

Case No. 2009-H20

---

**In the Supreme Court of the United States**

---

UNITED STATES OF AMERICA,  
*Petitioner,*

v.

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

---

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

---

**BRIEF FOR RESPONDENTS**

---

COMPETITION NUMBER 16

## TABLE OF CONTENTS

TABLE OF AUTHORITIES .....	iii
QUESTION PRESENTED.....	1
OPINIONS BELOW.....	1
CONSTITUTIONAL PROVISIONS AND STATUTES INVOLVED.....	3
STATEMENT OF THE CASE.....	3
SUMMARY OF THE ARGUMENT .....	5
ARGUMENT .....	6
I. The Colonial Football League Can Sue on Behalf of its Players Under Fed. R. Crim. P. 41(g).....	6
A. <i>The Government’s Unlawful Search and Seizure         Directly Aggrieved the CFL</i> .....	6
B. <i>The Government’s Unlawful Search and Seizure Aggrieved the CFL as an         Association that Represents its Players</i> .....	8
i. <i>The CFL’s Players have Standing to Sue on their own Behalf</i> .....	8
ii. <i>Because the CFL Required all of its Players to Submit to Drug Testing under             the Auspices of Protecting Confidentiality, it Directly Assumed Responsibility             for each Player’s Property Interests</i> .....	9
iii. <i>The CFL’s Players Need not be Parties to its Rule 41(g) Motion</i> .....	10
II. The Government Should not be Permitted to Rely on the Plain View Exception in Digital Searches. ....	11
A. <i>Digital Searches are Different from, and more Invasive than, Physical Searches,         and therefore do not fit within Existing Search and Seizure Doctrine</i> .....	12
B. <i>The Rationale for the Plain View Doctrine does not Exist         in the Digital Context</i> .....	15
C. <i>The Plain View Test Fails to Regulate         Government Warrantless Seizures Effectively</i> .....	16

D. <i>Efforts to Compensate for the Deficiencies of the Plain View Doctrine have Failed</i> .....	19
III. The Particularity Requirement must be Heightened in the Digital Evidence Context.....	21
A. <i>Traditional Fourth Amendment Reasonableness and Particularity Protect against General Searches</i> .....	21
B. <i>Segregation of Digital Media Requires Increased Particularity Requirements</i> .....	22
C. <i>The StarTests Warrant and Seizure were Unreasonable Under Existing Fourth Amendment Requirements</i> .....	26
CONCLUSION.....	27

## TABLE OF AUTHORITIES

### Federal Cases

<i>Andresen v. Maryland</i> , 27 U.S. 463 (1976) .....	13
<i>Arizona v. Hicks</i> , 480 U.S. 321 (1987) .....	15, 26
<i>Boone v. Spurgess</i> , 385 F.3d 923 (6th Cir. 2004) .....	16
<i>Coolidge v. New Hampshire</i> , 403 U.S. 443 (1971) .....	11, 21
<i>Guest v. Leis</i> , 225 F.3d 325, 335 (6th Cir. 2001) .....	17
<i>Hunt v. Wash. Apple Adver. Comm’n</i> , 423 U.S. 333 (1977) .....	8
<i>Horton v. California</i> , 496 U.S. 128 (1990) .....	<i>passim</i>
<i>Marron v. United States</i> , 275 U.S. 192 (1927) .....	26
<i>Nat’l Hockey League Players’ Ass’n v. Plymouth Whalers Hockey Club</i> , 325 F.3d 712 (6th Cir. 2003) .....	10
<i>Pennell v. City of San Jose</i> , 485 U.S. 1 (1988) .....	8, 11
<i>Rakas v. Illinois</i> , 439 U.S. 128 (1978) .....	6, 11
<i>Trupiano v. United States</i> , 334 U.S. 699 (1948) .....	26
<i>United States v. Abrams</i> , 615 F.2d 541 (1st Cir. 1980) .....	22
<i>United States v. Carey</i> , 172 F.3d 1268 (10th Cir. 1999) .....	14, 18, 19, 20
<i>United States v. Comprehensive Drug Testing</i> , 579 F.3d 989 (9th Cir. 2009) .....	<i>passim</i>
<i>United States v. Dichiarinte</i> , 445 F.3d 126, 128 (7th Cir. 1971) .....	17, 18
<i>United States v. Johns</i> , 707 F.2d 1093 (9th Cir. 1983) .....	7
<i>United States v. Johns</i> , 851 F.2d 1131 (9th Cir. 1988) .....	7
<i>United States v. Miranda</i> , 325 Fed. Appx. 858 (11th Cir. 2009) .....	17, 18, 20, 25
<i>United States v. Pollock</i> , 726 F.2d 1456 (9th Cir. 1984) .....	7

<i>United States v. Spilotro</i> , 800 F.2d 959 (9th Cir. 1986) .....	27
<i>United States v. Taketa</i> , 923 F.2d 665 (9th Cir. 1991) .....	7, 8
<i>United States v. Tamura</i> , 694 F.2d 591 (9th Cir. 1982).....	21, 22, 23
<i>United States v. Walser</i> , 275 F.3d 981 (10th Cir. 2001).....	13, 14
<i>United States v. Wong</i> , 334 F.3d 831 (9th Cir. 2003).....	18, 27
<i>Warth v. Seldin</i> , 422 U.S. 490 (1975).....	10, 11

#### Federal Statutes

U.S. Const. amend. IV .....	3, 21
Fed. R. Civ. P. 41(g) .....	3, 6

#### State Cases

<i>In re Search of 3817 W. West End</i> , 321 F. Supp. 2d 953 (N.D. Ill. 2004).....	13
<i>United States v. Gray</i> , 8 F. Supp. 2d 524 (E.D. Va. 1999).....	17, 20
<i>United States v. Hunter</i> , 13 F. Supp. 2d 574 (D. Vt. 1998).....	13

#### Secondary Authorities

Derek Regensburger, <i>Bytes, Balco and Barry Bonds: An Exploration of the Law Concerning the Search and Seizure of Computer Files and an Analysis of the Ninth Circuit’s Decision in United States v. Comprehensive Drug Testing, Inc.</i> , 97 J. Crim. L. & Criminology 1151 (2007) .....	6, 15
Oris S. Kerr, <i>Searches and Seizures in a Digital World</i> , 119 Harv. L. Rev. 531 (2005).....	12, 14, 19
Lee Rainie, Pew Res. Ctr., <i>Internet Broadband and Cell Phone Statistics</i> (2010) .....	13
Michael Madow, <i>Private Ownership of Public Image: Popular Culture and Publicity Rights</i> , 81 Cal. L. Rev. 125 (1993) .....	9
Robert Moore, <i>To View or not to View: Examining the Plain View Doctrine and Digital Evidence</i> , 21 Am. J. Crim. Just. 58 (2004) .....	17

