

**WILLIAM B. SPONG, JR.
INVITATIONAL MOOT COURT TOURNAMENT**

TEAM 18

No. 2009-H20

In the Supreme Court of the United States

OCTOBER TERM, 2010

UNITED STATES OF AMERICA

Petitioner,

-VERSUS-

STARTESTS, INC., and COLONIAL FOOTBALL LEAGUE

Respondent.

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

Team 18

Counsel for Respondents

January 13, 2010

QUESTIONS PRESENTED

- I. Does 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. Rule 41(g) when the professional football players have independent standing to sue, their interests are germane to the organization's purpose, and their claim does not require the players to be parties in the lawsuit?
- II. Should the plain view doctrine apply to the search and seizure of digital evidence when the nature of digital property is inherently different from physical property and when the plain view exception test as applied in digital evidence cases is too always satisfied and threatens to nullify Fourth Amendment protections?
- III. Should the particularity requirement of warrants be heightened in the digital evidence context as per the guidelines set for by the Fourteenth Circuit when intermingled information unsupported by probable cause is inherent in the digital evidence context?

TABLES OF CONTENTS

QUESTIONS PRESENTED i

TABLE OF AUTHORITIESv

CONSTITUTIONAL PROVISIONS AND STATUTES INVOLVED vii

OPINIONS BELOW.....1

STATEMENT OF THE CASE.....1

SUMMARY OF THE ARGUMENT4

ARGUMENT.....6

**I. THE COURT OF APPEALS FOR THE FOURTEENTH CIRCUIT
CORRECTLY HELD THAT THE COLONIAL FOOTBALL LEAGUE
HAS STANDING TO BRING A RULE 41(g) MOTION CHALLENGING
THE REASONABLENESS OF THE SEARCH AND SEIZURE.....7**

**II. THE PLAIN VIEW EXCEPTION SHOULD NOT APPLY TO DIGITAL
EVIDENCE BECAUSE IT THREATENS TO NULLIFY FOURTH
AMENDMENT SEARCH AND SEIZURE PROTECTIONS8**

**A. Digital Property Is Inherently Different From Physical Property, And
Application Of The Plain View Doctrine In Digital Evidence Cases May
Result In Transforming Digital Evidence Warrants Into General
Exculpatory Searches.....9**

**B. The Three-Prong Plain View Exception Test Applied In Digital Evidence
Cases Is Too Easily Satisfied And Thus Circumvents Well-Established
Search And Seizure Protections Under The Fourth Amendment.12**

**1. The First Prong Of The Plain View Exception Test Requiring That
A Police Officer Be Lawfully Present At A Place Where Evidence
Must Be Plainly Viewed Is Too Easily Satisfied When Applied In
Digital Evidence Cases.14**

**2. The Second Prong Of The Plain View Exception Test Requiring
That A Police Officer Must Have A Lawful Right Of Access To The
Object Is Too Easily Satisfied In Digital Evidence Cases.17**

3.	The Third Prong Of The Plain View Exception Test Requiring That The Incriminating Character Of The Object Be Immediately Apparent To The Police Officer Is Too Easily Satisfied In Digital Evidence Cases.....	19
C.	Reliance On The Plain View Doctrine In Digital Evidence Cases Is Misplaced, And The Ninth Circuit’s Standards In <i>Comprehensive Drug Testing</i> Should Be Adopted.....	20
III.	THE COURT OF APPEALS FOR THE FOURTEENTH CIRCUIT CORRECTLY HEIGHTENED THE PARTICULARITY REQUIREMENT BY IMPOSING GUIDELINES THAT FEDERAL MAGISTRATES MUST FOLLOW WHEN ISSUING SEARCH WARRANTS IN THE DIGITAL EVIDENCE CONTEXT.....	22
A.	This Court Should Adopt The Guidelines Set Forth In The Fourteenth Circuit For Issuing Warrants In The Digital Evidence Context Rather Than Permitting A General Warrant To Seize All Computer Equipment And Files For Later Sorting Because The Guidelines Are Consistent With This Court’s Jurisprudence And The Fourth Amendment.....	23
1.	The Heightened Particularity Requirement Strikes An Effective Balance Between The Rights Protected By The Fourth Amendment And The Needs of Law Enforcement Officials In Conducting Searches Of Digital Evidence.	25
a.	Insisting That The Government Waive Reliance Upon The Plain View Doctrine Protects An Individual’s Rights Under The Fourth Amendment While Permitting An Effective Search By Law Enforcement Officials.....	27
b.	Requiring That The Segregation And Redaction Process Be Performed Either By Specialized Personnel Or An Independent Third Party Who Agrees Not To Disclose Any Unresponsive Data Is Consistent With This Court’s Jurisprudence.....	31
c.	Requiring Disclosure Of The Actual Risks Of Destruction Or Concealment Of Information, As Well As Prior Efforts To Seize That Information In Other Courts, Strikes An Appropriate Balance Between Fourth Amendment Protections And The Ability To Conduct An Effective Search.....	35
d.	Requiring That The Government’s Search Protocol Is Designed To Uncover Only The Information For Which It	

Has Probable Cause Is Consistent With The Warrant Clause.	36
e. Requiring The Government To Destroy Or Return Non-Responsive Data Is Consistent With An Individual’s Constitutionally Protected Rights.	38
B. The 2009 Amendments To Fed. R. Crim. P. 41(g) Are Consistent With The Guidelines Set Forth By The Fourteenth Circuit	39
C. The Guidelines Assist Magistrates In Protecting An Individual’s Constitutionally Protected Rights When Magistrates Issue Warrants In Digital Evidence Cases	39
CONCLUSION	40

TABLE OF AUTHORITIES

	Page(s)
CASES	
<u>Andresen v. Maryland</u> , 427 U.S. 463 (1976).....	24
<u>Arizona v. Hicks</u> , 480 U.S. 321 (1987).....	15, 16, 19
<u>Boyd v. United States</u> , 116 U.S. 616 (1886).....	40
<u>Chimel v. California</u> , 395 U.S. 752 (1969).....	30
<u>Coolidge v. New Hampshire</u> , 403 U.S. 443 (1971).....	passim
<u>Horton v. California</u> , 496 U.S. 128 (1990).....	passim
<u>Illinois v. Gates</u> , 462 U.S. 213 (1983).....	24
<u>Johnson v. United States</u> , 333 U.S. 10 (1948).....	40
<u>Jones v. United States</u> , 357 U.S. 493 (1958).....	28
<u>Kitty’s East v. United States</u> , 905 F.2d 1367 (10th Cir. 1990)	38
<u>Kyllo v. United States</u> , 533 U.S. 27 (2001).....	24
<u>Maryland v. Garrison</u> , 480 U.S. 79 (1987).....	passim
<u>Oliver v. United States</u> , 466 U.S. 170 (1984).....	passim
<u>Payton v. New York</u> , 445 U.S. 573 (1980).....	23

<u>Pennell v. City of San Jose,</u> 485 U.S. 1 (1988).....	7
<u>Rakas v. Illinois,</u> 439 U.S. 128 (1978).....	7
<u>Ramsden v. United States,</u> 2 F.3d 322 (9th Cir. 1993)	38
<u>Stanford v. Texas,</u> 379 U.S. 476 (1965).....	26
<u>Trulock v. Freeh,</u> 275 F.3d 391 (4th Cir. 2001)	32
<u>United States v. Abrams,</u> 615 F.2d 541 (1st Cir. 1980).....	25
<u>United States v. Adjani,</u> 452 F.3d 1140 (9th Cir. 2006)	passim
<u>United States v. Alexander,</u> 574 F.3d 484 (8th Cir. 2009)	17
<u>United States v. Carey,</u> 172 F.3d 1268 (10th Cir. 1999)	19, 20, 32
<u>United States v. Comprehensive Drug Testing, Inc.,</u> 513 F.3d 1085 (9th Cir. 2008), <i>rev'd en banc</i> , 579 F.3d 989 (9th Cir. 2009)	25, 26
<u>United States v. Comprehensive Drug Testing, Inc.,</u> 579 F.3d 989 (9th Cir. 2009)	passim
<u>United States v. Dichiarinte,</u> 445 F.2d 126 (7th Cir. 1971)	14, 19, 20
<u>United States. v. Gonzalez Athehorta,</u> 729 F. Supp. 248 (E.D.N.Y 1990)	19
<u>United States. v. Gray,</u> 78 F. Supp. 2d 524 (E.D. Va. 1999)	15, 16
<u>United States v. Hill,</u> 459 F.3d 966 (9th Cir. 2006)	30
<u>United States v. Rabinowitz,</u> 339 U.S. 56 (1950).....	29

<u>United States v. Raney,</u> 342 F.3d 551 (7th Cir. 2003)	13, 14, 16
<u>United States v. Ross,</u> 456 U.S. 798 (1982).....	24
<u>United States v. Tamura,</u> 694 F.2d 591 (9th Cir. 1982)	21, 25, 32
<u>United States v. Turner,</u> 169 F.3d 84 (1st Cir. 1999).....	17
<u>United States v. Walser,</u> 275 F.3d 981 (10th Cir. 2001)	passim
<u>United States v. Wong,</u> 334 F.3d 831 (9th Cir. 2003)	14, 19, 20

OTHER AUTHORITIES

Aaron S. Lowenstein, <u>Commercial Electronic Databases</u> , 6 CARDOZO PUB. L. POL'Y & ETHICS J. 101 (2007).....	31
FED. R. CRIM. P. 41 advisory committee's note.....	39
Orin S. Kerr, <u>Searches and Seizures in a Digital World</u> , 119 HARV. L. REV. 531 (2005).....	9, 10
Raphael Winick, <u>Searches and Seizures of Computers and Computer Data</u> , 8 HARV. J.L. & TECH. 75 (1994)	24
Ray Ming Chang, <u>Why the Plain View Doctrine Should Not Apply to Digital Evidence</u> , 12 SUFFOLK J. TRIAL & APP. ADVOC. 31 (2007).....	10

CONSTITUTIONAL PROVISIONS AND STATUTES INVOLVED

FED. R. CRIM. P. 41	passim
U.S. CONST. AMEND. IV	passim

OPINIONS BELOW

The opinion of the United States Court of Appeals for the Fourteenth Circuit is not reported. It is reprinted in the Record at page 7. The opinion of the United States District Court for the District of Wythe is not reported. It is reprinted in the Record at page 1.

