

**No. 2009-H20**

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

**OCTOBER TERM, 2010**

---

**UNITED STATES OF AMERICA,**

**Petitioner,**

**vs.**

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

**Respondent.**

---

**ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR  
THE FOURTEENTH CIRCUIT**

---

**BRIEF OF THE RESPONDENT**

---

Team 4  
Counsel for Respondent  
January 13, 2010

## QUESTIONS PRESENTED

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

## TABLE OF CONTENTS

	<u>Page</u>
TABLE OF CONTENTS .....	iii
TABLE OF AUTHORITIES .....	v
OPINIONS BELOW .....	1
CONSTITUTIONAL PROVISIONS AND STATUTES INVOLVED .....	1
STATEMENT OF THE CASE .....	2
SUMMARY OF THE ARGUMENT .....	4
ARGUMENT .....	5
<b>I. THE CFL HAS STANDING TO BRING THIS LAWSUIT .....</b>	<b>5</b>
<b>A. The CFL’s Members Would Have Standing on Their Own to Seek the Return of Their Confidential Information and Test Results .....</b>	<b>5</b>
<b>B. The Interests the CFL Seeks to Protect Are Germane to the Organization’s Purpose .....</b>	<b>6</b>
<b>C. Participation of Individual CFL Players Is Not Required for the CFL to Bring This Lawsuit .....</b>	<b>7</b>
<b>II. THIS COURT SHOULD ADOPT THE APPROACH SET FORTH BY <u>UNITED STATES v. COMPREHENSIVE DRUG TESTING, INC.</u> TO AVOID ALLOWING A RUN AROUND OF THE FOURTH AMENDMENT IN DIGITAL EVIDENCE CASES .....</b>	<b>9</b>
<b>A. The Government Must Wave Reliance Upon the Plain View Doctrine in Digital Evidence Cases .....</b>	<b>10</b>
<b>B. Segregation and Redaction Must Be Either Done by Specialized Personnel or an Independent Third Party .....</b>	<b>11</b>
<b>C. Warrants and Subpoenas Must Disclose the Actual Risks of Destruction of Information as Well as Prior Efforts to Seize That Information .....</b>	<b>13</b>

D.	<b>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 Agents</b> .....	14
E.	<b>The Government Must Destroy or, If the Recipient May Lawfully Possess It, Return Non-responsive Data, Keeping the Issuing Magistrate Informed About the Progress</b> .....	15
III.	<b>EVEN IF THIS COURT DOES NOT ADOPT THE APPROACH OF THE NINTH CIRCUIT, THE EVIDENCE AGAINST OTHER CFL PLAYERS IS STILL INADMISSIBLE UNDER THE PLAIN VIEW DOCTRINE</b> .....	17
A.	<b>The Law Enforcement Officials Were Not Lawfully Present in the Location When They Gained Access to the Player’s Test Results Because the Warrant Was Overbroad</b> .....	18
i.	<b>The Warrant Was Not Particularized</b> .....	18
ii.	<b>The Warrant Was Unreasonably Broad</b> .....	20
B.	<b>The Officers Did Not Have a Lawful Right of Access to the Object</b> .....	23
C.	<b>The Incriminating Character of the Evidence Was Not Immediately Apparent</b> .....	25
	<b>CONCLUSION</b> .....	27

**TABLE OF AUTHORITIES**

<u>Cases</u>	<u>Page(s)</u>
<u>Account Services Corporation. v. United States</u> , No. 09 CV 1495 JM (RBB), 2009 U.S. Dist. LEXIS 76531, (S.D. Cal. Aug. 27, 2009) .....	15, 16
<u>Associated General Contractors of California, Inc. v. Coalition For Economic Equity</u> , 950 F.2d 1401 (9th Cir. 1991) .....	6, 8
<u>Coolidge v. New Hampshire</u> , 403 U.S. 443 (1971) .....	23
<u>Horton v. California</u> , 496 U.S. 128 (1990) .....	17, 18, 23, 25
<u>Hunt v. Washington State Apple Advertising Commission</u> , 432 U.S. 333 (1977) .....	5, 6, 7, 9
<u>International Union, United Automobile, Aerospace &amp; Agricultural Implement Workers of America v. Brock</u> , 477 U.S. 274 (1977) .....	6, 7
<u>Minnesota Federation of Teachers v. Randall</u> , 891 F.2d 1354 (1989). ....	7
<u>Pennsylvania Psychiatric Society v. Green Spring Health Services, Inc.</u> , 280 F.3d 278 (2002) .....	8, 9
<u>Pennell v. City of San Jose</u> , 485 U.S. 1 (1988) .....	5, 6
<u>Rakas v. Illinois</u> , 439 U.S. 128 (1978) .....	5
<u>Ramsden v. United States</u> , 2 F.3d 322 (9th Cir. 1993) .....	15, 16
<u>United Food &amp; Commercial Workers Union Local 751 v. Brown Group, Inc.</u> , 517 U.S. 544 (1996) .....	8
<u>United States v. Adjani</u> , 452 F.3d 1140 (9th Cir. 2006) .....	19, 20, 24
<u>United States v. Alexander</u> , 574 F.3d 484 (8th Cir. 2009) .....	26
<u>United States v. Burgess</u> , 576 F.3d 1078 (10th Cir. 2009) .....	19, 20
<u>United States v. Campos</u> , 221 F.3d 1143 (10th Cir. 2000) .....	12
<u>United States v. Carey</u> , 172 F.3d 1268 (10th Cir. 1999) .....	11, 25
<u>United States v. Comprehensive Drug Testing, Inc.</u> , 579 F.3d 989 (9th Cir. 2009) .....	9, 10, 14, 15, 16