NFL Personal Conduct Policy, available at:  
<http://www.nflplayers.com/user/template.aspx?fmid=181&lmid=336&pid=0&type=n> ..... 9

Raphael Winick, *Searches and Seizures of Computers and Computer Data*,  
8 Harv. J.L. & Tech. 75 (1994)..... 14

## QUESTIONS PRESENTED

1. Whether under Fed. R. Crim. P. 41(g), the Colonial Football League has standing to file a motion for return of its players' property that was illegally seized by the federal government;
2. Whether the government can no longer rely on the "plain view" exception to avoid the Fourth Amendment's warrant requirements in searches of digital material, such as computers, hard drives and disks;
3. Whether federal magistrates must abide by a heightened particularity requirement in the digital evidence context, as dictated by the Ninth Circuit's decision in *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989 (2009).

## OPINIONS BELOW

The Colonial Football League (CFL) and StarTests, Inc. (StarTests) filed a motion against the United States of America under Fed. R. Crim. P. 41(g), charging that the government illegally seized their property and should return it. R. 1.<sup>1</sup> CFL and StarTests asserted that the government violated the Fourteenth Amendment by exceeding the scope of its search warrant. *Id.* at 4. In response, the government first challenged CFL's and StarTests's standing. Then, relying on the "plain view" doctrine,<sup>2</sup> the government argued that it legally could seize information it came across about other players and substances not named in the warrant. *Id.* The United States District Court for the District of Wythe denied the Rule 41(g) motion upon finding

---

<sup>1</sup> R. refers to the Record, which includes the District Court's decision in *Startests, Inc. and the Colonial Football League v. United States*, Case No. 2010-W20 and the U.S. Circuit Court of Appeals for the Fourteenth Circuit's decision in *StarTests, Inc. and the Colonial Football League v. United States of America*, Case No. 2010-W23.

<sup>2</sup> As this Court clarified in *Horton v. California*, 496 U.S. 128, 136-37 (1990), the "plain view" doctrine allows the government to lawfully seize information that it finds in "plain view" when it is searching lawfully for other information. Evidence seized under this doctrine must pass a 3-part test: 1) the officer's presence in the location of the evidence must be lawful; 2) its seizure must be pursuant to a "lawful right of access"; and 3) its "incriminating character" need be "immediately apparent." *Id.*

the government's warrant valid and that its seizure of evidence passed the plain view doctrine's test. *Id.* at 1.

A timely notice of appeal was filed. *Id.* at 7. StarTests and CFL alleged the district court erred in failing to recognize that the government's search warrant lacked particularity in violation of Supreme Court Fourth Amendment precedent, and in its application of the plain view doctrine to a search and seizure of digital evidence. *Id.* StarTests and CFL further challenged the district court's failure to condemn the warrant as overbroad and invalid, claiming instead that the government had no lawful right to access information about players not named within it. *Id.* The government countered that the district court's error was in finding that the CFL had standing to bring the Rule 41(g) motion. *Id.* at 9. The government also contended the plain view doctrine should apply in the digital context, making its seizure of StarTests's and the CFL's equipment and databases lawful. *Id.* at 9–10. The Fourteenth Circuit reversed the district court's decision, upholding the validity of the CFL's standing but finding the government seized the evidence based on an "overly broad" warrant that failed to meet the standards set out by the Ninth Circuit in *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989 (9th Cir. 2009). *Id.* at 17. The government filed a timely appeal. *Id.* at 20.

In response to this appeal, the CFL and StarTests respectfully request that this Court affirm the Fourteenth Circuit's decision granting judgment to the CFL and StarTests, on the ground that the CFL has standing to sue, the government should be required to waive reliance on the plain view doctrine in the digital context, and adopt a heightened particularity standard for digital searches.

## CONSTITUTIONAL PROVISIONS AND STATUTES INVOLVED

### U.S. Const. amend IV:

“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.

### Fed. R. Crim. P. 41(g):

“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.”

## STATEMENT OF THE CASE

In 2005, the Colonial Football League (CFL) threatened to revoke the membership of any team that did not compel its players to submit to drug tests administered by StarTests, Inc. (StarTests). R. 1. The CFL and StarTests assured the players that their names and test results would be stored confidentially and anonymously by StarTests at its facility, as the tests were only being conducted to determine the extent of the steroid problem in professional football. *Id.* at 8. Both the CFL and StarTests persuaded the players to participate in the testing by promising that the only information released to the CFL and the public would be the percentage of players who tested positive for steroids. *Id.* The CFL soon became one of StarTests's largest clients, with almost all of StarTests's computers containing some information about the CFL's drug tests. *Id.* at 2.

Nearly four years later, the Federal Bureau of Investigation (FBI) began investigating five of the CFL's players who it suspected to be illegal steroid users. *Id.* at 1. The FBI was able to convince a magistrate judge in the United States District Court for the District of Wythe that it

had probable cause that each of the five CFL players had tested positive for using steroids during the CFL's testing that StarTests administered. *Id.* at 8. Although the FBI sought to seize an extremely broad array of information, the judge's search warrant restricted the search and seizure of the StarTests facility to "information 'reasonably related to the investigation into the five named players' illegal steroid use.'" *Id.* at 2. The warrant further limited the lawful seizure to computers that "law enforcement personnel trained in searching and seizing computer data" deemed necessary to search. *Id.* Additionally, once these personnel decided what equipment should be seized, the warrant further restricted the search to require "appropriately trained personnel" to review all data, extract only the information within the warrant's purview, and to return the remainder to its rightful owners, the CFL and StarTests. *Id.*

Upon realizing that StarTests had organized the CFL testing information in a complex manner in order to preserve the CFL's players' anonymity and confidentiality, the FBI decided to seize or copy all of StarTests's computers, digital media, documents and specimens, which contained information about all of the CFL's players. *Id.* at 8. At the FBI's office, agents viewed all of StarTests's databases containing information about the CFL's players. *Id.* at 2. After several weeks of searching, the FBI found the results for the five players named in the warrant, but also came across information indicating illegal steroid and other substance abuse by other CFL players. *Id.* at 9. Without getting a new warrant, the FBI broadened its investigation to include other illegal drugs and their use by other professional football players, and made the executive decision to hold on to StarTests's databases. *Id.* at 2. Only after it made copies of StarTests's hard drives did the FBI return equipment it deemed unnecessary to retain. *Id.*

## SUMMARY OF THE ARGUMENT

The CFL has standing to sue under Fed. R. Crim. P. 41(g), both directly and indirectly. The CFL satisfies the requirements for independent standing because the FBI seized test results that the CFL paid for and therefore owned. Additionally, the CFL has standing to protect the property of its members—its players—because each would have standing to sue on his own behalf, because it required them to submit to testing as a term of employment under the assurance that the results would be stored anonymously and confidentially, and because the CFL’s players need not be parties to its Rule 41(g) motion.