COUNTER STATEMENT OF THE CASE

This case involves the federal investigation of the distribution and use of illegal steroids in the Colonial Football League (“CFL”). (R. at 7.) The petitioner, the United States of America, established a case of probable cause that five CFL players were illegally procuring steroids. (R. at 7.) The government acquired a warrant to search all the computer data and files at StarTest, Inc.’s (“StarTests”) facility, and thereafter searched, seized, and copied data pertaining to every player in the CFL. (R. at 2.) The respondents, StarTests and the CFL, filed a motion for the return of the seized property pursuant to Fed. R. Crim. P. 41(g). (R. at 1.) The United States District Court for the District of Wythe denied the motion. (R. at 6.) Petitioner appealed the order of the United States Court of Appeals for the Fourteenth Circuit granting the return of all property. (R. at 16.)

A. The Government’s Search Warrant

In 2008, the Federal Bureau of Investigation (“FBI”) began an investigation of five well-known football players whom the government believed were taking steroids. (R. at 1.) After commencing its investigation, the FBI learned that StarTests had been administering drug-screening tests to all CFL players since 2005. (R. at 1.) The CFL had hired StarTests to conduct tests to determine what percentages of players were taking steroids. (R. at 1.) The players were assured that their names and test results would remain confidential. (R. at 1.) In 2008, the FBI

established a case for probable cause that “five” CFL players had tested positive for steroid use during the CFL testing. (R. at 1.)

The FBI applied for a search warrant of StarTest’s facility. (R. at 8.) The FBI made a “broad request” to search and seize “all computer records, files, and equipment” related to the drug tests because of the difficulties generally present in computer searches. (R. at 8.)

Computer searches are difficult because of the “massive” quantity of data at issue, the technical difficulties of locating and identifying files that may be hidden or mislabeled, and the necessity of using additional software. (R. at 8.) The magistrate judge issued the warrant. (R. at 8.)

The warrant authorized the FBI to “search computer equipment, storage devices, and – where an on-site search would be impracticable – seize either a copy of all data or the computer equipment itself.” (R. at 8.) The warrant contained only three restrictions: that the search be limited to information “reasonably related” to the investigation of the five players named in the warrant, that specialized personnel trained in searching computer data decide when “seizure and removal of computer equipment was necessary,” and that “appropriately trained personnel” review the acquired information, retain the responsive data, and return the remainder. (R. at 8.)

B. The Government’s Search

When the government executed the search warrant it learned of the “computer-hopping” procedure used by StarTests to maintain client confidentiality (R. at 8.) Essentially, this process involved three separate computer databases. The first computer database contained the names and personal health information of all the players; the second assigned each player an identification number; and the third contained the drug-testing results next to the assigned identification number, which did not include any player’s name. (R. at 8.) The government seized all of the computer equipment from the facility and searched the databases at its own

location. (R. at 9.) While the government acquired the data pertaining to the five players listed in the warrant, it also discovered positive steroid and narcotic results for many other players. (R. at 9.) The government copied and retained all of the data pertaining to positive test results and expanded the investigation to include all substance abuse by professional athletes. (R. at 9.)

C. The Decisions of the District Court and the Court of Appeals for the Fourteenth Circuit

The CFL moved for the return of the copied records and data under Fed. R. Crim. P. 41(g), claiming that the seizure of its player's medical tests was outside the scope of the warrant and violated the Fourth Amendment. (R. at 9.) In response, the government argued that the CFL did not have standing to file the motion. (R. at 10.) Next, the government "conceded a lack of probable cause to hold the additional information," but nevertheless argued that the plain view exception applied. (R. at 9.) The government argued that it did not need a warrant to seize the additional evidence, relying on the plain view doctrine. (R. at 4).

The United States District Court for the District of Wythe denied the motion. (R. at 1.) The District Court held that the CFL had standing to bring a Rule 41(g) motion because they satisfied the associational standing test. (R. at 3). The court also held that the search warrant was facially valid. (R. at 6). Additionally, the court held that the search and seizure satisfied the plain view doctrine because the FBI agents had lawful right of access to the computers and databases and that the incriminating nature of the data was immediately apparent. (R. at 6).

The CFL and StarTests appealed to the United States Court of Appeals for the Fourteenth Circuit claiming that the District erred by: 1) upholding the 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 affirmed the district court's holding that the CFL had standing. (R. at 10.) The Court of Appeals held that the warrant was invalid and imposed new

guidelines on magistrate judges when issuing warrants in digital evidence cases.¹ (R. at 17.)

The Court of Appeals reversed and remanded the case with instructions for the district court to enter an order for the return of all the seized equipment and data. (R. at 17.)

SUMMARY OF THE ARGUMENT

The decision of the Court of the Appeals for the Fourteenth Circuit should be affirmed for three reasons. First, the CFL has standing to bring a Rule 41(g) motion. Second, the government should not be able to rely on the plain view doctrine in digital searches. Third, the particularity requirement of the Fourth Amendment should be heightened in the digital evidence context as per the guidelines set forth by the Fourteenth Circuit.

I.

The CFL has standing to bring a motion under Rule 41(g). This Court has held that an association has standing to sue on behalf of its members when they would otherwise have independent standing to sue, the interests sought to be protected are germane to the organization's purpose, and the claim does not require the participation of the individual members of the lawsuit. The CFL is "aggrieved by an unlawful search and seizure" and satisfied this Court's three-prong associational test. The players have independent standing to sue, their privacy interests in the results are related to the CFL's organizational purpose, and since the players are only requesting the return of the results they do not need to be parties to the action.

II.

¹ First, magistrates should insist that the government waive reliance upon the plain view doctrine. Second, segregation and redaction of the computer evidence must be done by computer personnel or an independent third party. If performed by government personnel, the personnel must agree not to disclose any information outside the scope of the warrant. Third, warrants must disclose the actual risks of destruction or concealment of the information. Fourth, the government's search protocol must be designed to acquire only the information supported by probable cause. Finally, the government must destroy or return non-responsive data. (R. at 17.)

The plain view exception should not be applied in digital evidence cases because it threatens to nullify Fourth Amendment protections. The plain view doctrine is an exception to the Fourth Amendment warrant requirement, which allows police officers, during the execution of a warrant, to seize evidence of contraband or criminal wrongdoing technically outside the scope of the warrant. In order to satisfy the plain view exception test: an officer must be lawfully present at a place where evidence must be plainly viewed, the officer must have a lawful right of access to the object, and the incriminating character of the object must be “immediately apparent.” Horton v. California, 496 U.S. 128, 136–37 (1990). Typically, this exception applies in situations where police officers have a warrant to search a given area for specified objects and inadvertently discover some other object indicative of criminal activity during the course of the search.

Applying the plain view doctrine in digital evidence cases creates an end run around the Fourth Amendment. Since the nature applied of digital property is inherently different from physical property, application of the plain view doctrine in digital evidence cases transforms any warrant into a general warrant, which is prohibited by the Fourth Amendment. Additionally, the three-prong test is too easily satisfied in digital evidence cases. Here, the magistrate judge issued a broad warrant, authorizing the search and seizure of all of StarTests computers, files, and equipment. Therefore, FBI agents had lawful access to the computers and to the files, and easily satisfied the first and second prongs of the test. Additionally, since the warrant was incredibly broad, everything that the FBI agents viewed within the databases was immediately apparent, and thus the third prong was easily satisfied. Thus, application of the plain view doctrine creates an end run around the Fourth Amendment.

III.

The particularity requirement of search warrants should be heightened in the digital evidence context as per the guidelines set forth by the Fourteenth Circuit. This Court has consistently held that general, exploratory searches are the specific evil that the particularity requirement is designed to prevent. Conducting an effective search of digital evidence often requires the government to over-seize the materials and conduct an extended review of the evidence. However, the reality of conducting searches of computer data is that information supported by probable cause will be intermingled with information unsupported by probable cause. The requirements strike an appropriate balance between Fourth Amendment protections and the needs of law enforcement officials in conducting searches of digital evidence.

The requirements enable the government to acquire all the information for which it established probable cause while protecting individuals from general, exploratory searches. Requiring the government to waive reliance upon the plain view doctrine is consistent with this Court's jurisprudence because this exception would enable the government to conduct warrantless searches of unresponsive data and then claim that it was in plain view, thus nullifying an individual's Fourth Amendment protections. The segregation and redaction process ensures that the government only acquires information for which it established probable cause. This process precludes the government from acquiring the unresponsive, intermingled data that is inherent in the digital evidence context. Disclosure of the actual risks of destruction or concealment of information assists the judge in balancing the needs of the government and constitutionally protected rights. Requiring that the search protocol is designed to uncover only the information for which the government has probable cause is consistent with this Court's prohibition of general searches. Finally, requiring the government to return or destroy unresponsive information sufficiently protects individuals from general searches.