<u>United States v. Fleet Management, Ltd.</u> , 521 F. Supp. 2d 436 (E.D. P.A. 2007) .....	14
<u>United States v. George</u> , 975 F.2d 72 (2nd Cir. 1992).....	18, 20, 21
<u>United States v. Hansel</u> , 524 F.3d 841 (8th Cir. 2008).....	24
<u>United States v. Hansel</u> , No. 06-CR-102-LRR, 2006 U.S. Dist. LEXIS 76683, (N.D. Iowa Oct. 20, 2006).....	25
<u>United States v. Hill</u> , 459 F.3d 966 (9th Cir. 2006).....	10, 11, 18, 20, 21, 22
<u>United States v. Riccardi</u> , 405 F.3d 852 (2005).....	18, 19, 20, 21, 22
<u>United States v. Spilotro</u> , 800 F.2d 959 (9th Cir. 1986).....	18
<u>United States v. Stierhoff</u> , 477 F. Supp. 2d 423 (D. R.I. 2007).....	25, 26, 27
<u>United States v. Taketa</u> , 923 F.2d 665 (9th Cir. 1991).....	5
<u>United States v. Tamura</u> , 694 F.2d 591 (9th Cir. 1982) .....	11, 12, 14
<u>Statutes</u> .....	<u>Page(s)</u>
Fed. R. Crim. P. 41(g).....	1, 2, 3, 6, 8, 15, 27
<u>Constitutional Provisions</u> .....	<u>Page(s)</u>
U.S. Const. amend. IV.....	Passim

## **OPINIONS BELOW**

The Colonial Football League (CFL) and StarTests, Inc. (StarTests) timely filed a motion before the District Court of Wythe under Fed. R. Crim. P. 41(g) in response to the FBI retaining test results conducted by StarTests and ordered by the CFL. R. at 1, 9. The district court denied the Rule 41(g) motion, finding that the information was lawfully seized and therefore there was no reason to require its return. R. at 1. The CFL and StarTests filed a timely appeal in the United States Circuit Court of Appeals for the Fourteenth Circuit. R. at 7. The basis for appeal was that the district court erred by (1) “upholding [a] search warrant despite its lack of particularity;” and (2) “applying the plain view doctrine in a digital evidence search and seizure case.” R. at 7. The Court of Appeals for the Fourteenth Circuit reversed the district court decision, R. at 7, finding that the search and seizure was in violation of the Fourth Amendment. R. at 17. The case was remanded with instructions to return all information and equipment to the StarTests’ facility. R. at 17. The Supreme Court of the United States granted certiorari to the government (the Petitioner in the case at bar). R. at 20.

## **CONSTITUTIONAL PROVISIONS AND STATUTES INVOLVED**

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.

U.S. Const. amend. IV.

When a party is aggrieved by an unlawful search and seizure he or she can motion for the return of the property under Federal Rule of Criminal Procedure 41(g) that provides:

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.

Fed. R. Cim. P. 41(g).

### **STATEMENT OF THE CASE**

Amid controversy surrounding the use of steroids among professional athletes in 2003 (2005 in the Appellate Court opinion) the CFL resolved to require athletes, of each franchise comprising the CFL, to undergo drug testing. R. at 1, 8. It was made clear that such testing was to remain private. R. at 1, 8. Athletes were told that no results would be used against any individual player, but rather they would serve as an indicator and benchmark for the CFL to determine whether it should continue testing athletes the following year. R. at 1, 8. If five percent or greater of the players tested positive for illegal steroids, the CFL would test again the following year. R. at 1. The CFL hired StarTests to administer the drug tests. R. at 1, 8. The players were assured that only the percentage of players who tested positive for illegal steroid use would be released to the CFL and to the public; all other information would remain confidential with StarTests. R. at 1, 8.

Starting in July 2008, the Federal Bureau of Investigation (FBI) began investigating five well-known players in the CFL. R. at 1, 7. From the Wythe City Lightning, the FBI investigated quarterback John Reynolds and wide receiver John Reeves. R. at 1, 7. From the Marshall Phoenixes, the Wythe City Lightning rivals, the FBI investigated Danny Rodriguez, Michael Fleming, and Ace Hall for distribution and use of illegal steroids. R. at 1, 7. After procuring a large sum of evidence against the five players, the FBI wanted to enhance its case by proving

that the athletes had actually tested positive for steroid use. R. at 8. Learning of the drug testing the CFL and StarTests conducted on all players, the FBI applied for a warrant to search and seize “all computer records, files, and equipment” regarding the drug tests administered by StarTests and ordered by the CFL. R. at 1-2, 8. The magistrate judge issued a sweeping warrant, but qualified it by (1) restricting the information they could search and seize to the five players the FBI had investigated; (2) designating trained personnel to decide whether equipment had to be removed from the premises; and (3) ordering that only “appropriately trained personnel” were to review the digital data and then pass on only information regarding the original five players investigated. R. at 8.

The FBI executed the warrant it obtained on November 1, 2008. R. at 2. Upon arriving at the StarTests facility in Millerville, the FBI agents realized that the data was contained in three separate computer systems, a procedure enacted in order to protect the athletes’ privacy. R. at 2. The first contained the players personal and health information. R. at 2. The second contained a database of numbers assigned to each player as an identifier. R. at 2. Lastly, the third computer included the test results, and linked those results to specific athletes by using an assigned number found in the second computer system. R. at 2. While matching the test results to the five players, the agents also matched and uncovered other player information and test results. R. at 2. After finding a myriad of other positive test results, the FBI decided to expand its investigation. R. at 2. The FBI returned StarTests’ equipment after thoroughly copying and duplicating all the hard drives. R. at 2. StarTests and the CFL filed a timely motion for the return of the copied material under Fed. R. Crim. P. 41(g), claiming that any evidence seized regarding players other than the five players included in the warrant constituted an illegal seizure. R. at 2-3.

## SUMMARY OF THE ARGUMENT

As more and more information is being stored digitally, the disparity between issuing warrants to seize digital information and the protection of citizens' Fourth Amendment rights becomes clearer. Investigators may uncover incriminating evidence on a computer or hard drive, to which they concededly have no lawful right to be searching or seizing, but may then pursue that evidence and later claim protection under the plain view doctrine. The nature of digital evidence, and the requirements imposed by the plain view doctrine, leaves a void in citizens' Fourth Amendment protection against unreasonable searches and seizures. In cases involving the search and seizure of digital data, the three-prong test of the plain view doctrine will almost always be satisfied. This grants investigators the ability to easily overstep the bounds of a warrant, whether purposely or inadvertently, and effectively strip a citizen of his or her Fourth Amendment right to be free from an unreasonable search or seizure.