Additionally, the government should be forewarned from relying on the plain view doctrine when applied to seizures of digital media. The deep differences between seizures of traditional physical objects and digital media invite a reconsideration of existing Fourth Amendment doctrine. Not only does the rationale underlying the plain view doctrine disappear in the digital context, but the plain view doctrine’s three-pronged test, and judicial attempts to compensate for it, entirely fail to regulate warrantless seizures of digital media.

Finally, although existing Fourth Amendment particularity requirements sufficiently limit searches of physical objects, the nature of digital media demands heightened requirements. This Court should adopt the particularity mandates established in *United States v. Comprehensive Drug Testing* for warrants involving digital media. These requirements will prevent digital warrants from becoming judicially sanctioned vehicles for general searches. If this Court declines to adopt the particularity requirements of *Comprehensive Drug Testing*, this Court should rule the government’s warrant was impermissible under existing Fourth Amendment jurisprudence.

## ARGUMENT

### I. THE COLONIAL FOOTBALL LEAGUE CAN SUE ON BEHALF OF ITS PLAYERS UNDER FED. R. CRIM. P. 41(g).

The CFL has standing to sue under Fed. R. Crim. P. 41(g) because the FBI's illegal search and seizure targeted and victimized it both directly and by association. Rule 41(g) requires the moving party to have been "aggrieved by an unlawful search and seizure of property or by the deprivation of property." Fed. R. Crim. P. 41(g). A party is "aggrieved by an unlawful search and seizure" when it is "a victim of a search or seizure," or "one against whom the search was directed." *Rakas v. Illinois*, 439 U.S. 128, 134–35 (1978). Several years later, the Rule was amended to address injury that can be caused by "the interference with the lawful use of property by persons who are not suspected of wrongdoing." See Derek Regensburger, *Bytes, Balco and Barry Bonds: An Exploration of the Law Concerning the Search and Seizure of Computer Files and an Analysis of the Ninth Circuit's Decision in United States v. Comprehensive Drug Testing, Inc.*, 97 J. Crim. L. & Criminology 1151, 1174 (2007) (quoting Fed. R. Crim. P. 41(g) advisory committee's comments, 1972 Amendment). As a result, "an aggrieved person may seek return of property that has been unlawfully seized, and a person whose property has been lawfully seized may seek return of property when aggrieved by the government's continued possession of it." *Id.* The CFL is both a victim and a target of the government's illegal search and seizure, and suffers from the very harm the Rule and its Amendment seek to redress. As a result, the CFL has both direct and associational standing to file a motion for the return of its property.

#### *A. The Government's Unlawful Search and Seizure Directly Aggrieved the CFL.*

Although the FBI did not search or seize evidence from the CFL's physical headquarters, it did search and seize the CFL's property when it confiscated material from StarTests's facilities. As the Fourteenth Circuit appropriately observed, the CFL arguably "has a stronger

ownership interest in the databases than StarTests does,” as “[i]t paid the facility to administer the tests, and to store the results in its computer databases for anonymity purposes.” R. 10. Having paid for the ownership rights of the material, the CFL merely stored its property off-site with StarTests, a “business specializing in conducting drug tests for professional sports franchises,” to best ensure it would make good on its promise to its players that their test results would be kept confidential and anonymous. *Id.* at 8; 10. As a result, the CFL is not “suing to challenge the search of another party’s office because the evidence is potentially damaging to its business,” as the government contends. *Id.* at 10. Even the government itself referred to its search of the StarTests facility as targeting the “CFL drug test databases.” *Id.*

In the alternative, the CFL has the right to seek the return of StarTests’s property because it contracted with StarTests to collect and store it confidentially. The Ninth Circuit has repeatedly recognized that a party may “contest a search of a third party’s property if he had a reasonable expectation of privacy in the property based on a formal arrangement.” *United States v. Taketa*, 923 F.2d 665, 671 (9th Cir. 1991) (citing *United States v. Johns*, 851 F.2d 1131, 1135–36 (9th Cir. 1988) (per curiam) (“formalized arrangement indicating joint control and supervision supports a legitimate expectation of privacy”); *United States v. Pollock*, 726 F.2d 1456, 1465 (9th Cir. 1984) (“defendant exercised ‘joint control’ over drug laboratory in his friend’s house”); *United States v. Johns*, 707 F.2d 1093, 1099–1100 (9th Cir. 1983) (“defendant could contest seizure of drugs from another’s vehicle because of their formal arrangement to transport contraband”)). The CFL’s circumstances differ greatly from those in *United States v. Taketa*, the case on which the government’s argument rest. 923 F.2d at 671. In *Taketa*, the Ninth Circuit found objectively unreasonable a federal agent’s subjective expectation of privacy in a personal office at a facility run by the Drug Enforcement Administration. *Id.* The CFL, in

contrast, contracted with StarTests for, and thus undeniably had a “reasonable expectation of privacy” in, the computer databases of which it commissioned the creation. *See id.* at 671.

*B. The Government’s Unlawful Search and Seizure Aggrieved the CFL as an Association that Represents its Players.*

Even if this Court does not find that the CFL’s own physical property was searched or seized, the CFL has standing as an association on behalf of its players, whose test results the FBI improperly confiscated. “Associational standing” is established by a three-part test that demonstrates an organization’s need to protect its members’ interests. *Pennell v. City of San Jose*, 485 U.S. 1, 7 n.3 (1988). An association has standing 1) when its individual members would have sufficient standing on their own; 2) when it seeks to protect interests that serve its organizational mission; and 3) when the individual members need not participate in asserting the claim. *Id.* at 7 (quoting *Hunt v. Wash. Apple Adver. Comm’n*, 423 U.S. 333, 343 (1977)). In filing a Rule 41(g) motion, the CFL satisfies all three prongs of the test.