ARGUMENT

I. THE COURT OF APPEALS FOR THE FOURTEENTH CIRCUIT CORRECTLY HELD THAT THE COLONIAL FOOTBALL LEAGUE HAS STANDING TO BRING A RULE 41(g) MOTION CHALLENGING THE REASONABLENESS OF THE SEARCH AND SEIZURE.

Federal Rule of Criminal Procedure 41(g) permits an individual who has been “aggrieved by an unlawful search and seizure of property” to order the return of the seized property. FED. R. CRIM. P. 41(g). This Court defines a person aggrieved by an unlawful search and seizure as one who is either a “victim [or] one who 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 of seizure directed at someone else.” Rakas v. Illinois, 439 U.S. 128, 134–35 (1978). This Court has held that an association has standing to sue on behalf of its members when they 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. See Pennell v. City of San Jose, 485 U.S. 1, 7 (1988)

Here, the CFL has standing because they are a “person aggrieved by an unlawful search and seizure.” Rakas, 439 U.S. at 134–35. The Fourteenth Circuit correctly held that the CFL was a victim. (R. at 10.) Even though the drug testing records were seized from the StarTests facility, the CFL’s ownership interest was stronger than that of StartTests. The CFL paid StarTests to administer the tests and StarTests retained the results for confidentiality purposes. (R. at 10.)

Even if this Court finds that the CFL is not a victim, the reasoning of the District Court should be adopted because the CFL is “aggrieved by an unlawful search and seizure” and satisfied the three-prong associational test adopted by this Court. See Pennell, 485 U.S. at 7. First, each player would have the right to seek the return of his or her own testing records, (R. at 3), and therefore the ability to sue. Second, the CFL players’ privacy interests in the results are

related to the CFL's organizational purpose. (R. at 3.) As the District Court explained, the CFL is contractually obligated to protect the privacy interests of each individual player. (R. at 3.) Lastly, the CFL seeks only the return of the drug testing information contained on StarTests's computers. (R. at 2.) Therefore, this Court should affirm the Fourteenth Circuit and hold that the CFL has standing to bring a 41(g) motion seeking the return of the seized property.

II. THE PLAIN VIEW EXCEPTION SHOULD NOT APPLY TO DIGITAL EVIDENCE BECAUSE IT THREATENS TO NULLIFY FOURTH AMENDMENT SEARCH AND SEIZURE PROTECTIONS.

The Fourth Amendment to the United States Constitution guarantees “the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures...” U.S. Const. amend IV. The Fourth Amendment is designed to protect people from both unreasonable searches and seizures and the issuance of general warrants. See Horton v. California, 496 U.S. 128, 143 (1990) (holding that the Fourth Amendment prohibits unreasonable searches and seizures, and mandates the issuance of warrants that particularly describe the place to be searched and the objects to be seized).

The plain view doctrine is an exception to the Fourth Amendment warrant requirement, which allows police officers, during the execution of a warrant, to seize evidence of contraband or criminal wrong doing technically outside the scope of the warrant. Coolidge v New Hampshire, 403 U.S. 443, 464–65 (1971). Any evidence seized by the police must be in plain view at the moment of seizure. Id. at 465. As articulated by the this Court, “[t]he problem with the ‘plain view’ doctrine has been to identify the circumstances in which plain view has legal significance rather than being simply the normal concomitant of any search, legal or illegal.” Id.

The “plain view” exception test is satisfied when an officer is lawfully present at the place where the evidence can be plainly viewed, the officer must have a lawful right of access to

the object, and the incriminating character of the object must be “immediately apparent.” Horton, 496 U.S. at 136–37 (holding that the plain view exception applied when a police officer discovered weapons used in a robbery in plain view that were outside the scope of the warrant). While the plain view doctrine is a well-established exception to the Fourth Amendment, its application in digital evidence cases threatens to abolish Fourth Amendment protections of digital property. The Tenth Circuit examined the implications of applying the plain view doctrine to digital evidence:

The advent of the electronic age and the development of desktop computers that are able to hold the equivalent of a library's worth of information, go beyond the established categories of constitutional doctrine. Analogies to other physical objects, such as dressers or file cabinets, do not often inform the situations we now face as judges when applying search and seizure law. This does not, of course, mean that the Fourth Amendment does not apply to computers and cyberspace. Rather, we must acknowledge the key differences and proceed accordingly.

United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001).

As articulated by the Tenth Circuit, the sacred and heavily guarded Fourth Amendment protections are threatened if key differences between physical property and digital property are ignored. Id. Additionally, search and seizure protections are circumvented when applied to digital evidence cases because the plain view doctrine is far too easily satisfied. Thus, this Court should disallow the “plain view” exception to the Fourth Amendment warrant requirement in digital searches including searches of computers, hard drives, and disks.

A. Digital Property Is Inherently Different From Physical Property, And Application Of The Plain View Doctrine In Digital Evidence Cases May Result In Transforming Digital Evidence Warrants Into General Exculpatory Searches.

Search and seizure principles historically involve the search of physical spaces, such as homes, automobiles, and bags. A “search” is typically triggered when a person’s reasonable expectation of privacy is invaded. Orin S. Kerr, Searches and Seizures in a Digital World, 119

HARV. L. REV. 531, 536 (2005). However, a search can only occur when police officers have a warrant or when an exception to the warrant requirement applies. Id. A “seizure” occurs when there is a taking away of physical property named in a warrant. Id. However, under the plain view doctrine officers can seize other evidence inadvertently discovered in plain view so long as the incriminating nature of the evidence is “immediately apparent.” Horton, 496 U.S. at 136–37.

Naturally, Fourth Amendment protections extend to the search and seizure of digital property. Walser, 275 F.3d at 986. However, well-established search and seizure jurisprudence fails to account for the inherent differences between the search of physical property and the search of digital property. For example, digital data may be hidden, encrypted, or booby-trapped. Comprehensive Drug Testing, 579 F.3d at 998 (holding that the government cannot rely on the plain view doctrine when recovering digital evidence). Therefore, in order to conduct a thorough and effective search, police officers must search digital property in its entirety due to the amorphous nature of digital data. Ray Ming Chang, Why the Plain View Doctrine Should Not Apply to Digital Evidence, 12 SUFFOLK J. TRIAL & APP. ADVOC. 31, 33 (2007). Whereas, physical property can often be isolated or separated from other objects, such as removing a firearm from a vehicle glove box, digital evidence is not easily isolated as one cannot easily remove a file from a computer without copying or seizing the entire computer. Id. Further, digital evidence often requires translation or interpretation with some type of expert assistance because police officers cannot determine whether the digital data is criminal. Id.

Without recognition of such inherent differences, application of the plain view doctrine to digital evidence threatens to transform constitutionally compliant warrants into general warrants, which are strictly prohibited by the Fourth Amendment. See Walser, 275 F.3d at 986; Comprehensive Drug Testing, 579 F.3d at 1004. The warrant clause emphatically prohibits

judicial officials from issuing a warrant except one that “particularly” describes “the place to be searched and the persons or things to be seized.” U.S. Const. amend IV; see Maryland v. Garrison, 480 U.S. 79, 84 (1987). The Court issued numerous warnings against the manipulation of computer warrants into authorizations for general exploratory searches. See Coolidge, 403 U.S. at 466; Comprehensive Drug Testing, 579 F.3d at 1004.

Many of the circuits failed to implement adequate procedural safeguards for the search of digital evidence. The Tenth Circuit explained in detail the issues caused by the application of the plain view exception in digital evidence cases. While the Tenth Circuit court did not explicitly adopt the plain view doctrine, this search methodology still transforms warrants for digital evidence into a general exculpatory search. Consequently, the plain view doctrine and Tenth Circuit’s approach render similar results. Since the police officers have already discovered the incriminating evidence, the government can either rely on the plain view doctrine or seek to obtain another warrant ensuring that the evidence was legally seized. In Walser, the court categorically rejected application of the plain view exception. 275 F.3d at 981 (holding that the scope of the warrant authorizing the search for digital evidence of drug trafficking was not exceeded when the police officer opened and viewed a video file containing child pornography). The Tenth Circuit hoped to avoid authorizing general searches of digital property by requiring that police officers obtain additional search warrants when digital evidence of crimes outside the scope of the original warrant is discovered. Id. Neither the plain view doctrine nor the Tenth’s Circuit search methodology provides procedural safeguards protecting Fourth Amendment protections against unreasonable searches and seizures of digital property.

Like many courts unwilling or reluctant to hamper criminal investigations, here, the judge, persuaded by the government’s request, issued a broad warrant authorizing agents to seize “all

computer records, files, and equipment.” (R. at 2.) In part, the magistrate judge was persuaded by the government’s concern that files may be mislabeled, or deceptively labeled for confidentiality. (R. at 2.) Additionally, the government argued that it needed to seize such a mass quantity of computers and equipment, that an on-site search would be impracticable, and that encryption devices may not be possible on StarTests computers. (R. at 2.)