This dire result has been approached and remedied with a straightforward and uncomplicated solution. Both the Ninth Circuit and the Fourteenth Circuit (lower court decision) have implemented five factors to stop the runaround of the Fourth Amendment that is created by applying the plain view exception in a digital evidence case. The factors include: (1) it should be insisted that the government waive reliance upon the plain view doctrine; (2) "segregation and redaction of the computer evidence must be either done by specialized personnel or an independent third party"; (3) "warrants must disclose the actual risks of destruction or concealment of information, as well as prior efforts to seize that information in other courts"; (4) "the government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by non-computer personnel agents"; and (5) "the government must destroy, or, if the recipient may lawfully possess it, return

non-responsive data.” R. at 17. By imposing those five restrictions, citizens’ Fourth Amendment rights are preserved, and investigators are not unduly burdened in their pursuit of law enforcement.

## **ARGUMENT**

### **I. THE CFL HAS STANDING TO BRING THIS LAWSUIT.**

An individual has standing to challenge the validity of a search or seizure if he or she was the one against whom the search or seizure was directed. Rakas v. Illinois, 439 U.S. 128, 134-35 (1978). An association may also have standing to challenge the validity of a search or seizure on behalf of its members whose rights may have been violated if (1) the association’s members would otherwise have standing to sue in their own right; (2) the interests the association 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, 342-43 (1977). Additionally, a party challenging the validity of a search or seizure must have a reasonable expectation of privacy. United States v. Taketa, 923 F.2d 665, 669 (9th Cir. 1991).

#### **A. The CFL’s Members Would Have Standing in Their Own Right to Seek the Return of Their Confidential Information and Test Results.**

The first requirement of the association standing test is that the association’s members would otherwise have standing to sue in their own right. Hunt, 432 U.S. at 342-43. This Court in Pennell v. City of San Jose granted standing to a landlord association because each member of the association would have had standing to sue, due to the hardship they would face as a result of the City’s plan to use various private property for public use in violation of the Fifth Amendment. Pennell v. City of San Jose, 485 U.S. 1, 7-8 (1988). The Ninth Circuit similarly granted standing to an organization of construction contractors because each member of the

organization would have suffered an injury if they could demonstrate that the city ordinance, giving bidding preference to minority business enterprises, caused a legally cognizable injury. Associated Gen. Contractors of Cal., Inc. v. Coalition for Econ. Equity, 950 F.2d 1401, 1407 (9th Cir. 1991). While it ultimately found the organization could not prevail on the merits, the Ninth Circuit noted that this Court has only denied standing to organizations when the alleged injury is either too speculative, or its members had not in fact suffered a legally cognizable injury. Id.

Each CFL player whose test results were confiscated has the right to seek the return of his confidential information under Fed. R. Crim. P. 41(g). There were many players whose test results were swept up in the FBI seizure of StarTests' computers, in addition to those five players suspected of illegal steroid use. R. at 2, 9. Each of the players, whose test results were unintentionally collected, had an expectation of privacy of their test results, R. at 1, 8, and should have the right to request the return of their private information, or move to suppress the evidence, should it be used against them. Similar to the situations in Pennell and Associated General Contractors of California, where each member of the association or organization would have had individual standing to sue as a result of an invasion of a legal right, each CFL player affected has an individual right to sue. As such, the association has standing because each CFL player would have standing on his own.

**B. The Interests the CFL Seeks to Protect Are Germane to the Organization's Purpose.**

The second requirement of the association standing test is that the interests being sought to be protected by an organization or association are germane to the organization's purpose. Hunt, 432 U.S. at 342-43. This Court granted standing to the United Auto Workers Union (UAW), in International Union, United Automobile, Aerospace and Agricultural Implement Workers of America v. Brock, because the Court determined that a workers union exists to

protect the interests of its members. Int'l Union, United Auto., Aerospace and Agric. Implement Workers of America v. Brock, 477 U.S. 274, 287 (1977). Because of the union's purpose, the action brought by the union, on behalf of its members, involving a dispute regarding wages and benefits, was germane to the organization's purpose. Id.

The Eighth Circuit, however, denied standing to the Minnesota Federation of Teachers because a suit regarding taxpayer funding of sectarian schools was not germane to the organization's purpose. Minn. Fed'n of Teachers v. Randall, 891 F.2d 1354, 1359 (1989). The court held that the Teachers Federation was not an organization of taxpayers and there was nothing about the organization's purpose that would be germane to the interests it sought to protect. Id.

The CFL has the obligation to protect and represent the interests of the players, as stated in their contracts. R. at 3, 10. Similar to the UAW in Brock, one of the purposes of the CFL is to represent the players, which would include protecting the players from unreasonable invasions of privacy arising out of actions taken by the CFL itself. The contractual relationship between the CFL and its players includes the protection of the players' privacy, which would certainly include privacy issues arising from the content of the players' bodily fluids. R. at 10. Unlike the teachers' federation in Randall, the interests the CFL seeks to protect are directly related to the organization's purpose of protecting the interests of their players. Therefore, the interests the CFL seeks to protect are germane to the organization's purpose.

**C. Participation of Individual CFL Players is Not Required for the CFL to Bring This Lawsuit.**

The final requirement for an association to have proper standing to bring suit on behalf of its members is that neither the claim asserted, nor the relief requested, requires the participation of individual members in the lawsuit. Hunt, 432 U.S. at 342-43. Suits involving claims of

monetary relief usually require individual participation of the injured parties, and courts have generally held that an organization cannot bring such a claim on behalf of its members. United Food & Commercial Workers Union Local 751 v. Brown Group, Inc., 517 U.S. 544, 546 (1996).