*i. The CFL’s Players have Standing to Sue on their own Behalf.*

First, as the Wythe District Court observed and the Fourteenth Circuit affirmed, the CFL’s players undoubtedly have independent standing to seek the return of their unlawfully seized property. *See* R. 3; 10. The testing commissioned by the CFL and administered by StarTests catalogued information about what should have remained the player’s most private personal property—their own “bodily fluids.” *Id.* at 10. In *Comprehensive Drug Testing*, the Ninth Circuit considered a Fourth Amendment challenge to the seizure of drug-test results of hundreds of professional baseball players. *See United States v. Comprehensive Drug Testing*, 579 F.3d 989 (9th Cir. 2009). There, the court held that each player “could certainly sue in his own right to seek return of his own drug testing records.” *Id.* The same premise applies to the CFL’s professional football players.

- ii. *Because the CFL Required all of its Players to Submit to Drug Testing under the Auspices of Protecting Confidentiality, it Directly Assumed Responsibility for each Player's Property Interests.*

Second, it is germane to the CFL's organizational purpose to retrieve the information it contracted StarTests to gather and guard. The purpose of a professional sports league is to bring high quality athletic competitions to the public, which makes protecting a league's players fundamental to delivering its product. A professional sports league is only as strong as the reputation of its players, and players' reputations derive from both athletic prowess and perceived moral and ethical standing.<sup>3</sup> It is for this reason that all major American professional sports leagues require their players to adhere to a code of conduct: The NFL Personal Conduct Policy, for example, requires players to "avoid 'conduct detrimental to the integrity of and public confidence in the National Football League.'" See the NFL Personal Conduct Policy, available at: <http://www.nflplayers.com/user/template.aspx?fmid=181&lmid=336&pid=0&type=n>. Even when drug test results eventually exonerate a professional athlete from any suspicions of steroid use, if the government improperly reads the database and makes any indication of continued investigation or allegations of guilt based on having access to those databases without a proper warrant, the information could tarnish that player's and, by extension, his league's reputation. Even more concretely, if a league's players are distracted by the illegal seizure of their property, this distraction may impact their ability to play at the highest level, which impacts the league's organizational mission. Therefore, seeking the return of its players' property furthers the CFL's mission—the players and the League have a shared interest in the integrity of the drug-testing process to which they both consented.

---

<sup>3</sup> See, e.g. Michael Madow, *Private Ownership of Public Image: Popular Culture and Publicity Rights*, 81 Cal. L. Rev. 125, 128 (1993) (arguing that the public monitors professional athletes' "comings and goings, their missteps and heartbreak").

As both lower courts noted, the CFL is contractually obligated to protect its players' privacy interests—the CFL has contracts with the franchises, who have contracts with the players. R. 3; 10. Generally a professional sports league might be considered a separate entity from its players, as represented by their own union or association.<sup>4</sup> Here, however, the CFL assumed responsibility for its players when it required them to submit to drug testing. Because the CFL required each franchise to test each of its players, it made taking the drug tests a condition of employment for all team members. By later acting to protect the results of the testing it itself commissioned, the CFL was directly representing its players' interests in the same capacity that a players' association typically would. *See Comprehensive Drug Testing*, 513 F.3d at 1096 (holding that protecting the players' privacy interests in their drug testing records was directly within the purview of the players' association's "sole purpose: to represent the interests" of professional baseball players). This made the property interest especially acute here because the players' "privacy was intruded upon under the CFL's prerogative." R. 3. The CFL assumed a role as a "protector of players' interests" when it required its players, via the franchises for which they play, to submit to drug testing under the auspices of guarding their anonymity and confidentiality.

*iii. The CFL's Players Need not be Parties to its Rule 41(g) Motion.*

Finally, as both lower courts emphasized, the type of prospective relief the CFL seeks does not require the individual players as parties to the legal action. R. 3. (citing *Warth v. Seldin*, 422 U.S. 490, 515 (1975)). An association may sue on behalf of its members seeking "a declaration, injunction, or some other form of prospective relief." *Warth*, 422 U.S. at 515.

---

<sup>4</sup> *See, e.g., Nat'l Hockey League Players' Ass'n v. Plymouth Whalers Hockey Club*, 325 F.3d 712, 714 (6th Cir. 2003) (allowing the National Hockey League Players Association to sue their league, the National Hockey League, "on behalf of the hockey players it represents.").

Unlike in *Warth*, the CFL seeks only the return of its drug testing information stored in StarTests’s property, and not damages. *See id.* The Ninth Circuit upheld the extension of this premise to the drug-testing context, finding that individual professional athletes need not be party to actions designed to retrieve their drug testing results. *See Comprehensive Drug Testing*, 579 F.3d at 1006–07. The same should apply to the CFL’s drug test results.

Under the standards articulated in *Pennell* and *Rakas*, the CFL has either associational standing or sufficient ownership interest in the seized property to establish standing independently.

## II. THE GOVERNMENT SHOULD NOT BE PERMITTED TO RELY ON THE PLAIN VIEW EXCEPTION IN DIGITAL SEARCHES.

It is axiomatic that warrantless searches and seizures are “per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well delineated exceptions.” *Coolidge v. New Hampshire*, 403 U.S. 443, 444–45 (1971). Any exceptions to the warrant requirement must be “jealously and carefully drawn.” *Id.* at 445. The plain view doctrine, one of the few exceptions to the warrant requirement, allows an officer with a valid warrant to seize materials not specified in the warrant and “exten[d] . . . the original justification” for the seizure. *Horton v. California*, 496 U.S. 128, 136 (1990) (quoting *Coolidge*, 403 U.S. at 466).

As the plain view doctrine permits the seizure of materials outside the scope of the warrant, this Court has cautioned that the doctrine “may not be used to extend a general exploratory search from one object to another to another until something incriminating at last emerges.” *Horton*, 496 U.S. at 136. Ultimately, in practice “any evidence seized by police will be in plain view, at least at the moment of seizure.” *Id.* at 134. To prevent the plain view doctrine from swallowing the warrant requirement whole, the doctrine only applies when three

criteria are met. First, the officer must be legally located in a place from which the object can plainly be seen. *Id.* at 137. Second, the officer must have a lawful right of access to the object itself. *Id.* And third, the incriminating character of the object must be immediately apparent. *Id.* at 136.