Judicial officials will continue authorizing extremely broad warrants, such as the seizure of all computers and equipment, until the inherently different nature of digital property is recognized. Additionally, to allow police officers to search every file because data may be encrypted, mislabeled, or hidden in a computer trash bin, permits anything that police officers stumble upon to come into the plain view and become legally seized evidence. In the wake of a new digital age, one marked by people storing everything from grocery lists to deeply guarded personal diaries on computers or other digital devices, this Court should recognize the difference between digital evidence and physical evidence in order to sustain the sacred protections of the Fourth Amendment as applied to digital property. Without recognizing these key differences between a search and seizure of physical property as compared to one of digital evidence, the plain view exception will have the practical effect of abolishing Fourth Amendment protections.

B. The Three-Prong Plain View Exception Test Applied In Digital Evidence Cases Is Too Easily Satisfied And Thus Circumvents Well-Established Search And Seizure Protections Under The Fourth Amendment.

In digital evidence cases, the plain view exception test is almost always satisfied and threatens to negate Fourth Amendment protections. It is a well-established exception to the Fourth Amendment that under certain circumstances police may seize evidence in plain view without a warrant. Coolidge, 403 U.S. at 465. In order to satisfy the plain view exception test: an officer must be lawfully present at a place where evidence must be plainly viewed, the officer

must have a lawful right of access to the object, and the incriminating character of the object must be “immediately apparent.” Horton, 496 U.S. at 136–37. The plain view test is not easily satisfied in physical evidence cases. On the contrary, in digital evidence cases, the three-prong plain view test is ostensibly always satisfied. Comprehensive Drug Testing, 579 F.3d at 998. In a growing digital age, the Fourth Amendment will lose its strength and veracity and will be unable to protect persons from prohibited unreasonable searches and seizures.

Historically, the plain view doctrine applies in situations where police have a warrant to search a given area for specified objects and inadvertently discover some other object indicative of criminal activity during the course of the search. Id. The plain view doctrine functions to supplement the prior justification for the search “whether it be a warrant for another object, hot pursuit, search incident to lawful arrest, or some other legitimate reason for being present unconnected with a search directed against the accused-and permits the warrantless seizure.” Id. at 466. However, extending the original justification search is only justified when it is immediately apparent to the police that they have criminal evidence before them. Id. Additionally, the plain view doctrine must never be used to conduct a general exploratory search until something incriminating emerges. Id.

Application of the plain view exception in digital evidence cases has confused the circuit courts. However, the Ninth and Fourteenth Circuit have correctly dealt with the plain view doctrine in digital evidence cases. For instance, in United States v. Raney, the Seventh Circuit adopted the plain view exception in digital evidence cases. 342 F.3d 551, 555 (7th Cir. 2003) (holding that digital evidence from the defendant’s computer was legitimately seized after a police officer discovered a stack of computer printed photographs then proceeded to search the defendant’s computer for additional evidence of child pornography). However, the Ninth and

Tenth Circuits, respectively, have either waived reliance on or avoided application of the plain view doctrine in digital evidence cases. See Comprehensive Drug Testing, 579 F.3d at 998 (holding that the government should waive reliance on the plain view doctrine in digital evidence cases); Walser, 275 F.3d at 981 (holding that officers must obtain a second warrant when they inadvertently discover evidence of criminal wrongdoing outside the scope of the original warrant).

1. The First Prong Of The Plain View Exception Test Requiring That A Police Officer Be Lawfully Present At A Place Where Evidence Must Be Plainly Viewed Is Too Easily Satisfied When Applied In Digital Evidence Cases.

The first prong of the plain view exception test is too easily satisfied in digital evidence cases. The first prong of the plain view exception test requires that an officer be lawfully present at place where evidence is plainly viewed. Horton, 496 U.S. at 136–37. An officer is lawfully present by either the issuance of a warrant or the defendant’s consent. See Raney, 342 F.3d at 559 (holding that police officers were lawfully present when acting within the issuance of a warrant); United States v. Dichiarinte, 445 F.2d 126, 128 (7th Cir. 1971) (holding that police officers were lawfully present after the defendant consented to a “free and voluntary invitation” into his home). In United States v. Wong, the Ninth Circuit held that digital evidence related to child pornography found during a search connected to the murder of Wong’s girlfriend was admissible under the plain view exception because “the police were lawfully searching for evidence of murder in the graphics files, that they had legitimately accessed and where the incriminating child pornography was located.” 334 F.3d 831, 838 (9th Cir. 2003).

A court issued warrant to search or seize a computer is meaningless if police officers cannot access the files. See United States v. Adjani, 452 F.3d 1140, 1152 (9th Cir. 2006). The first prong of the plain view exception test will always be satisfied when executing a warrant in

digital evidence cases because police officers will be lawfully present on the computer, or digital device. In United States v. Gray, the Eastern District of Virginia held that a FBI agent was entitled to examine all of the defendant's digital files in order to determine whether they contained items that fell within the scope of the warrant. 78 F. Supp. 2d 524, 529 (E.D. Va. 1999). Additionally, the court held that the evidence discovered beyond the scope of the warrant was admissible under the plain view exception because the agent was lawfully present on the defendant's computer. Id. Therefore, under the first prong of the plain view test, it is virtually impossible to imagine a scenario where officers would not be lawfully present while searching among computer files to which they are broadly authorized to search. In digital evidence cases, this prong of the plain view exception test is rendered meaningless because it is so easily satisfied.

The application of the first prong in non-digital evidence cases demonstrates that the plain view exception test is meant to function as a rigorous protection against under unreasonable searches and seizures. The strength and intended veracity of this prong is evidenced in its application to physical property searches. In Arizona v. Hicks, a bullet was fired through the floor of Hicks' apartment injuring the man in the apartment below. 480 U.S. 321, 323 (1987). The police entered Hicks' apartment to search for the shooter, for other victims, and for weapons and while there, one of the police officers noticed two sets of expensive stereo components. Id. Police suspected that they were stolen, so they read and recorded their serial numbers. Id. The government justified the search of the stereo equipment claiming that the officers were lawfully present in a place where the stereo equipment was in plain view. Id. at 326. This Court rightly held that the moving of the equipment was a search separate and apart from the lawful access that the police officers had to search the apartment for evidence of the assault. Id. at 321.

Therefore, the evidence was not admissible under the plain view doctrine. Id. at 326.

As demonstrated in Hicks, the first prong of the plain view exception test is intended to provide rigorous protection to searches of an area not authorized by a warrant. However, in the majority of digital evidence cases, the first prong of the plain view exception test is too easily satisfied. See generally Raney, 342 F.3d at 559 (holding that the first prong of the plain view test was satisfied because the government had lawful access to search the defendant's computer).

Like the broad warrant issued in Gray, here, the warrant issued by the magistrate judge in the United States District Court for the District of Wythe authorized FBI agents to search and seize "all computer records, files, and equipment" related to the administered drug tests at StarTests facility in Millersville, Wythe. (R. at 2.) While the agents were searching the computer records, files, and equipment for evidence of illegal steroid use by the five football players in question, the agents discovered positive results for illegal steroid use for many other football players, as well as results indicating extensive narcotics and marijuana usage. (R. at 2.) The agents were lawfully present because the agents were authorized by warrant to access all of StarLab's computer records and files. (R. at 2.) As a result, the FBI agents copied and retained all of the digital information. (R. at 2.) In digital evidence cases, this prong will virtually always be satisfied since issued warrants authorize officers to be lawfully present while accessing a defendant's computer or digital device. Thus, in digital evidence cases the first prong is too easily satisfied which creates an end run around the sacred Fourth Amendment.

2. The Second Prong Of The Plain View Exception Test Requiring That A Police Officer Must Have A Lawful Right Of Access To The Object Is Too Easily Satisfied In Digital Evidence Cases.

Like the first prong of the plain view exception test, the second prong is nearly always satisfied in digital evidence cases. The second prong of the plain view test requires that an officer

must have a lawful right of access to the object. Horton, 496 U.S. at 136–37; United States v. Alexander, 574 F.3d 484, 490–91 (8th Cir. 2009) (holding that police officers had a lawful right of access to the defendant’s computer because the search warrant authorized the search of the defendant’s computer and any area of his home). In a search made pursuant to a warrant, only specifically enumerated items may be seized. Horton, 496 U.S. at 139. Like the first prong, the second prong was intended to provide rigorous protections against unreasonable searches and seizures. For example, in United States v. Turner, the police officers believed that an intruder, suspected of assault, entered the defendant’s apartment. 169 F.3d 84, 85 (1st Cir. 1999). With Turner’s consent, officers searched his apartment and found bloody clothes and suspected him of committing assault on his neighbor. Id. at 84. Subsequently, officers obtained a warrant to search the defendant’s personal property. Id. Officers searched Turner’s computer where they subsequently discovered child pornography. Id. The First Circuit held that police officers did not have a lawful right of access to defendant’s computer even when he consented to a search of his apartment because it was unlikely that evidence of sexual assault could be obtained from a search of computer files. Id. at 86. In Turner, the second prong was not so easily satisfied and afforded the defendant rigorous protections under the Fourth Amendment.

In digital evidence cases, the application of the second prong arms law enforcement with unjustified protection under the plain view doctrine when searching for files outside the scope of a 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.) Due to the nature of digital evidence, access to a computer is meaningless without the ability to access files, thus officers will always have lawful access to the files. Adjani, 452 F.3d at 1152. As rightly stated by the Fourteenth Circuit, the distinction between the first and second prong makes sense when there is an actual

spatial difference between the place of entry and an object requiring effort to lift or seize, e.g. an apartment versus the expensive stereo equipment located inside it. See generally Hicks, 480 U.S. at 321. Thus the second prong of the plain view exception test is just as easily satisfied as the first prong because access to a computer is simply meaningless without access to the files.