The Ninth Circuit granted standing to the contractors association in Associated General Contractors of California, Inc. because the court determined that individual participation of the organization's members was not required in order to request injunctive relief against the City of San Jose. Associated Gen. Contractors of Cal., Inc., 950 F.2d at 1408. The Third Circuit similarly granted standing to the Pennsylvania Psychiatric Society, in Pennsylvania Psychiatric Society v. Green Spring Health Services, Inc., because the organization's claim that its members' rights were violated by the policies and procedures of managed care organizations did not require participation of the organizations members. Pa. Psychiatric Soc'y v. Green Spring Health Servs., Inc., 280 F.3d 278, 286-87 (2002). While the court noted that the nature of the tort claims in the suit could potentially require the involvement of individual members at trial, the court stated that it must accept all material allegations as true and construe the complaint in favor of the plaintiff, as required by the standard of review for the sufficiency of pleadings. Id. Consequently, because the Pennsylvania Psychiatric Society maintained the suit would not require individual participation of its members, standing was granted. Id.

The CFL seeks the return of the players' confidential drug test information under Fed. R. Crim. P. 41(g). The CFL is not seeking monetary damages, as this Court in United Food & Commercial Workers Union Local 751 noted that would generally preclude an organization from bringing suit on behalf of its members. United Food & Commercial Workers Union Local 751, 517 U.S. at 546. Similar to the contractors association in Brock, in which the organization

sought an injunction, the CFL only seeks the return of the players' test results. Such a suit does not require individual participation of individual members of the association.

Additionally, as the Third Circuit noted Pennsylvania Psychiatric Society, the standard of review for the sufficiency of pleadings requires the court to accept all material allegations as true and construe the complaint in favor of the plaintiff. Pa. Psychiatric Soc'y, 280 F.3d at 286-87. Given the sufficiency of pleadings requirements, and because the CFL maintains that the suit would not require individual participation of its players, the Court should construe the motion in favor of the moving party and grant the organization standing to bring this suit.

The CFL has met the requirements of the association standing test outlined in Hunt. Each player would have standing to seek the return of his own test results, the interests the CFL seeks to protect are germane to the organization's purpose, and neither the claim asserted, nor the relief requested requires the participation of any CFL players in the suit. As such, the CFL has standing to seek the return of its players' confidential test results that were swept up in the seizure of StarTests' computers.

**II. THIS COURT SHOULD ADOPT THE APPROACH SET FORTH BY UNITED STATES v. COMPREHENSIVE DRUG TESTING, INC. TO AVOID ALLOWING A RUN AROUND OF THE FOURTH AMENDMENT IN DIGITAL EVIDENCE CASES.**

In applying the plain view doctrine to cases involving the search or seizure of digital data, the particularity requirement of the warrant must be heightened. Failure to do so will otherwise result in allowing a sweeping search that would enable officers or government agents to have access to a vast amount of digitally stored personal and confidential information. Without a heightened particularity requirement, the elements of the plain view doctrine will always be satisfied and will provide a "run around" the Fourth Amendment. In order to safeguard and protect Fourth Amendment rights and the privacy of citizens, five restrictions must be imposed:

(1) the government must waive reliance upon the plain view doctrine in digital evidence cases; (2) an independent third party or specialized personnel must segregate or redact the information; (3) the actual risks and possible destruction to the information must be disclosed along with any prior efforts to seize the material; (4) the government must design its searches to uncover only the information for which it has probable cause, and it may only search that information; and (5) the government must destroy or return non-responsive data if the recipient may legally possess it. United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1006 (9th Cir. 2009).

**A. The Government Must Wave Reliance Upon the Plain View Doctrine In Digital Evidence Cases.**

Waiving the reliance upon the plain view doctrine is the only reasonable approach to dealing with digital searches, given the vast amount of information and the complex techniques with which it can be stored. Waiving reliance on the plain view doctrine in a digital evidence case maintains the “privacy of materials that are intermingled with seizable materials” and avoids turning searches for specific material into general exploratory searches. Id. at 998. If reliance on the plain view doctrine is not waived, then the government may search every file and every folder looking for any incriminating information with no incentive to contain its search to what is prescribed in the warrant. The government would be able to seize anything it wishes, and later claim that all the information that it came into contact with was in plain view. As the court stated in Comprehensive Drug Testing, investigators cannot be allowed to have the approach: “let’s take everything back to the lab, have a good look around and see what we might stumble upon.” Id.

In United States v. Hill, a warrant allowed officers to seize anything they wanted for later sorting. United States v. Hill, 459 F.3d 966, 986 (9th Cir. 2006). In that case, the government was investigating an individual for two photos that a computer technician had viewed on his

computer. Id. While the warrant authorized the seizure of the defendant’s computer, the officer never found the computer and instead seized computer storage media and zip disks in the defendant’s room and other equipment they felt was consistent with the warrant. Id. at 969. The officers proceeded to search all of the seized equipment the defendant had in his room, and never once searched the computer for which they were originally granted the warrant. Id.

Similarly, in the present case, the plain view doctrine has been used to allow the government to seize and search all the digital equipment that StarTests owns, and all information regarding the drug tests the CFL ordered. The government has been allowed to expand its search to examine all the directories and test results from all players, instead of limiting the search to the five suspected players identified in the warrant. Similar to Hill, the government was allowed to search all of the databases until more incriminating evidence was found, and then claim that evidence is admissible under the plain view doctrine. This creates a “run around” to the protections of the Fourth Amendment, and leaves citizens and their privacy in a vulnerable position.

**B. Segregation and Redaction Must Be Either Done By Specialized Personnel or an Independent Third Party.**

The first reasonable and effective step in stopping a “run around” of Fourth Amendment protections is to require evidence searched and analyzed by an individual other than an investigating officer or agent. Courts have indicated a need for an “intermediate step of sorting various types of documents” when computers have a multitude of documents. United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999). This safeguard is triggered in a digital evidence case when a “neutral, detached magistrate” monitors the seizure and later sorts the obtained evidence, prior to the investigators analyzing the evidence. United States v. Tamura, 694 F.2d 591, 596 (9th Cir. 1982). Additionally, the American Law Institute Model Code of Pre-

Arrest Procedure states that if documents cannot be seized and searched without examining other documents, then there must be extra steps taken to safeguard those other documents. Id. at n.3. Any other wholesale search and seizure would be unreasonable. Id. at 596. In the present case a neutral third party was not responsible for uncovering the information. Rather, investigators were responsible for locating the five players' results in the database, and in the process uncovered all players' test results.