The plain view doctrine was conceived prior to the computer age, and its rationale and application fare well in the traditional context of physical searches and seizures. However, there are fundamental differences between the nature and seizure of digital information and physical objects. As a result, the rationale behind the doctrine disappears when applied to the digital context, and the doctrine's three-pronged test fails to place a meaningful limit the scope of warrantless seizures. The government therefore should not be permitted to rely on the plain view doctrine in the context of digital seizures, as outlined in *United States v. Comprehensive Drug Testing*, 579 F.3d 989 (9th Cir. 2009).

*A. Digital Searches are Different from, and more Invasive than, Physical Searches, and Therefore do not Fit Within Existing Search and Seizure Doctrine.*

Digital searches and seizures are different from and more invasive than those of traditional physical objects, inviting this Court to reconsider the plain view doctrine's fit in the digital context. This is not surprising, as Fourth Amendment doctrine was not developed with the digital context in mind. Rather, the current doctrine was developed "almost exclusively" to regulate government searches of homes or containers. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. R. 531, 584 (2005).

Yet computers and other digital content equipment are unlike homes or containers: they are "virtual warehouses" that store a "staggering" amount of data. *Id.* at 539, 543. Due to computers' ability to hold so much information, and so many types of information, there is a high potential for intermingling of seizable and non-seizable information in digital searches. In

other words, the needle for which the government has a warrant to search is hidden in a haystack of unrelated data. Courts have long-recognized the problem of digital intermingling. *See, e.g., United States v. Walser*, 275 F.3d 981, 986 (10th Cir. 2001) (“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.”); *In re Search of 3817 W. West End*, 321 F. Supp. 2d 953, 959 (N.D. Ill. 2004) (noting how the storage capacity of computers “increases the risk that many of the intermingled documents will have nothing to do with the alleged criminal activity that creates the probable cause for a search and seizure”). As a result of this intermingling, “over-seizing is an inherent part of the electronic search process.” *Comprehensive Drug Testing*, 579 F.3d at 1006. And as the case at bar demonstrates, such over-seizing can implicate the privacy and confidential information of innumerable third parties.

Even though the problem of intermingled information and over-seizing existed prior to the prevalence of computers, *see Andresen v. Maryland*, 27 U.S. 463, 482 n.11 (1976), the vast storage capacity of computers has given rise to a much larger amount of intermingled and irrelevant data. *See U.S. v. Hunter*, 13 F. Supp. 2d 574, 583 (D. Vt. 1998) (observing that “[c]omputer searches present the same problem as document searches—the intermingling of relevant and irrelevant material—but to a heightened degree”). Furthermore, due to cheap networking and high levels of Internet penetration,<sup>5</sup> it is commonplace that individuals have “personal data that are stored with innumerable strangers.” *Comprehensive Drug Testing*, 579 F.3d at 1005. These individuals may have little control over how their information is saved or with whom it is intermingled. *Id.*

---

<sup>5</sup> It is estimated that 74% of American adults use the Internet, and 60% have broadband access at home. Lee Rainie, Pew Res. Ctr., *Internet, Broadband and Cell Phone Statistics* 3 (2010).

For these reasons, “[a]nalogies to other physical objects, such as dressers or file cabinets, do not often inform . . . [digital seizure] situations.” *Walser*, 275 F.3d at 986. The inaptness of analogies to seizures of physical objects, as well as the ever-increasing usage of computers to store confidential and intermingled data, suggests that digital searches do not fit well within the existing search and seizure framework.

When compared to traditional physical searches of homes, the invasiveness of digital seizures is even more apparent. Traditional physical searches are expensive and time consuming, requiring a specialized and trained team operating on-site. A digital search, conversely, is conducted off-site, free from time pressures, and is relatively cheap to conduct. *Kerr, supra*, at 569–70. Thus, while an invasive home search is possible, computer searches “lower the cost and inconvenience of invasive searches, making such searches the norm rather than the exception.” *Id.* Moreover, it is difficult to carry away an entire warehouse of documents; it is easy to carry away hard drives with, as here, many years worth of confidential medical information belonging to hundreds or thousands of third parties. Such ease of use, coupled with the amount and variety of information that computers store, make computers “tempting targets in searches for incriminating information.” *United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999) (quoting Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 Harv. J.L. & Tech. 75, 104 (1994)).

Accordingly, the massive storage capacity and prevalence of computers, as well as the low cost and high convenience of digital searches, renders current search and seizure doctrine, designed primarily to regulate searches of homes and containers, ill-suited to the digital context. It is time to reconsider the plain view doctrine.

B. *The Rationale for the Plain View Doctrine does not Exist in the Digital Context.*

The rationale for the plain view doctrine, conceived prior to the prevalence of computers, falls apart in the digital context. Properly understood, the plain view doctrine is an extension of the long-recognized authority of police to make warrantless searches in public of contraband or weapons, allowing the police to make such seizures in private spaces for which they already have a warrant. *Arizona v. Hicks*, 480 U.S. 321, 326–27 (1987). The plain view doctrine thus permits authorities to make the type of seizures in private spaces that they had long-been permitted to make in public. *See id.* The rationale behind the doctrine is to save police from obtaining another warrant, during which time the evidence sought could be destroyed, and to ensure the safety of the officers:

[T]he practical justification for [the plain view doctrine] is the desirability of sparing police, whose viewing of the object in the course of a lawful search is as legitimate as it would have been in a public place, the inconvenience and the risk—to themselves or to preservation of the evidence—of going to obtain a warrant.

*Id.* at 327.

While this rationale holds in the physical context, where delays in obtaining a second warrant could lead to the destruction of evidence, the rationale fails in the digital context. When executing a computer search, government agents typically move the computers off-site, copy their data, and return them—which is exactly what occurred here. As the government holds the computers while copying them, there is no risk that evidence will be altered or erased. *See* Derek Regensburger, *Bytes, Balco and Barry Bonds: An Exploration of the Law Concerning the Search and Seizure of Computer Files and an Analysis of the Ninth Circuit's Decision in United States v. Comprehensive Drug Testing, Inc.*, 97. J. Crim. L. & Criminology 1151, 1201 (2007). Therefore, the rationale supporting the plain view doctrine fails in the digital context.

C. *The Plain View Test Fails to Regulate Government Warrantless Seizures Effectively.*

The problem with the plain view doctrine concerns not only its underlying rationale, but its application as well. When applied to digital searches, the plain view doctrine fails to regulate government seizures effectively or adequately. Its three-pronged test requires that the authorities be lawfully present, that the authorities have lawful access to the object seized, and that the object's incriminating character be immediately apparent. *Horton*, 496 U.S. at 136–37. The first prong is not problematic: it simply requires that the officer have an underlying warrant or otherwise be legally present in order for the warrantless seizure to be valid. *See id.* at 137. Examination of the second and third prongs, however, demonstrates that while the plain view doctrine is well designed to regulate warrantless seizures of physical objects, it lacks the same effectiveness when applied to digital information.

