by the plain view exception in August 2009. *Comprehensive Drug Testing*, 579 F.3d at 989. In facts quite similar to this case, the FBI raided three different facilities searching for evidence of steroid usage. *Id.* It seized all the computer equipment and hard drives at every facility. *Id.* When the drug testing company brought suit to have their property returned, the government responded that it complied with the procedures articulated in *Tamura* by asking for prior authorization to seize the computer equipment. *Id.* As such, the government was not required to return the computer equipment because that evidence was in plain view once its agents began to examine the contents. *Id.* at 997. The Ninth Circuit immediately responded to the flaw in this argument by saying that “if the government can not 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, under this theory, come into plain view.” *Id.* at 998. With this prerogative, government agents will be tempted to seize “more rather than less.” *Id.* (citation omitted). Accepting the government’s argument would virtually wipe out Fourth Amendment protections for computer searches. *Id.*

To avoid “mak[ing] a mockery of *Tamura*” and to heed the common Fourth Amendment judicial warning against allowing the government to “seize the haystack to look for the needle,” the Ninth Circuit laid out new guidelines to guide magistrate judges in issuing warrants and law enforcement officials in tailoring their future digital searches. *Comprehensive Drug Testing*, 579 F.3d at 998; *Hill*, 459 F.3d at 975. It stated that “the government should, in future warrant applications, forswear reliance on the plain view doctrine or any similar doctrine that would allow it to retain data to which it has gained access only because it was required to segregate seizable from non-seizable data.” *Comprehensive Drug Testing*, 579 F.3d at 998. If the government refuses, the magistrate judge must order that the seizable and nonseizable data be separated by an “independent third party” under the court’s supervision. *Id.* The court also imposed a duty on the government to disclose the actual risks of concealment and destruction of evidence in any given computer search, and that the search protocol must be designed to root out only the documents for which the government has probable cause. *Id.* at 998–99.

These safeguards will ensure that investigatory agents only see images and documents authorized by a warrant supported by probable cause issued by a neutral and independent magistrate. (R. at 13–14.) Given the fact that “[c]omputers are simultaneously file cabinets and locked desk drawers,” with comingled information, this reexamination of plain view does little more than harmonize current technological complexity with the Fourth Amendment’s reasonableness requirement. *United States v. Adjani*, 452 F.3d 1140, 1152 (9th Cir. 2006); *Giberson*, 527 F.3d at 888–89 (holding that computer searches do not merit heightened procedural protection beyond the Fourth Amendment’s reasonableness requirement simply due to the potential intermingling of materials).

As the FBI has conceded a lack of probable cause to seize the additional drug test information, then its seizure and retention is an illegal search and seizure under the Fourth Amendment because the government erroneously relied on the plain view doctrine. (R. at 14.)

CONCLUSION

For the foregoing reasons, the Supreme Court of the United States should affirm the decision of the United States Circuit Court of Appeals for the Fourteenth Circuit to order the return of all property to the StarTests facility in Wythe.