Tamura further explains that the presence of intermingled documents, which are frequently found in computers, must be treated with special care, “[i]f the documents to be seized cannot be searched for or identified without examining the contents of other documents, or if they constitute . . . other documents containing matter not specified in the warrant, the executing officer shall not examine the documents” but should take other actions to protect the individuals privacy and await further instructions. Id. at 596.

In United States v. Campos, the Tenth Circuit expressed the same concerns regarding crucial limitations on computer searches because of the intermingling of documents. United States v. Campos, 221 F.3d 1143, 1148 (10th Cir. 2000). In Campos, the court noted the special approach needed for intermingled documents, which included an intermediate step to sort the documents in order to assure that only those documents specified in the warrant are searched. Id. If the documents are so intermingled, such as in the present case, then the officers must hold the documents and wait for further instructions on how to properly search the documents to avoid placing themselves in a situation that would infringe upon a citizens' Fourth Amendment rights. Id.

The numerous databases, concealed test result numbers, and jumbled test results in the current case, present a perfect example of intermingled documents. When investigators

discovered that the information they sought was contained on three separate computers and was concealed to maintain privacy, they should have sealed the documents and allowed specialized personnel or a third party to search through the databases and gather the test results of the five players with which they were authorized to search. If investigators fail to take this step, whenever a warrant is issued that includes the search of a computer, the officers or agents will have almost unlimited discretion in what information they are able to search and seize.

**C. Warrants and Subpoenas Must Disclose the Actual Risks of Destruction of Information as Well as Prior Efforts to Seize that Information.**

Because of the nature of digital evidence and the potential amount of information accessible to investigators, the risks and prior efforts to access such evidence must be disclosed to the court issuing the warrant. In the current case, and as the lower court found, investigators were not required to inform the CFL or StarTests of the risks of destruction or concealment. R. at 14. StarTests, because it is good business and because of contractual agreements, has a duty to keep the test results confidential. R. at 14. The need for confidentiality caused StarTests to store the test result data on three separate computers, with each player's results being linked to a number, rather than his name. Investigators could have easily found the identification number in one database, and then matched those five numbers with the results linked to the five players, which they were authorized to search. R. at 14. The investigators had no need to breach the confidentiality that StarTests was providing, go outside the scope of the warrant issued, or risk the destruction and loss of files by searching through all the databases. R. at 14. If the investigators found it necessary to place the equipment and information at risk, they should have disclosed those risks in the warrant.

**D. 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 Agents.**

Limiting search protocols to the bounds of the probable cause on which the warrant is based, is both reasonable and consistent with principles of the plain view doctrine as well as the basic principles of Fourth Amendment protections. The Ninth Circuit condemned the action of searching evidence beyond that for which the probable cause allowed, by stating that “the wholesale seizure for later detailed examination of records not described in the warrant is significantly more intrusive and has been characterized as the kind of investigatory dragnet that the [F]ourth [A]mendment was designed to prevent.” Tamura, 694 F.2d at 595.

In situations in which officers have no specific guidance in searching electronic databases, courts have often suppressed the resulting evidence. United States v. Fleet Mgmt., Ltd., 521 F. Supp. 2d 436 (E.D. P.A. 2007). In Fleet Management, the officers had “unbridled discretion” and lacked guidance in their search. Id. at 443. Similarly, the investigators in the present case had no guidance in their search, and had unbridled discretion to seize any information or equipment that they felt was important or necessary. R. at 15. This opens the door to endless violations of a citizen’s Fourth Amendment rights. When investigators are not given clear guidelines they are able to rummage through files and later rely on the plain view doctrine to excuse searching beyond what they have probable cause for or what they are authorized to search for. These actions, whether purposeful or unintentional, are a clear violation of the fundamental right to be free from unreasonable searches and seizures that all citizens possess. Id. at 447. As the Ninth Circuit stated in Comprehensive Drug Testing when faced with facts very similar to the case at bar, “if the government is allowed to seize information pertaining to ten names, the search protocol must be designed to discover data pertaining to those ten names

only, not to others, and not those pertaining to other illegality.” Comprehensive Drug Testing, 579 F.3d at 999.

**E. The Government Must Destroy or, if the Recipient May Lawfully Possess It, Return Non-responsive Data, Keeping the Issuing Magistrate Informed About the Progress.**

Federal Rule of Criminal Procedure 41(g) states that “a person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property’s return.” Fed. R. Crim. P. 41(g). In instances where the party making the motion has no criminal charges being brought against them, it is a petition to invoke the court’s equitable jurisdiction. Account Servs. Corp. v. United States, No. 09 CV 1495 JM (RBB), 2009 U.S. Dist. LEXIS 76531, at \*5-6 (S.D. Cal. Aug. 27, 2009). Under Fed. R. Crim. P. 41(g), there are four factors to be balanced in order to determine whether the government may retain possession of the property, or whether the court must order its return. Ramsden v. United States, 2 F.3d 322, 324-25 (9th Cir. 1993). The four factors are: (1) “whether the government displayed a callous disregard for the constitutional rights of the movant; (2) whether the movant has an individual interest in and need for the property he wants returned; (3) whether the movant would be irreparably injured by denying return of the property; and (4) whether the movant has an adequate redress of his grievance.” Id.

In Comprehensive Drug Testing, the court ordered the return of property under Fed. R. Crim. P. 41(g). Comprehensive Drug Testing, 579 F.3d at 1001. In that case, the movant was not attempting to suppress any evidence, but rather it was acting to protect the integrity of the company, Comprehensive Drug Testing, Inc. (CDT), and the Players Association was acting to protect its members. Id. at 1001. Similarly, in the current case, StarTests desires to have its equipment returned to protect the company’s integrity, confidentiality agreements, and good

name. R. at 9. The CFL desires the return of the information to protect its clients and their privacy. R. at 9. In Comprehensive Drug Testing, the court quickly and easily came to the conclusion that the movant was “(1) plainly aggrieved by the deprivation, and (2) likely to suffer irreparable injury if it’s not returned.” Id. at 1002. Further, the government had wrongfully obtained the documents, and thus should not be rewarded for its wrongdoing. Id. at 1003.