The second prong of the plain view doctrine, which requires that the officer have a lawful right of access to the object itself, *id.*, only works to control effectively governmental seizures in the physical context. This prong is “meant to guard against warrantless entry onto premises whenever contraband is viewed from off the premises in the absence of exigent circumstances.” *Boone v. Spurgess*, 385 F.3d 923, 928 (6th Cir. 2004). For example, if police officers were lawfully positioned on the sidewalk (thereby meeting the first prong), and observed illegal marijuana plants growing inside someone's home, they would not be allowed to enter the home absent exigent circumstances. Therefore, “[t]he difference between ‘lawfully positioned’ and ‘lawful right of access’ is . . . that the former refers to where the officer *stands* when she sees the item, and the latter to where she must be to retrieve the item.” *Id.* (emphasis added). Accordingly, there is a *physical* difference between an officer being in a place legally and having

lawful right of access. This difference gives the second prong teeth in the context of a seizure of discrete physical objects.

In a digital seizure, however, no such logical or physical distinctions exist: the difference between the first and second prong dissolves. The problem is that to have lawful access to a computer is to have potential access to every file on the computer. See Robert Moore, *To View or not to View: Examining the Plain View Doctrine and Digital Evidence*, 21 Am. J. Crim. Just. 58, 71 (2004) (remarking that “[t]o ensure that all evidence is uncovered, it is often necessary for forensic examiners to search the entire storage device, section by section”). After all, the government should not have to rely on a suspect’s self-labeling or placement of files; otherwise, suspects would “be able to shield evidence from a search simply by ‘misfiling’ it in a directory labeled ‘email.’” *Guest v. Leis*, 225 F.3d 325, 335 (6th Cir. 2001). Thus, courts have found that as long as a warrant allows seizure of the computer, the second prong is easily met. See, e.g., *United States v. Miranda*, 325 Fed. Appx. 858, 860 (11th Cir. 2009) (unpublished opinion) (officer had a “lawful right to view each file” because the officer had a warrant to search the defendant’s hard drive for evidence of counterfeiting crimes); *United States v. Gray*, 8 F. Supp. 2d 524, 529 (E.D. Va. 1999) (officer “was entitled to examine all of defendant’s files to determine whether they contained items that fell within the scope of the warrant”). In the digital context, such carte blanche entry means access to millions of intermingled files, which can implicate, in a business-related seizure, the files of countless third parties.

Similarly, the third prong of the plain view doctrine functions well in the physical context but fails in the digital context. This prong requires that the incriminating character of the object be “immediately apparent” before it can be subject to the plain view exception. *Horton*, 496 U.S. at 136. For example, in *United States v. Dichiarinte*, 445 F.3d 126, 128 (7th Cir. 1971),

officers were permitted to enter a suspect's home to search for narcotics. While searching for narcotics among the suspect's personal papers, the officers read the papers, which contained evidence of tax fraud. *Id.* at 130. The Seventh Circuit suppressed the documents, finding that their criminal character was "not apparent on a mere surface inspection." *Id.* at 131. Rather, the documents had to be opened and read for their incriminating character to become obvious. *Id.* Thus, in the physical context, the third prong of the plain view doctrine has force.

Yet the strength of the "immediately apparent" prong withers in the digital context. Many courts have simply brushed over this prong, finding that once an officer views an incriminating image on screen, its criminality is immediately apparent. *See, e.g., United States v. Wong*, 334 F.3d 831, 838 (9th Cir. 2003) (holding that once an officer clicked on graphics file, its criminality was immediately apparent); *Miranda*, 325 Fed. Appx. at 860 (same). Because warrants may authorize the seizure and potential viewing of all computer files, and because a computer file's character becomes immediately apparent upon viewing, the "immediately apparent" does little to regulate warrantless digital media seizures.

Admittedly, a situation could arise in the physical document context, where an officer sees an immediately incriminating photograph of child pornography while conducting an unrelated search and is able to seize it under the plain view doctrine. But while it is hard to summon sympathy for those who collect child pornography—either on computers or in shoeboxes—the digital context creates a problem of a different magnitude. Because seizures of computers may necessitate combing through hard drives for months, unearthing mountains of confidential data belonging to third parties, it is critical to place meaningful limits on the government's warrantless seizure authority. The plain view doctrine manifestly fails to do so.

D. *Efforts to Compensate for the Deficiencies of the Plain View Doctrine have Failed.*

Some circuits have tried to compensate for the weakness of the plain view doctrine in creative but ultimately ineffective ways. In *Carey*, the Tenth Circuit tried to do so by focusing on the subjective intent of the officer. *See* 172 F.3d at 1273. After seizing a suspect's computers pursuant to a warrant based on a drug investigation, an officer opened a picture file with a sexually suggestive title because he thought that the file could contain evidence relevant to the drug investigation. *Id.* at 1270–71. Finding child pornography instead, the officer then proceeded to look for and find more child pornography contained in the picture files. *Id.* at 1271. The Tenth Circuit held that, because the officer happened upon the first image inadvertently, that picture fell within the plain view exception. *Id.* However, the search for the subsequent files, in which the officer “expected” to find child pornography, constituted an abandonment and unlawful expansion of the original search. *Id.* at 1273 & n.4. The *Carey* decision demonstrates that attempts to strengthen the plain view doctrine in the digital context are likely futile. First, the Tenth Circuit focused its analysis on the subjective intent of the officer, *id.* at 1272–73, curiously resurrecting the “inadvertence” requirement long ago abandoned by this Court as unworkable. *See Horton*, 496 U.S. at 138 (“[E]venhanded law enforcement is best achieved by the application of objective standards of conduct, rather than standards that depend on the subjective state of mind of the officer.”).