Here, under the authorization of a warrant, the federal agents were searching StarTest's database in order to find five CFL player's drug testing results. (R. at 1.) However, during the course of the authorized search, the agents came across evidence of other football players' drug testing results. (R. at 2.) While the government conceded that they did not have probable cause to search beyond the test results for the five CFL players, the FBI unilaterally expanded their search without seeking another warrant. (R. at 2.) Then, the FBI claimed protection under the plain view doctrine, (R. at 4.), which has the practical effect of circumventing Fourth Amendment protections in this case. Like in many other digital evidence cases, here, the second prong of the plain view exception test was satisfied as the agents had a lawful right of access to every single file since the warrant so broadly authorized the search and seizure of "all computer records, files, and equipment" related to the administered drug tests at StarTests facility in Millersville, Wythe. (R. at 1-2.) Since a computer is meaningless with out access to the files, this authorization is overly broad, and violates the Fourth Amendment.

In digital evidence cases, Fourth Amendment protections are threatened when the plain view exception is applied because of the potential to transform such searches into general exculpatory searches. Carey, 172 F.3d at 1272. Consequently, with broad issuance of lawful access to files, this prong, like the first prong, is nearly always satisfied in digital evidence cases, but rightfully maintains its rigorous application in physical evidence cases.

3. The Third Prong Of The Plain View Exception Test Requiring That The Incriminating Character Of The Object Be Immediately Apparent To The Police Officer Is Too Easily Satisfied In Digital Evidence Cases.

The third prong of the plain view test requires that the incriminating character of the object must be immediately apparent before it can be seized. Horton, 496 U.S. at 136–37. “Immediately apparent” requires that the police officers have probable cause to believe that the object or evidence they are viewing is evidence of a crime, or some kind of contraband. Hicks, 480 U.S. at 326. There is only one court to hold that documents were not immediately apparent because the documents had to be open and read. Dichiarinte, 445 F.2d at 130–31 (holding that the plain-view doctrine did not apply because the paper receipts had to be opened, and therefore the criminal nature of the documents was not immediately apparent after a surface inspection). Comparatively in physical property cases, currency discovered in aluminum wrapped package in the freezer was not admissible under the plain view doctrine because the package had to be removed and unwrapped and thus its incriminating nature was not immediately apparent. See United States. v. Gonzalez Athehorta, 729 F. Supp. 248, 251 (E.D.N.Y 1990). While Dichiarinte correctly imposed a procedural safeguard protecting the Fourth Amendment, other circuits, including the Tenth Circuit removed this safeguard, making this prong easily satisfied in digital evidence cases. Carey, 172 F.3d at 1273. In Carey, the court held that a child pornography image was admissible when a police officer discovered the image while looking for evidence of a drug transaction. Id. The criminal nature of the pornography was not immediately apparent to the officers because the file needed to be opened and viewed. Id. Additionally, in Wong, pornographic images were admissible despite the fact that the files were unopened and contained in separate files. 334 F.3d at 837. As evidenced by Carey, and Wong, there are no procedural safeguards in applying the “immediately apparent” prong in digital evidence cases. While the

illusory limits created by Dichiarinte court seemingly created protection in digital evidence cases, they were consequently obliterated in Carey, thus leaving yet another too easily satisfied prong in the plain view exception test.

Here, the FBI executed the search warrant on the StarTests Millerville facility on the morning of November 1, 2008. (R. at 2.) StarTests personnel informed agents that most of the computers in the facility included at least one CFL drug-testing database. (R. at 2.) As evidenced by testimony given at the motions hearing, the three CFL databases were contained on different computers. (R. at 2.) Many of these files were encrypted, while others were hidden in various H- or S-drives. (R. at 2.) Like in Wong where the files were closed and separate, here, the databases were contained in three separate computers. (R. at 2.) The agents had access to all of the files on every StarTest database. Consequently, once opened, each and every result in the third database was “immediately apparent” to the agents equipping this prong with little power to protect persons against unreasonable search and seizures. This prong of the plain view exception cannot logically be applied in this digital evidence case because results indicating positive use of “cocaine” or “steroid” would give rise to probable cause regardless of the context used.

Since FBI agents were permitted to open all of the closed databases, anything the FBI agents view will be immediately apparent and thus satisfy the third prong of the plain view test. As the plain view doctrine is applied, there are no procedural safeguards protecting digital evidence against unreasonable searches and seizures.

C. Reliance On The Plain View Doctrine In Digital Evidence Cases Is Misplaced, And The Ninth’s Circuit’s Standards In *Comprehensive Drug Testing* Should Be Adopted.

In recognizing the apparent faults in applying the plain view exception in digital evidence cases, the Ninth Circuit waived government reliance on the plain view exception to the Fourth

Amendment. Comprehensive Drug Testing, 579 F.3d at 998. The facts of Comprehensive Drug Testing are strikingly similar to the case at bar. In Comprehensive Drug Testing, the FBI raided three different facilities searching for evidence of steroid usage. Id. at 993. The agents seized all the computer equipment and hard drives at every drug testing 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 all the computer equipment. Id. at 998. The government relied on the plain view doctrine and argued that it was not required to return the computer equipment because the evidence was in plain view once its agents began to examine the contents of the computers. Id. The Ninth Circuit immediately responded to the obvious flaw in this argument in stating:

If the government can't be sure whether data may be concealed, compressed, erased or booby-trapped without carefully examining the contents of every file...then everything the government chooses to seize will, under this theory, come into plain view." With this prerogative, the court continued, government agents will be tempted to seize "more rather than less: ... Why just that directory and not the entire hard drive? Why just this computer and not the one in the next room and the next room after that? Can't find the computer? Seize the Zip disks under the bed

Id. (citing United States v. Hill, 322 F. Supp. 2d 1081 (C.D. Cal. 2004)). The Ninth Circuit articulated its concern that the plain view doctrine would virtually wipe out Fourth Amendment protections for computer searches. Id. The Ninth Circuit discussed the dangers of allowing the government to seize all evidence, and search until something criminal surfaces, that would ostensibly be in plain view and thus admissible. Id. After waiving reliance on the plain view exception in digital evidence cases, the Ninth Circuit articulated a set of standards for when the government wishes to obtain a warrant to examine a computer hard drive or digital storage device in searching for certain incriminating files, or when a search for evidence could result in the seizure of a computer. Id. at 1006. Magistrate judges must be vigilant in observing the

following: (1) they should insist the government waive reliance upon the plain view doctrine; (2) segregation and redaction must be either done by specialized personnel or an independent third party, and if segregation is to be done by government computer personnel, it must agree in the warrant application that computer personnel will not disclose to investigators any information other than what is the target of the warrant; (3) warrants and subpoenas must disclose actual risks of destruction of information as well as prior efforts to seize that information in other judicial fora; (4) government's search protocol must be designed to uncover only information for which it has probable cause, and only that information may be examined by case agents; and (5) government must destroy or, if recipient may lawfully possess it, return non-responsive data, keeping issuing magistrate informed about when it has done so and what it has kept. Id.

The Ninth Circuit recognized the inherent differences between physical property and digital property, and feared that the plain view exception as applied would eviscerate Fourth Amendment protections in digital evidence cases. Id. at 998. These standards adequately address the issues caused by application of the plain view doctrine in digital evidence cases without hindering law enforcement's ability to investigate crimes. Thus, reliance on the plain view exception should be waived in place of the standards articulated by the Ninth Circuit in Comprehensive Drug Testing and adopted by the Fourteenth Circuit in this case.

III. THE COURT OF APPEALS FOR THE FOURTEENTH CIRCUIT CORRECTLY HEIGHTENED THE PARTICULARITY REQUIREMENT BY IMPOSING GUIDELINES THAT FEDERAL MAGISTRATES MUST FOLLOW WHEN ISSUING SEARCH WARRANTS IN THE DIGITAL EVIDENCE CONTEXT.

This Court should affirm the decision of the United States Court of Appeals for the Fourteenth Circuit and hold that the particularity requirement of warrants be heightened in the digital evidence context. The Fourth Amendment provides that “no Warrants shall issue, but upon probable cause . . . and particularly describing the place to be searched, and the persons or

things to be seized.” U.S. Const. amend. IV. The Warrant Clause requires “that warrants be particular and supported by probable cause.” Payton v. New York, 445 U.S. 573, 583–84 (1980). As this Court stated in Maryland v. Garrison, “the Warrant Clause of the Fourth Amendment categorically prohibits the issuance of any warrant except one ‘particularly describing the place to be searched and the things to be seized.’” 480 U.S. 79, 84 (1987). Permitting federal magistrates to issue warrants authorizing the government to seize “all” computer equipment and files for later sorting runs afoul of the Fourth Amendment’s Warrant Clause and this Court’s jurisprudence. See id. (explaining the necessity of limiting the authorization to the specific areas where there is probable cause to search so that the warrant will not take on the character of the “wide-ranging exploratory searches” that the Fourth Amendment prohibits). Therefore, this Court should hold that when federal magistrates issue warrants in the digital evidence context, the particularity requirement must be heightened as per the guidelines set forth in United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989 (9th Cir. 2009), and subsequently adopted by the Fourteenth Circuit below.

A. This Court Should Adopt The Guidelines Set Forth In The Fourteenth Circuit For Issuing Warrants In The Digital Evidence Context Rather Than Permitting A General Warrant To Seize All Computer Equipment And Files For Later Sorting Because The Guidelines Are Consistent With This Court’s Jurisprudence And The Fourth Amendment.