In contrast, in Account Services Corporation v. United States, the court declined to order the return of property, as the four requirements were not met. Account Servs. Corp., 2009 U.S. Dist. LEXIS 76531, at \*13. First, the court did not find any “callous disregard” for the movant’s constitutional rights because the seizures were conducted according to warrants based on “neutral and independent” findings of probable cause. Id. at \*8. Secondly, the court held the company’s interest in the seized property as “neutral” because the need for the company to pay debts and avoid liability underscored the exigent circumstances the government used to seize the funds. Id. at \*9. Third, the court felt that the potential liability of only losing funds was not irreparable harm since damages given can remedy economic injuries, unlike the potential loss of a football player never being able to step on the field again. Id. at \*10. Fourth, unlike the CFL, the company in Account Services had another adequate legal remedy: “an ancillary proceeding in the criminal action itself.” Id. at \*12.

The facts in the current case are strikingly similar to those in Comprehensive Drug Testing, suggesting that the Court should consider the ruling found in Comprehensive Drug Testing, with the Court ordering the return of the wrongfully seized and retained property. As noted by the circuit court, the government effectively shut down the StarTests facility when it seized all of the company’s equipment. R. at 16. Applying the four balancing factors that were established in Ramsden to the current case results in all of the information unlawfully seized by

investigators being returned to StarTests and the CFL. First, the lower court has categorized the investigators actions as a “callous disregard” for StarTests’ and the CFL’s constitutional rights. R. at 16. The government is attempting to keep StarTests’ property for evidence in an investigation it was not involved with until after uncovering information that was beyond the scope of the warrant and to which it had no probable cause for. R. at 16.

Secondly, both the CFL and StarTests have a strong need and interest in having the information returned. The CFL has a duty to protect the privacy of its players and StarTests has a need to protect its company and the integrity of its confidentiality contracts. R. at 16. Third, both the CFL and StarTests could be irreparably damaged. The CFL could face lawsuits for breach of confidentiality agreements and players could be removed from playing. R. at 16. StarTests cannot operate without its equipment, and could be irreparably damaged by having its confidentiality agreements compromised. R. at 16. Lastly, no other remedy would suffice in this case. Only the return of the information and equipment can remedy the damages suffered by the CFL and StarTests. R. at 16. No other option is available to rectify the damage caused by the confidentiality breach and loss of reputation. R. at 16.

**III. EVEN IF THIS COURT DOES NOT ADOPT THE APPROACH OF THE NINTH CIRCUIT, THE EVIDENCE AGAINST OTHER CFL PLAYERS IS STILL INADMISSIBLE UNDER THE PLAIN VIEW DOCTRINE.**

The Fourth Amendment prohibits unreasonable searches and seizures. U.S. Const. amend. IV. A law enforcement officer may, however, lawfully seize evidence of a crime without a warrant, under the plain view doctrine, if (1) the officer was lawfully in the position from which he viewed the object seized in plain view; (2) the officer had a lawful right of access to the object itself; and (3) the object’s incriminating character was immediately apparent Horton v. California, 496 U.S. 128, 134-35 (1990).

**A. The Law Enforcement Officials Were Not Lawfully Present in the Location When They Gained Access to Other CFL Player’s Confidential Test Results.**

The first requirement of the plain view doctrine is that a law enforcement official must lawfully be in the location from which he or she viewed the evidence seized in plain view. Id. When a law enforcement officer gains access to a location through a warrant, in order for the officer to be lawfully present, the warrant must be valid. Hill, 459 F.3d at 973. Validity of a warrant is determined by its specificity, which is measured by two aspects: (1) the warrant’s particularity and (2) its breadth. Id. Both aspects are analyzed in light of the circumstances of the case and the type of items or property involved. Id.

**i. The Warrant Was Not Particularized.**

The Fourth Amendment requires that a warrant particularly describe the place to be searched, or things to be seized. United States v. Spilotro, 800 F.2d 959, 963 (9th Cir. 1986). A warrant is sufficiently particular if it enables the officer executing the warrant to ascertain and identify with reasonable certainty the specific items that the magistrate or judge has authorized the officer to search or seize, based upon probable cause. United States v. George, 975 F.2d 72, 75 (2nd Cir. 1992). The purpose of the particularity requirement is to prevent general, exploratory searches that would unreasonably infringe on a citizens’s Fourth Amendment rights. Spilotro, 800 F.2d at 963.

The Second Circuit held in United States v. George that the warrant was unreasonable because it failed to state with particularity what was being searched or seized and authorized a broad search for “all evidence of a crime.” George, 975 F.2d at 75-76. The court stated that the authorization that officers may seize “any other evidence relating to the commission of a crime,” without identifying any specific items, was too broad and was not sufficiently particular. Id.

The Tenth Circuit similarly held in United States v. Riccardi that a warrant was not

sufficiently particular because it did not contain a detailed description of the computer files being sought. United States v. Riccardi, 405 F.3d 852, 858 (10th Cir. 2005). Instead, the warrant authorized officers to seize Riccardi's personal computer and all other media storage devices and search everything for evidence of child pornography. Id. The court concluded that the warrant failed the particularity requirement because it did not state any specific files being sought or the suspected location of those files. Id.

The Ninth Circuit, however, in United States v. Adjani upheld a warrant because it particularly described the items to be searched and seized. United States v. Adjani, 452 F.3d 1140, 1148 (9th Cir. 2006). The court stated that the warrant was sufficiently particular because it described in detail the nature of the communications sought between the three suspected individuals and the types and nature of the documents being sought relating to the extortion investigation. Id. The Tenth Circuit in United States v. Burgess also held that a warrant was sufficient particular that allowed officers to search a personal computer for evidence of a specific kind of drug and drug trafficking of a specific controlled substance. United States v. Burgess, 576 F.3d 1078, 1091-92 (10th Cir. 2009). While the court noted that on its face the warrant lacked specific details of the items to be searched, the supporting affidavit included a detailed list of items to be searched on the computer. Id.

The warrant authorizing the FBI to search and seize StarTests' computers and files was not particular. The warrant allowed the agents to seize urine samples and documents, as well as all computer records, files and equipment relating to the steroid testing of the five suspected players. No where does the warrant, or the supporting affidavits, detail the nature and type of computer records and files being sought, or their suspected location.