The deeper problem with relying on subjective intent is that in most cases, it will fail to curb the expansion of searches. Under FBI forensic protocol, for example, officers are generally instructed to conduct “highly comprehensive examinations” leaving “no digital stone unturned.” Kerr, *supra* at 579. Thus, if officers are simply following protocol when they examine every file, it would be nearly impossible to demonstrate that the officer had the subjective intent to expand

the scope of the search beyond the warrant. For example, in *Gray*, the court found that the officer permissibly opened all directories on the suspect's computer, including those labeled "Teen" and "Tiny Teen," during a search for evidence of computer hacking. 78 F. Supp. 2d at 526–527. Because the officer's systematic search was "routine," *id.* at 527, there is no way that the officer could intend to expand the scope of the search. Thus, as long as a forensic search protocol is sufficiently comprehensive, focusing on subjective intent as urged in *Carey* does nothing to remedy the weakness of the plain view doctrine in the digital context.

Second, and for the same reason, the fact that the officer in *Carey* abandoned his initial search to begin a new, unrelated search, does not save the plain view doctrine. 172 F.3d at 1277–78. The "abandonment" in *Carey*, after all, would not have occurred had the officers authority to search every file: it is hard to imagine "abandoning" one search for another if the search itself is comprehensive and systematic. And as previously described, courts typically find that officers have the authority to conduct a comprehensive search that can include every file. *See, e.g., Miranda*, 325 Fed. Appx. at 860; *Gray*, 8 F. Supp. 2d at 529.

Accordingly, in the case at bar, it is immaterial that the FBI merely "came across" the new, unrelated information regarding the additional players and substances, rather than abandoned the original search. R. 5. If the FBI had potential access to every file, then a finding of "abandonment" would have been impossible. Therefore, the fact that the officers abandoned the original search in *Carey* and did not do so here is a distinction without a difference, and the "abandonment" requirement in *Carey* does little to compensate for the shortcomings of the plain view doctrine.

Given the lack of rationale for the plain view doctrine, the flimsiness of the three-pronged test, and the failure to strengthen the doctrine by focusing on subjective intent or abandonment,

the best approach is to jettison entirely the doctrine when applied to seizures of digital evidence. This clear approach recognizes that warrantless digital seizures, if left unchecked by reliance on the plain view doctrine, have the potential to breach the privacy of countless third parties. At the same time, waiving reliance on the plain view doctrine in no way affects the government's ability to execute valid warrants.

### III. THE PARTICULARITY REQUIREMENT MUST BE HEIGHTENED IN THE DIGITAL EVIDENCE CONTEXT.

In order to prevent general searches, this Court should adopt the new particularity requirements established in *United States v. Comprehensive Drug Testing* for warrants involving digital media. *See* 579 F.3d 989, 1006 (9th Cir. 2009). If this Court declines to adopt the particularity requirements of *Comprehensive Drug Testing*, this Court should deem the warrant impermissible under existing Fourth Amendment jurisprudence.

#### A. *Traditional Fourth Amendment Reasonableness and Particularity Protect against General Searches.*

The Fourth Amendment seeks to avoid general searches. *See Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). To that end, the Amendment explicitly requires warrants “particularly describing the place to be searched and the persons or things to be seized.” U.S. Const. amend. IV. Throughout the past several decades, courts have struggled to draft warrants with a limited scope where the sought-after evidence, frequently in the form of documents, is intermingled with many other irrelevant or “non-responsive” papers. *See* Brief for Respondent, *supra*, at 12–14. Where the initial segregation of the documents must necessarily involve a large number of non-responsive documents, courts have frequently required the government to seize and hold the documents pending additional judicial approval before proceeding. *See United States v. Tamura*, 694 F.2d 591, 596 (9th Cir. 1982).

A Ninth Circuit case involving intermingled documents is a useful example here. *United States v. Tamura* concerned a warrant authorizing the seizure of records of contracts, payments, and travel involving specific employees and clients of a company. *See* 694 F.2d at 594. To segregate the information on-site, the government agents would have needed to engage in a lengthy sorting process. *See id.* at 594–95. Instead, the government seized all of the office’s accounting records for off-site review, including eleven boxes of computer printouts and twenty-eight drawers of checks and vouchers. *See id.* at 595.

Reviewing the seizure for Fourth Amendment violations, the Ninth Circuit determined the confiscation of all the accounting records was unreasonable, despite the lengthy segregation procedure. *See id.* at 595 (“The wholesale seizure for later detailed examination of records not described in a warrant is . . . ‘the kind of dragnet that the fourth amendment was designed to prevent’”) (quoting *United States v. Abrams*, 615 F.2d 541, 543 (1st Cir. 1980)). The court held where the government encounters documents so “intermingled that they cannot feasibly be sorted on site,” it can “avoid violating Fourth Amendment rights by sealing and holding the documents pending approval by a magistrate of a further search.” *See id.* at 596.

B. *Segregation of Digital Media Requires Increased Particularity Requirements.*

The segregation issues that have emerged in the modern age demand increased particularity requirements for digital media warrants. Unable to draft digital media warrants limiting searches to a small number of relevant files, courts have increasingly been forced to authorize warrants for wholesale search and seizure of vast digital storage systems. Although a government search always has necessarily involved viewing some irrelevant information, the user interfaces particular to computer systems “require examining a great many other files to exclude the possibility that the sought-after data are concealed there.” *See United States v.*

*Comprehensive Drug Testing, Inc.*, 579 F.3d at 1006. Previously, warrants likely exposed individuals only to a cursory government viewing of information protected by the Fourth Amendment. Now, even warrants authorizing a search of a commonplace, digital storage media implicate the “equivalent of millions of pages of information.” *See Id.* at 1004 (noting *Tamura* considered the confiscation of a “few dozen boxes” to be a “broad seizure”).

This Court should adopt the Ninth Circuit’s requirements for federal warrants involving digital media as announced in *United States v. Comprehensive Drug Testing*. *See id.* at 996. In *Comprehensive Drug Testing*, the court considered a Fourth Amendment challenge to the seizure of drug test results of hundreds of professional athletes. *Id.* at 996. In a separate investigation, the federal government gained information linking ten professional baseball players to illegal steroids. *Id.* at 993–95. The government then used that information to get a warrant authorizing the search of all testing results at a drug testing company’s office. *Id.* When executing the search, the government decided on-site segregation would be too lengthy and seized all the company’s digital media for off-site sorting. *Id.* at 998. Addressing the company’s Fourth Amendment challenge, the Ninth Circuit used *Comprehensive Drug Testing* as an opportunity to rework the particularity requirements for the digital age. *Id.* at 997.