Generally, a federal magistrate may issue a search warrant if the government establishes that it has “probable cause” to believe evidence of a crime will be found in a particular place. See Illinois v. Gates, 462 U.S. 213, 238 (1983). In this case, whether the government established probable cause for the search and seizure of the computer records relating to the five players named in the affidavit is not in question. (R. at 8.) The issue before this Court is whether the

broad warrant that permitted the search and seizure of the test results for players who the government did not have probable cause violated the Fourth Amendment. (R. at 9.)

This Court stated that “the manifest purpose” of the particularity requirement is “to prevent general searches.” Garrison, 480 U.S. at 84. It is well settled that the Warrant Clause is designed to prohibit general exploratory searches. See e.g., Garrison, 480 U.S. at 84; Andresen v. Maryland, 427 U.S. 463, 480 (1976); Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971) (stating a general exploratory search is the “specific evil” the particularity requirement is designed to prevent). As this Court explained in United States v. Ross, probable cause to believe a lawnmower is located in the garage does not support a warrant to search an upstairs bedroom, nor does probable cause to believe undocumented aliens are being transported in a motor vehicle justify the search of a suitcase. 456 U.S. 798, 824 (1982). This seemingly simple distinction in physical searches becomes far more complex in the digital evidence context. See Raphael Winick, Searches and Seizures of Computers and Computer Data, 8 HARV. J.L. & TECH. 75, 78 (1994) (noting “that the massive storage capacity of modern computers creates a high risk of overbroad, wide-ranging” searches and seizures).

This Court has noted that “it would be foolish to contend the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.” Kyllo v. United States, 533 U.S. 27, 33–34 (2001). The problem that arises in the context of computer searches is that the relevant information to the warrant is often “intermingled” with irrelevant information. See Comprehensive Drug Testing, 579 F.3d at 997 (explaining that the drug-testing results for the athletes named in the warrant were intermingled with results for athletes not named in the warrant). Given the complexities of conducting effective searches of computer data, it is often necessary for the government to “over-seize” materials and conduct

offsite review of the digital evidence. See id. at 995. The rationale is that files may be disguised in various ways, that there may be “booby traps” to destroy data, and that there may be too much information to be examined at the site. Id.; but see United States v. Tamura, 694 F.2d 591, 596 (9th Cir. 1982) (“[T]he wholesale seizure for later detailed examination of records . . . is significantly more intrusive, and has been characterized as the ‘kind of investigatory dragnet that the Fourth Amendment was designed to prevent.’” (quoting United States v. Abrams, 615 F.2d 541, 543 (1st Cir. 1980))). While it is uncontested that computer files are often so intermingled that over-seizure may be required, this Court’s jurisprudence requires that Fourth Amendment protections are not diminished when implementing procedures for effective law enforcement. See Oliver v. United States, 466 U.S. 170, 181 (1984) (holding a case-by-case approach to access the validity of an “open field” search fails to provide a “workable accommodation between the needs of law enforcement and the interests protected by the Fourth Amendment”).

1. The Heightened Particularity Requirements Strike An Effective Balance Between The Rights Protected By The Fourth Amendment And The Needs Of Law Enforcement Officials In Conducting Searches Of Digital Evidence.

Although the warrant requirements set forth by the Ninth and Fourteenth Circuits specifically dealt with federal investigations into steroid use by professional athletes, they set forth “procedures and safeguards that federal courts must observe in issuing and administering search warrants . . . for electronically stored information.” Comprehensive Drug Testing, 579 F.3d at 993. In his panel dissent, Judge Thomas stated, “the stakes in this case are high.” United States v. Comprehensive Drug Testing, Inc., 513 F.3d 1085, 1117 (9th Cir. 2008) (Thomas, J., dissenting), *rev’d en banc*, 579 F.3d 989 (9th Cir. 2009). In that case, even though the government established probable cause to garner a search warrant for the drug-testing records of eleven Major League Baseball players, the government seized “thousands of test results

involving every single” player. Id. The magistrate judge had granted broad authority for the seizure of data because of the “hazards of retrieving” electronically stored data. Comprehensive Drug Testing, 579 F.3d at 995. The Ninth Circuit “accept[ed] the reality that such over-seizing is an inherent part of the electronic search process,” but required the proper “balance” between the government’s interests in law enforcement and an individual’s Fourth Amendment protections. Id. at 1006 (setting guidelines for judges to follow when issuing search warrants); see also Oliver, 466 U.S. at 181 (holding that the needs of law enforcement must be balanced with Fourth Amendment protections). In essence, the government used the broad search warrant to acquire sensitive and private information of individuals not mentioned in the warrant and not implicated in criminal activity. Comprehensive Drug Testing, 579 U.S. at 1005. As that court stated, “What ever happened to the Fourth Amendment? Was it . . . repealed somehow?” Id.

The Fourth Amendment’s Warrant Clause and this Court’s jurisprudence prohibits the general searches permitted by the United States District Court for the District of Wythe, (R. at 6.), and criticized by the Ninth Circuit. See e.g., Garrison, 480 U.S. at 84; Stanford v. Texas, 379 U.S. 476, 509–10 (1965). This Court stated in Stanford: “These words are precise and clear. They reflect the determination . . . that the people of this . . . Nation should forever ‘be secure in their persons, houses, papers, and effects’ from intrusion and seizure by officers acting under the unbridled authority of a general warrant.” Stanford, 379 U.S. at 509–10. This Court should adopt the guidelines set forth by the Ninth and Fourteenth Circuits because they strike a proper balance between the needs of law enforcement officials to conduct effective searches of digital evidence and the rights protected by the Fourth Amendment.

Before issuing a warrant in a digital evidence case, a magistrate judge must observe five guidelines. (R. at 17.) First, the magistrate should insist that the government waive reliance on

the plain view doctrine. (R. at 17.) Second, specialized personnel or an independent third party should segregate and redact computer evidence that is outside the scope of the warrant. (R. at 17.) Third, the warrant must disclose the actual risks of destruction or concealment of relevant information, including prior efforts to seize the data. (R. at 17.) Fourth, the search protocol must be designed to discover only that information for which the government has probable cause. (R. at 17.) Finally, the government must destroy or return unresponsive information. (R. at 17.) As discussed below, the magistrate judge in this case failed to follow these requirements and thus the CFL's Fourth Amendment rights were violated. Therefore, this Court should affirm the decision of the Court of Appeals for the Fourteenth Circuit and hold that the particularity requirement of warrants be heightened in the digital evidence context, as per the guidelines announced in the Ninth and Fourteenth Circuits. (R. at 17).

a. Insisting That The Government Waive Reliance Upon The Plain View Doctrine Protects An Individual's Rights Under The Fourth Amendment While Permitting An Effective Search By Law Enforcement Officials.

Insisting that the government waive reliance upon the plain view doctrine ensures that an individual's Fourth Amendment rights will not be rendered a nullity. See Comprehensive Drug Testing, 579 F.3d at 998 (“[T]he plain view doctrine too often . . . becomes an end run around the Fourth Amendment warrant requirement.”). This Court has stated that under certain circumstances the plain view doctrine permits law enforcement officials to seize evidence in plain view without a warrant. Coolidge, 403 U.S. at 465. However, this Court warned that the plain view exception must be cautiously applied and that “we must not lose sight of the Fourth Amendment's fundamental guarantee” of the warrant requirement. Id. at 453; see also Jones v. United States, 357 U.S. 493, 499 (1958) (stating that exceptions to the warrant requirement must be “jealously and carefully drawn”).

Application of the plain view exception in the digital evidence context is problematic due to the intermingled nature of electronic records. Electronic records are unique in the sense that responsive material is often, if not always, coupled with unresponsive material. See United States v. Adjani, 452 F.3d 1140, 1152 (9th Cir. 2006) (“Computers are simultaneously file cabinets (with millions of files) and locked desk drawers; they can be repositories of innocent and deeply personal information, but also of evidence of crimes.”). Therefore, permitting application of the plain view exception would provide the government with a means to conduct warrantless searches of unresponsive data and then claim that it was in plain view, thus nullifying an individual’s Fourth Amendment protections. See Comprehensive Drug Testing, 579 F.3d at 1004 (“This pressing need of law enforcement for broad authorization to examine electronic records . . . creates a serious risk that every warrant . . . will become . . . a general warrant, rendering the Fourth Amendment irrelevant.”). Such a loophole is in contravention of the very purpose of the plain view exception.

It is uncontested that searches in the digital evidence context impose certain difficulties on law enforcement officials because relevant data may be “concealed, compressed, erased or booby-trapped.” Id. at 998. Therefore, it is often necessary to conduct a detailed examination of the data by opening unmarked files, using specialized forensic software, or performing another search technique. Id. 1004. The problem is that locating the particular files stated in the warrant “require[s] examining a great many other files to exclude the possibility that the sought-after data are concealed there.” Id.; see also Adjani, 452 F.3d at 1152.

The Fourteenth Circuit correctly stated that the requirements of the plain view exception will “inevitably pass the test each time it is applied.” (R. at 11.) This would enable the government to “seize the haystack to look for the needle,” (R. at 13.), and thereafter claim the

evidence was discovered in plain view. See Comprehensive Drug Testing, 579 F.3d at 998. The potential ramifications of applying the plain view exception in this context are endless. As that court explained, this would encourage the government to “seize more rather than less” and render the warrant requirement a “nullity.” Id. (“Why stop at the list of baseball players when you can seize the entire [] directory? Why just that directory and not the entire hard drive?”).