Similar to Riccardi, the warrant in this case failed to state the nature and type of files

being sought on the computers and media storage devices. Unlike the warrants in Burgess and Adjani, which specifically stated the types and nature of the files being sought, the warrant in this case allowed the investigators to seize all files related to the StarTests administered tests, without describing the specific files being sought or their suspected location. Therefore, the warrant failed to state with particularity the nature and type of the specific documents being targeted in the warrant.

**ii. The Warrant Was Unreasonably Broad.**

The second requirement of a valid warrant is that its breadth must be reasonably limited by the probable cause upon which the warrant is based. Hill, 459 F.3d at 973. The purpose of the breadth requirement is to ensure that a warrant does not allow for a “wide-ranging, exploratory search” looking for evidence of a crime. George, 975 F.2d at 75.

As noted above, the Second Circuit held the warrant in question in United States v. George failed to state with particularity the items to be searched or seized. George, 975 F.2d at 75-76. The court also noted that the warrant was unreasonably broad because it stated that officers were able to seize “any other evidence relating to the commission of a crime.” Id. The court stated that the warrant was unreasonably broad because it allowed the officers to go beyond the scope on which the probable cause for the warrant was based, which was investigating a robbery at a McDonald’s restaurant. Id.

Similarly, the Tenth Circuit in Riccardi held a warrant was unreasonably broad because it allowed officers to seize Riccardi’s computer and all electronic and magnetic media, such as CD-ROMs and removable media drives, without specifying the specific nature and suspected location of the incriminating files. Riccardi, 405 F.3d at 862. The court stated that officers conducting searches cannot conduct a sweeping, comprehensive search of a computer’s hard drive, unless such a search would be supported by probable cause. Id. The court stated:

Because computers can hold so much information touching on many different areas of a person's life, there is a greater potential for the "intermingling" of documents and a consequent invasion of privacy when police execute a search for evidence on a computer. . . . Officers must be clear as to what it is they are seeking on the computer and conduct the search in a way that avoids searching files of types not identified in the warrant.

Id. The Ninth Circuit, however, in United States v. Hill held that a warrant was reasonable, even though it allowed the search and seizure of a personal computer and all electronic media related to it for purposes of looking for images containing sexually explicit acts involving minors. Hill, 459 F.3d at 968. The court reasoned that given the nature of the suspected child pornographic images and the fact that the images were discovered while the computer was being serviced at a computer store, the warrant could not be any more specific given the nature and circumstances of the case. Id. at 973-74. The court noted the difficulty in obtaining a warrant to search a computer for child pornography when the images could have been disguised or were not readily visible. Id. While the court noted that such difficulties usually result in a broader warrant, the warrant must nonetheless be no broader than is reasonably permissible given the facts and circumstances of the case and the probable cause. Id.

The warrant in the current case allowed agents to seize and search all of StarTests computer equipment and storage devices. This enabled them to conduct a sweeping search that extended beyond the scope of the probable cause for test results of the five suspected players. This form of search was exactly the kind that the court in George sought to prevent. This case is very similar to Riccardi, in which the court held a warrant was overbroad, because it allowed the seizure of all StarTests' computers and other media storage devices, without reasonably narrowing the scope of the search to specific files or documents involving the five suspected players. As the court noted in Riccardi, when searching a computer there is a much greater possibility for an invasion of privacy, due to the amount of information usually stored on an

individual's or company's computers, and investigators must tailor the search or seizure only to the files or documents absolutely necessary. Riccardi, 405 F.3d at 862. The warrant that enabled agents to search and seize StarTests' computers did not limit their search only to those files and documents necessary to their investigation. Instead, the warrant allowed for the search and seizure of all computers and media storage devices where there was even a possibility that documents relating to the drug testing could be found.

Unlike in Hill, where the broad language of the warrant was reasonable because of the circumstances of that case, the warrant in the current case enabled the FBI to seize all of StarTests' computers and equipment that related to the drug testing. While the supporting affidavit allowed for a broader search because of the volume of information, potentially misleading file names, and the potential for encountering decrypted files, the probable cause only extended to the test results for the five suspected individuals. Even though there may have been challenges to obtaining the files relating to the test results of the suspected players, allowing agents to seize all computers and media storage relating to testing was unreasonable. There were only five suspected players that the FBI was investigating and the warrant should have been tailored to specific documents relating to those five individuals. Instead, the warrant allowed the investigators to have access to thousands of test results that were in no way related to the steroid investigation of five CFL players. Therefore, the warrant was overbroad and unreasonable.

The warrant was unreasonable because it lacked particularity and was overbroad. As such, the investigators were not lawfully in the location when they observed the incriminating evidence. Because law enforcement officers or agents must lawfully be in the location from which they viewed the incriminating objects or items seized under the plain view doctrine, the evidence was illegally seized. Therefore, the evidence fails the first requirement of the plain

view doctrine as espoused in Horton and is inadmissible.

**B. The Officers Did Not Have a Lawful Right of Access to the Object.**

The second requirement of the plain view doctrine is that investigators must have a lawful right of access to the information or objects in question at the time the incriminating evidence was first seen. Horton, at 136-37. Warrantless seizures of material are prohibited by the Fourth Amendment. Id. at 137 n.7. No amount of probable cause can justify a warrantless seizure. Id. Simply because an object's incriminating nature is plainly seen, an officer does not have the lawful right of access to seize an object absent other circumstances. Id. at 137. If a valid warrant allows an officer to enter a location, giving him or her a lawful right of access, the officer may seize incriminating evidence he or she may encounter under the plain view doctrine. Id. at 136. The presence of a valid warrant gives the officer a right of access to material that is not directly connected with the authorized search. Id. As the lower court noted, if an officer is lawfully present, then he has a lawful right of access to the object the officer has come across that is unconnected to the initial search. R. at 11. 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." Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971).