The Ninth Circuit began by noting the goal of the Fourth Amendment’s particularity requirement and *Tamura*’s seize and seal mandate was to “maintain the privacy of materials that are intermingled with seizable materials, and to avoid turning a limited search for particular information into a general search of office file systems and computer databases.” *Id.* at 998. Nonetheless, the court recognized the ease with which digital media can hide evidence of criminal activity requires the government closely examine of the contents of virtually every file. *Id.* at 998. To “update” the Fourth Amendment protections, the court introduced new

requirements for warrants involving digital media: 1) the government must waive reliance on the plain view doctrine; 2) warrants must include the actual risks of destruction of information as well as prior efforts to obtain that information, 3) the government must use a search protocol designed only to uncover information for which it has probable cause; 4) the government must destroy or return non-responsive data; 5) segregation must be done by a third party or non-investigative government agent that agrees not to reveal any of the non-responding information to investigators. *See id.* at 1006.

This Court should adopt the Ninth Circuit’s requirements for federal warrants involving digital media. As discussed in the foregoing analysis, the rationale behind the plain view doctrine and its ability to place an effective limit on the scope of warrantless seizures are inapplicable in the digital media context. *See* Brief for Respondent, *supra*, at 11–20. Therefore, this Court should bar the doctrine’s application to digital media. Second, this Court should require applications for digital media warrants to explain the *actual* risks of destruction of information, as distinguished from mere generic risks inherent in any digital search. *See Comprehensive Drug Testing*, 579 F.3d at 998 (noting the actual dangers of data destruction are “highly relevant in determining whether a warrant is needed at all and, if so, what its scope should be”). In the instant case, no information appears on the record indicating why StarTests—a third party accused of no criminal wrongdoing—did not conduct the initial segregation.

Next, this Court should hold digital media warrants must include a tailored search protocol limiting searches to that information for which the government has established probable cause. *See id.* at 1000. This mandate will ensure government agents do not impinge constitutionally protected privacy more than is required. At the same time, the requirement of a

search protocol should not be construed to limit unduly searches *ex ante*, given the complexity of computer searches. In this case, the absence of a tailored search protocol unnecessarily exposed large numbers of confidential medical records to an intrusive government search. Further, this Court should require the government to return or destroy any copies of seized information that, after an initial segregation, prove to be outside the scope of the warrant. *See id.* This requirement ensures owners of the seized data that their private information will not be exposed to unwarranted searches absent additional judicial approval.

Finally, and most importantly, this Court should hold warrants for searches of digital media must provide for an initial segregation of the seized information by a third party or a non-investigative agent. *Id.* at 1006. Although intermingled documents are familiar to Fourth Amendment jurisprudence, the practical difficulties of segregating digital information without viewing the contents of large numbers of files makes the process *per se* unreasonable if conducted by a member of the investigation. Though warrants necessarily will continue to authorize the seizure of large amounts of digital evidence, segregation by a third party or non-investigative agent will avoid the danger of a vast amount of data being subjected to a general search by the government.

In the instant case, segregation by a third party or a non-investigative agent would have protected both StarTests's interests in avoiding a general search and the government's need to cast a sufficiently broad net to capture the evidence pertaining to the football players named in its investigation. *See United States v. Miranda*, 325 Fed. Appx. 858, 860 (11th Cir. 2009) (unpublished opinion) (noting that courts issuing warrants are allowed a "practical margin of flexibility, taking into account the nature of the items to be seized and the complexity of the case"). Under this requirement—assuming the warrant application indicates an actual danger of

data destruction—the agents could have initially seize all the digital storage media, avoiding any risk of lost evidence. Then, a third party would have been able to sort the data, passing on the information relevant to the search to government agents. This intermediary would prevent the government from determining for itself the extent of its search, a safeguard on which “depends much of the potency of the right of privacy.” *See Trupiano v. United States*, 334 U.S. 699, 710 (1948); *Marron v. United States*, 275 U.S. 192, 196 (1927) (“The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one things under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant,”).

Certainly segregation by a third party or a non-investigative government agent of digital media will lead to some evidence of criminal activity being either destroyed, if illegal to possess, or returned to the owner. But, as this Court has emphasized, “there is nothing new in the realization that the Constitution sometimes insulates the criminality of a few to in order to protect the privacy of us all.” *Arizona v. Hicks*, 480 U.S. 321, 329 (1987). Balancing individual constitutional interests against those of the federal government recurs throughout this Court’s jurisprudence. The axiomatic justifications for this time-honored balancing approach apply equally in the digital era as they have throughout this Court’s 200-year history.

C. *The StarTests Warrant and Seizure were Unreasonable under Existing Fourth Amendment Requirements.*

If this Court declines to require segregation by a third party or non-investigative agent in all federal warrants for digital media, the FBI’s warrant here should still be held unconstitutional under the existing Fourth Amendment reasonableness framework. The authorized seizure of “all computer records, files, and equipment related to the StarTests-administered drug tests” at the Wythe facility is impermissibly broad. *See United States v. Wong*, 334 F.3d 831, 837 (9th Cir.

2003) (indicating a warrant authorizing seizure of all files on an individual’s computer without specific restrictions would not be sufficiently specific). In light of the large number of medical records implicating professional athletes involved in this case, the issuing magistrate should have greatly restricted the scope of the search. In addition, the warrant failed to establish “objective standards by which executing officers can determine which items are subject to seizure.” *See id.* at 837 (quoting *United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986)). The warrant merely required “appropriately trained personnel” to sort the data, either on or off-site, and return the non-responsive information. *See R. 8.*

### CONCLUSION

How the judicial system structures the legal framework around digital media will have a significant impact on the lives of many Americans. *See Comprehensive Drug Testing*, 579 F.3d at 1005 (“Electronic storage and transmission of data is no longer a peculiarity or a luxury of the rich; it’s a way of life.”). As the Ninth Circuit has emphasized, a warrant for the seizure of just one company’s email servers could threaten the privacy of millions. *See id.* In addition, individuals frequently have no choice as to whether their information is stored electronically. *See id.* Still, digital storage presents substantial advantages to society despite the problems it presents the judiciary. *See id.* (highlighting the potential to backup data off-site, access information while traveling, and quickly spread information among professionals). In developing Fourth Amendment rights around digital media, this Court should acknowledge the unique challenges digital media presents to the Fourth Amendment framework and adapt its long-standing reasonableness approach to ensure the protection of private, digital media while not allowing technology to become a safe haven for criminality.

Accordingly, this Court should affirm the Fourteenth Circuit's grant of standing to Respondent CFL, forswear reliance of the plain view doctrine, and adopt the heightened particularity requirements set forth by the Ninth Circuit in *Comprehensive Drug Testing*.

---

Competition Number 16, January 11, 2009.