In Comprehensive Drug Testing, the government had probable cause to believe that ten Major League Baseball players were illegally taking steroids and acquired a warrant to search for their test results. Id. at 999. After the government over-seized the computer data, its subsequent search revealed the files of a “huge number” of test results beyond the players for which the government had probable cause. Id. at 1005. The Ninth Circuit refused to use the plain view exception because that would render Fourth Amendment a “nullity.” Id. at 998.

Insisting the government waive reliance upon the plain view doctrine is consistent with this Court’s jurisprudence. This Court has explained that “[i]t is not an inconvenience to” balance the warrant requirement against “claims of police efficiency.” Coolidge, 403 U.S. at 481. Rather, the warrant requirement operates as a “check” to “any system of law enforcement.” Id. This Court has repeatedly stated that if the warrant requirement “is to be a true guide to constitutional police action, rather than just a pious phrase, then ‘[t]he exceptions cannot be enthroned into the rule.’” Id. at 482 (quoting United States v. Rabinowitz, 339 U.S. 56, 80 (1950) (Frankfurter, J., dissenting), *overruled by* Chimel v. California, 395 U.S. 752 (1969)).

This case demonstrates that waiving reliance upon the plain view exception strikes an appropriate balance between an individual’s Fourth Amendment interests and effective law enforcement. See Oliver, 466 U.S. at 181. Here, the government established probable cause that five players had tested positive for steroids during the CFL’s drug testing program. (R. at 1.)

The magistrate judge authorized the seizure of “all computer records, files, and equipment” relating to the administered tests because of the inherent complexities in searching computer data. (R. at 8.) While the warrant limited the search to data “reasonably related to the investigation” of the five players, the government discovered positive steroid and narcotic test results for “many” other players. (R. at 9.) The government retained this information and thereafter expanded the scope of its investigation to illegal substance abuse by all athletes. (R. at 9.) The government “conceded a lack of probable cause” to retain the test results of players outside the scope of the warrant, but asserted the plain view exception. (R. at 9.)

The Fourteenth Circuit correctly held that the plain view exception “would virtually wipe out Fourth Amendment protections for computer searches.” (R. at 13.) The court acknowledged that the seizure of “all the computer equipment and hard drives” was necessary, but stated that the use of the exception failed to protect the information of individuals for whom the government did not have probable cause. (R. at 13.) The exception would allow the government to “seize the haystack to look for the needle,” and thereafter assert that the information relating to the other players test results was in plain view. See United States v. Hill, 459 F.3d 966, 975 (9th Cir. 2006). The court recognized that this Court warned in Coolidge that the plain view exception could be used to nullify the Fourth Amendment’s warrant requirement. (R. at 11.) Consistent with this Court’s warnings, the Fourteenth Circuit correctly balanced the need for effective law enforcement and an individual’s Fourth Amendment interests by insisting the government waives reliance upon the plain view exception.

b. Requiring That The Segregation and Redaction Process Be Performed By Either Specialized Personnel Or An Independent Third Party Who Agrees Not To Disclose Any Unresponsive Data Is Consistent With This Court’s Jurisprudence.

Requiring specialized personnel or an independent third party to segregate and redact information that is not the target of the warrant ensures that the search of computer evidence will not become the general exploratory search that this Court has repeatedly prohibited. See, e.g., Coolidge, 403 U.S. at 467 (stating a general exploratory search is the “specific evil” the particularity requirement is designed to prevent). The inherent problem in conducting a search of computer data is that information of private individuals that is not the target of the search is often “intermingled” with the otherwise seizable materials. Comprehensive Drug Testing, 579 F.3d at 998; see also Aaron S. Lowenstein, Search and Seizure on Steroids: United States v. Comprehensive Drug Testing and Its Consequences for Private Information Stored on Commercial Electronic Databases, 6 CARDOZO PUB. L. POL’Y & ETHICS J. 101, 102 (2007) (“[M]aterials that are responsive to a search warrant are said to be ‘intermingled’ when they are so mixed with irrelevant materials As a practical matter, potentially every search of a computer database presents a problem of intermingled documents.”). The intermingled nature of electronic data and the ability of wrongdoers to make relevant information difficult to locate requires officials to have a “thorough understanding of the filing and classification systems.” Comprehensive Drug Testing, 579 F.3d at 1004. It is not in dispute that conducting an effective search is a “difficult, exacting and sensitive task” that may require “the need to scoop up large quantities of data, and sift through it carefully for concealed or disguised pieces of evidence,” but that does not diminish an individual’s Fourth Amendment protections. Id. (explaining that this process creates the risk that every warrant for electronic information could become a general warrant and render the Fourth Amendment irrelevant).

The segregation and redaction requirement recognizes the “daunting realities of electronic searches” while maintaining the government’s ability to search and seize the information for which they had probable cause. See id. at 1006. Over thirty-five years ago, the Ninth Circuit noted that it was “rare” when documents would be “so intermingled that they” could not feasibly be sorted onsite and therefore required a broad seizure to conduct an offsite review. Tamura, 694 F.2d at 595–96 (disapproving of the wholesale seizure of several boxes and file drawers). But Tamura “preceded the dawn of the information age.” Comprehensive Drug Testing, 579 F.3d at 996 (explaining that electronic storage of data has become a “way of life”).

The reality of conducting an electronic search is that the data responsive to the warrant will be intermingled with private data unsupported by probable cause. See id. at 1005. In Comprehensive Drug Testing, the government’s search for the relevant records of the players named in the warrant not only lead to the discovery of drug testing results for those players but also to the discovery of results for hundreds of other baseball players. Id. Recently, several circuits have acknowledged the evolving complexities of computer searches and intermingled data. See Adjani, 452 F.3d at 1152 (recognizing that computers are “simultaneously file cabinets” that contain innocent information intermingled with evidence of crimes); United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001) (“[T]here is a great[] potential for the intermingling of documents and a consequent invasion of privacy when police execute a search for evidence on a computer”); Trulock v. Freeh, 275 F.3d 391, 404 (4th Cir. 2001) (recognizing that “the law of computers is fast evolving”); United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999) (searching computers requires officers to come across intermingled, irrelevant information). As previously discussed, the amount of information to search, the complexities of a search, and the potential hazards of conducting electronic searches often require the broad

seizure of electronic data. See Comprehensive Drug Testing, 579 F.3d at 1004. Therefore, segregating and redacting unresponsive information that is intermingled with information supported by probable cause is necessary to ensure that searches do not automatically become the general exploratory searches that this Court has consistently refused to sanction. See Garrison, 480 U.S. at 84; Comprehensive Drug Testing, 579 F.3d at 1004.

Requiring specialized personnel or an independent third party to segregate and redact the irrelevant information ensures that this process “will not become a vehicle” to acquire information for which the government lacks probable cause. Comprehensive Drug Testing, 579 F.3d at 1004. While the government may argue that it is an unnecessary burden to have a third party segregate and redact the unresponsive data, the requirement explicitly provides that government personnel may perform this task if they “agree not to disclose any information other than that which is the target of the warrant.” (R. at 17.) This permits an effective search because the government will acquire the data for which they had probable cause. See Comprehensive Drug Testing, 579 F.3d at 1000. It also protects the Fourth Amendment rights of individuals for whom the government lacked probable cause by precluding the government from acquiring the unresponsive, intermingled data inherent in the digital evidence context. Id. at 999. In Comprehensive Drug Testing, the investigating agent reviewed data for “all professional baseball players and used it to generate additional warrants” to expand the investigation beyond names in the initial warrant. Id. The court imposed the segregation and redaction requirement to protect the confidential records of those individuals not listed in the warrant while still permitting an effective search. Id.

Similarly in this case, the government had probable cause to believe five professional football players were illegally using steroids. (R. at 7.) The CFL hired StarTests to conduct drug

tests on all CFL players, and the government obtained a warrant to search all computer equipment and files at StarTests. (R. at 8.) While the warrant restricted the data review process to “appropriately trained personnel,” it failed to impose a segregation and redaction requirement and it did not prohibit personnel from communicating unresponsive data to the government. (R. at 14.) The personnel conducting the search of intermingled data provided the government with the drug-testing results of players not named in the warrant, and the government thereafter expanded the scope of its investigation to cover drug abuse by all professional athletes. (R. at 9.)

The government turned an otherwise limited search into a general exploratory search to acquire unresponsive data. See Garrison, 480 U.S. at 84 (stating that exploratory searches violate the Fourth Amendment). The record reflects that the government “conceded a lack of probable cause” for the additional information, but nevertheless used the information to expand the investigation. (R. at 9.) The Fourteenth Circuit correctly required the segregation and redaction of computer evidence to be done by a party who agrees to not disclose any information beyond that which is the target of the warrant. (R. at 17.) Not only does this procedure “ensure that agents’ eyes only see images and documents authorized by a warrant supported by probable cause,” but it also sufficiently protects the Fourth Amendment interests of those individuals whose irrelevant and private information was intermingled with responsive data. (R. at 13.)