The application of the plain view doctrine in a digital evidence case, however, drastically alters the foundational purposes of the doctrine. The Fourteenth Circuit noted the disturbing results when it applied the plain view doctrine to the current case. R. at 12. The lower court acknowledged a differing result, and reasoned that "[i]n the case of a computer, however, gaining access to the desktop is the same as having access to all the files in the My Computer file folder." R. at 11. In digital evidence cases, the government is able to obtain a warrant for a computer and then proceed to search and seize any evidence or information from a computer with the first two prongs of the plain view exception being satisfied. R. at 12. For example, in

Adjani, the government obtained a warrant to seize a defendant's computer, storage devices, and hard drives. Adjani, 452 F.3d at 1144. The warrant stated that in order to determine what data was necessary, the government would need to search all data and any computer equipment it deemed necessary to search. Id. In that case, the presence of a warrant allowed the officers to meet the first two prongs of the plain view doctrine, search anything they could locate related to a computer, including the computer of the defendant's girlfriend, and rummage through the computers to find incriminating evidence. Id. This is the type of disturbing example that Justice Freehouse references in the lower court opinion when speaking of illogical results and run-arounds of the Fourth Amendment. R. at 12.

In contrast, a valid warrant outside the context of a digital evidence case can provide an investigator with the lawful right of access to an incriminating object that is in plain view. In United States v. Hansel, the warrant provided the officers the authority to search a defendant's residence. United States v. Hansel, 524 F.3d 841, 843 (8th Cir. 2008). Thus when the officers found child pornography computer printouts in the defendant's bedroom, they were found to have a lawful right of access. Id. at 843. They were validly in the defendant's home through the warrant and, therefore, had a lawful right to access to the printouts sitting on the table, which were obviously and immediately incriminating. Id.

In the current case, dealing with digital evidence, however, the investigators were not lawfully present because they did not have a valid warrant. Because the warrant did not meet the particularity and breadth requirements, the investigators did not have a lawful right of access to any other test results beyond the five players to which they had probable cause, and had no lawful right to continue to decipher other players' test results.

**C. The Incriminating Character of the Evidence Was Not Immediately Apparent.**

The final requirement of the plain view doctrine requires that the incriminating character of the evidence be immediately apparent. Horton, 496 at 137. To satisfy this requirement, there must be probable cause to associate the property with incriminating activity. United States v. Hansel, No. 06-CR-102-LRR, 2006 U.S. Dist. LEXIS 76683, at \*17 (N.D. Iowa Oct. 20, 2006). Probable cause requires that “the facts available to the officer would ‘warrant a man of reasonable caution in the belief’ that certain items may be . . . useful as evidence of a crime.” Id. at \*18.

In United States v. Carey, an officer came across a computer file, opened the file, and discovered a picture of child pornography. Carey, 172 F.3d at 1273. After viewing that photo, the officer, who believed there were more incriminating photos, continued to open files in order to establish if there was more unlawful material. Id. Until he opened each file, it was unclear if the file contained incriminating material or not, thus the file contents themselves were not immediately apparent. Id. The court in Carey concluded that items seized were not admissible through the plain view doctrine and were not authorized by the warrant. Id.

Similarly, in the current case, the players’ test results and evidence of criminal activity was not clear until the officer began matching identifying numbers found in one computer with the test results that were found in another computer. The results themselves were not incriminating until the investigators took the next step to decipher and uncover which players’ name corresponded to those test result.

Furthermore, a file or document on a computer does not invite an investigator to search the computer to see if the contents are incriminating, the requirement dictates that the incriminating nature must be immediately apparent. United States v. Stierhoff, 477 F. Supp. 2d

423, 447 (D. R.I. 2007). In Stierhoff, the government argued, unsuccessfully, that file labels could be clearly incriminating on their face. Id. at 444. The government was investigating the individual in Stierhoff for stalking a college student and sending her numerous poems. Id. at 425. Officers began to search the defendant's computer for evidence of poems the defendant had written when they came across a file named "Offshore." Id. at 438, 439. Although the officer already had the information he came for, the officers continued searching the files, without obtaining a warrant, thinking that other files might contain evidence of criminal acts. Id. at 443. However, to lawfully continue searching the computer, the government should have first obtained another search warrant. Id. at 447. The court held that the plain view doctrine did not apply because the file was not "readily identifiable as contraband or evidence of a crime." Id. at 446. The officer had to open the files to see if they were incriminating. By reading the label "Offshore" no criminal activity was immediately apparent. Id. at 439. Further, the file was identical in "size, shape, and color to literally thousands of other folders." Id. at 446. When the officers in Stierhoff began searching the "Offshore" folder, the officers went beyond the search of the stalking investigation. Id. at 448.

In United States v. Alexander, a warrant specifically authorized the seizure of digital storage devices to investigate the defendant's potential invasion of privacy. United States v. Alexander, 574 F.3d 484, 487 (8th Cir. 2009). During the search of the residence, the officers came across email printouts showing a child pornography subscription. Id. at 487. Child pornography pictures were also found in the defendant's attic. Id. at 487. The court stated that the child pornography was immediately incriminating. Id. at 490. Because the very nature of the photographs was illegal, the incriminating character of the evidence was immediately apparent to the officers. However, in the present case, the incriminating character of the evidence was not

immediately apparent because of the jumbled test results, numerous passwords, and secret identifiers. The officers were required to do more work and take extra steps to determine what was incriminating.

The present case is very similar to Stierhoff. The identification numbers and results alone were not incriminating to the CFL players. It took an additional step by the investigators to match the corresponding identification number to an individual player's name to uncover any criminal activity. Prior to the investigators taking that step, there was nothing immediately incriminating or identifiable as a crime. The investigators admitted that after deciphering the test results, they expanded and went beyond the original search of the five players to include all players in the CFL. Because of the vast amount of information, and the reliance of one computer database on another, the investigators could have easily deciphered only the test results of the five players with which they had probable cause to obtain.

### **CONCLUSION**

Wherefore, in light of the foregoing reasons, this Court should affirm the opinion of the Fourteenth Circuit. The CFL has standing to bring this suit and the evidence should be returned under Fed. R. Crim. P. 41(g). The evidence is inadmissible under the plain view doctrine and this Court should hold that the government should not rely on the plain view doctrine in digital evidence cases. Furthermore, the Court should adopt the factors as provided in Comprehensive Drug Testing.

---

Team 4  
Counsel for the Respondent  
January 13, 2010