This process could have been accomplished in a few simple steps. StarTests used a “computer-hopping” procedure to protect the confidentiality of all its clients, including CFL players. (R. at 2.) The procedure was as follows: the first computer database contained the players’ personal and health information; the second assigned each player an identification number; and the third contained the test results, “with the subjects identified only by their identification number.” (R. at 2.) Therefore, the computer trained personnel simply had to

locate the five listed players' identification numbers in the second database and then locate those identification numbers in the third database to acquire the relevant results. See Comprehensive Drug Testing, 579 F.3d at 1016 (Bea, J., concurring) (explaining a copy-and-paste procedure to ensure officials only acquire drug testing for which they had a warrant). The relevant results would then be given to the appropriate officials so they could search the information for which they had probable cause. In essence, the computer personnel would have been an "effective barrier" between the irrelevant information and the case agents. (R. at 15.) This would be a proper balance between constitutionally protected rights and effective law enforcement, and is therefore consistent with this Court's jurisprudence. See Oliver, 466 U.S. at 181.

c. Requiring Disclosure Of The Actual Risks Of Destruction Or Concealment Of Information, As Well As Prior Efforts To Seize That Information In Other Courts, Strikes An Appropriate Balance Between Fourth Amendment Protections And The Ability To Conduct An Effective Search.

Disclosure of the risks associated with acquiring information supported by probable cause is consistent with this Court's jurisprudence and the Fourth Amendment because it permits a magistrate judge to balance these protections against the appropriate means to conduct an effective search. See Coolidge, 403 U.S. at 481. Even though a broad warrant of computer data is often required, courts require sufficient justification for such a warrant. See Comprehensive Drug Testing, 579 F.3d at 998; Adjani, 352 F.3d at 1145. The implicit fear is that officials will discuss the "theoretical" and "general" risks associated with conducting any computer search in an "effort to seize" more data than which it had probable cause. Comprehensive Drug Testing, 579 F.3d at 1000 (explaining that the government's contentions "created the false impression" that if a broad seizure was not granted quickly the data would be forever lost).

The government contends that it was not required to provide disclosure of any risks besides the "difficulties common to all computer searches." (R. at 8.) The court explained that

there was no risk of destruction, but rather only a risk of concealment because StarTests had a duty to protect confidential information. (R. at 14.) Therefore, if this information was disclosed in the warrant, the judge could have appropriately instructed the computer personnel to perform the simple process of matching the identification numbers with the corresponding test results. (R. at 14.) Potentially exposing “exceedingly sensitive information” of individuals for whom the government lacked probable cause “calls for greater vigilance on the part of judicial officers in striking the right balance between . . . law enforcement and the right of individuals.” Comprehensive Drug Testing, 579 F.3d at 1006. Consistent with this Court’s jurisprudence, this process enables judges to sufficiently balance these competing interests when issuing warrants. See, e.g., Oliver, 466 U.S. at 181; Coolidge, 403 U.S. at 481.

d. Requiring That The Government’s Search Protocol Is Designed To Uncover Only The Information For Which It Has Probable Cause Is Consistent With The Warrant Clause.

Requiring that the government’s search protocol is designed to uncover only the information for which it has probable cause is consistent with this Court’s repeated assurance that the Warrant Clause protects individuals from general exploratory searches. See e.g., Coolidge, 403 U.S. at 466. Such an approach enables the government to acquire all the data for which it had probable cause, while also protecting the privacy interests of the individuals for whom the government lacked probable cause. Permitting otherwise displays “deliberate overreaching by the government” to seize more information than necessary. Comprehensive Drug Testing, 579 F.3d at 1000. While the government claims that this is an unnecessary and burdensome safeguard, failure to impose this restriction would permit the “callous disregard of the Fourth Amendment” by allowing the government to reach information “clearly not covered by the warrant.” Id.

The search protocol in this case failed to meet the Fourth Amendment’s particularity requirement. (R. at 15.) The government conducted an unnecessarily overbroad, general search of the computer databases. See Garrison, 480 U.S. at 84. As previously discussed, the “computer-hopping” procedure did not require the government to search through the results of every player. (R. at 14.) The search protocol should have stated that the personnel locate the five players’ identification numbers in the first computer, and then match their identification numbers with the corresponding drug-testing results. (R. at 14.) Rather than using an effective, particular search like the one just described, the government acquired the test results for many players beyond the five listed in the warrant. (R. at 9.)

The search in this case was unreasonable for two reasons. First, the computer personnel failed to act as an “effective barrier” between the irrelevant information and the case agents. (R. at 15.) In fact, the opposite occurred when the government viewed the results of players not named in the warrant and decided to expand its investigation. (R. at 9.) Second, the search displayed a “deliberate overreaching” to seize data beyond the scope of the warrant.

Comprehensive Drug Testing, 579 F.3d at 1000. While the government contends it only “came across the test results” of the other players, (R. at 2.), the record fails to support this proposition.

There are only two manners in which the government could have “come across” these results. First, the government could have acquired the identification numbers for every player and then matched each number with its respective test result. Or, the government could have recorded the identification numbers that corresponded with positive test results and then matched the number with each player’s name. Either way demonstrates a complete disregard of the Fourth Amendment and a general, exploratory search, which is the “specific evil” the Warrant Clause is designed to prevent. See Coolidge, 403 U.S. at 467.

e. Requiring The Government To Destroy Or Return Non-Responsive Data Is Consistent With An Individual's Constitutionally Protected Rights.

Requiring the return of non-responsive data is consistent with an individual's Fourth Amendment protections and Federal Rule of Criminal Procedure 41(g). Such a requirement ensures that the government will not retain irrelevant information that was only acquired because of the inherent, intermingled nature of electronic evidence. See Adjani, 452 F.3d at 1152. Additionally, Rule 41(g) provides that a "person aggrieved by an unlawful search and seizure of property . . . may move for the property's return." FED. R. CRIM. P. 41(g).

If the government fails to adhere to the first four procedural safeguards, then an illegal search has occurred and an individual may bring a Rule 41(g) motion. See Kitty's East v. United States, 905 F.2d 1367, 1370 (10th Cir. 1990). When a party against which no criminal charges are brought files a Rule 41(g) motion, the court invokes its "civil equitable jurisdiction" to determine if the property should be returned. See Ramsden v. United States, 2 F.3d 322, 324–25 (9th Cir. 1993). The court will balance four factors: whether the government displayed a callous disregard for the constitutional rights of the movant; whether the movant has an individual interest in and need for the property; whether the movant would be irreparably injured by denying return of the property; and whether the movant has an adequate remedy at law. Id.

This provides an appropriate balance between law enforcement and an individual's Fourth Amendment rights. As discussed above, the record reflects that the government failed to abide by the other procedural safeguards and therefore disregarded the CFL's Fourth Amendment rights. Second, the CFL has "standing" to bring this motion because they have an individual interest and need for the property. (R. at 16.) Third, denying the return of the results to the CFL would irreparably injure them. Retaining the results of the players not listed in the warrant could lead to extensive litigation, (R. at 16.), which would effectively remove these

players from the field. Also, the CFL promised the players their results would remain confidential so there is a potential lawsuit to be filed against the CFL. (R. at 1.) Fourth, the return of the unlawfully seized data is the only adequate remedy. (R. at 16.) Compensating the CFL and retaining the information is not an adequate remedy because the government could continue to use the information and expand its investigations even further. (R. at 16.)

B. The 2009 Amendments To Fed. R. Crim. P. 41(g) Are Consistent With The Guidelines Set Forth By The Fourteenth Circuit.

The amendments do no more than acknowledge the inherent necessity of over-seizing data in digital evidence cases. Specifically, Rule 41(e) permits the government to conduct a broad seizure of data and conduct a further review to determine what information is within the scope of the warrant, and Rule 41(f) states that the investigating officer "may retain a copy of the electronically stored information that was seized or copied." FED. R. CRIM. P. 41. In essence, the amendments address the "two-step process inherent in electronically stored information." FED. R. CRIM. P. 41 advisory committee's note. While it may be argued that these amendments trump the procedural safeguards imposed by the Fourteenth Circuit, the Advisory Committee Note states that the "amended rule does not address the specificity of description that the Fourth Amendment may require in a warrant for electronically stored information, leaving the application of this and other constitutional standards . . . to ongoing case law development." *Id.*

C. The Guidelines Assist Magistrates In Protecting An Individual's Constitutionally Protected Rights When Magistrates Issue Warrants In Digital Evidence Cases.

It is uncontested that it is the duty of "neutral and detached magistrates" to issue search warrants. *See Coolidge*, 403 U.S. at 449; *Johnson v. United States*, 333 U.S. 10, 14 (1948). In recognizing the inherent complexities electronic searches and the Fourth Amendment interests at stake, the Ninth Circuit stated: "Everyone's interests are best served if there are clear rules to

follow that strike a fair balance between the legitimate needs of law enforcement and the right of individuals and enterprises to the privacy that is at the heart of the Fourth Amendment.”

Comprehensive Drug Testing, 579 F.3d at 1006. The guidelines set forth by the Fourteenth Circuit permit the government to review the data for which it had probable cause. Magistrates still have discretion in determining the need for a broad search, accessing search protocols, and balancing privacy protections against the government’s needs to conduct a search.

This Court stated “we must not lose sight of the Fourth Amendment’s fundamental guarantee . . . [and] ‘it is the duty of courts to be watchful for the constitutional rights of citizens, and against any stealthy encroachments thereon.’” Coolidge, 403 U.S. at 453 (quoting Boyd v. United States, 116 U.S. 616, 635 (1886)). The Ninth and Fourteenth Circuits adhered to this principle by striking an appropriate balance between Fourth Amendment protections and the needs of the government in conducting effective searches of digital evidence. Accordingly, this Court should affirm the decision of the Court of Appeals for the Fourteenth Circuit.

CONCLUSION

For the reasons set forth above, the Respondent respectfully requests that the judgment of the United States Court of Appeals for the Fourteenth Circuit be affirmed.

Respectfully submitted,

Team 18
Counsel for Respondent

January 13, 2010