

IN THE

**Supreme Court of the United States**

---

UNITED STATES OF AMERICA,

*Petitioner,*

v.

STARTESTS, INC. AND THE COLONIAL FOOTBALL LEAGUE,

*Respondent.*

---

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

---

BRIEF FOR PETITIONER

---

Team Number 21

Attorneys for Petitioner

---

---

TABLE OF CONTENTS

Table of Authorities .....	iii
Questions Presented .....	viii
Opinions Below .....	1
Constitutional Provisions and Statutes Involved .....	2
Statement of the Case .....	3
Summary of Argument .....	7
Argument .....	9
I. THE CFL LACKS STANDING TO FILE A 41(g) MOTION FOR RETURN OF THE RECORDS SEIZED. ....	9
II. THE PLAIN-VIEW EXCEPTION SHOULD APPLY TO COMPUTER SEARCHES. ....	2
A. <i>The Fourteenth and Ninth Circuits Exceeded Their Supervisory Powers in Crafting the Plain-View Waiver Rule.</i> .....	14
B. <i>Forswearing Reliance on the Plain-View Exception Will Significantly Hamper Law-Enforcement’s Ability to Prosecute Crime and Will Work Substantial Social Costs.</i> .....	15
C. <i>The Plain View Waiver Rule Will Sow Confusion Because it Conflicts with Treatment of Computer Searches in the Border Search and Search Incident to Arrest Contexts.</i> .....	18
D. <i>Fourth Amendment Exceptions Should Not Be Technology Specific.</i> .....	21
III. COMPUTER-SEARCH WARRANTS DO NOT REQUIRE A HEIGHTENED PARTICULARITY REQUIREMENT. ....	23
A. <i>The Requirements Promulgated in Comprehensive Drug Testing and Adopted in StarTests Impose an Unworkable Burden on Law Enforcement.</i> .....	24
1. The heightened scrutiny required by <i>Comprehensive Drug Testing</i> eviscerates law enforcement’s ability to search electronic storage and protects criminal activity. ....	25
2. Requiring the government to disclose the actual risks of data-destruction exceeds the scope of knowledge available to the government. ....	28
B. <i>The Bright-Line Test for Heightened Particularity Stands in Direct Conflict with an Extensive Body of Binding Precedent.</i> .....	29
1. Bright-line rules are disfavored in the Fourth Amendment context. ....	29

2. The Fourth Amendment requires warrants to particularly describe only the place to be searched and items to be seized, not the precise manner in which warrants are to be executed.....	30
3. The heightened particularity requirements run afoul of Rule 41 of the Federal Rules of Criminal Procedure.....	31
4. The Fourteenth Circuit erred in adopting <i>CDT</i> 's mandatory protocols. ....	32
Conclusion.....	34

TABLE OF AUTHORITIES

**Cases**

<i>Allen v. Wright</i> , 468 U.S. 737 (1984).....	12
<i>Automobile Workers v. Brock</i> , 477 U.S. 274 (1986).....	10
<i>Bank of Nova Scotia v. United States</i> , 487 U.S. 250 (1988).....	31
<i>Coolidge v. New Hampshire</i> , 403 U.S. 443 (1971).....	14, 15, 18
<i>Dalia v. United States</i> , 441 U.S. 238 (1979).....	30
<i>Flast v. Cohen</i> , 392 U.S. 83 (1968).....	10
<i>Florida v. Bostick</i> , 501 U.S. 429 (1991).....	29
<i>Florida v. Jimeno</i> , 500 U.S. 248 (1991).....	29
<i>Florida v. Royer</i> , 460 U.S. 491 (1983).....	30
<i>Horton v. California</i> , 496 U.S. 128 (1990).....	15
<i>Hunt v. Wash. Apple Adver. Comm’n</i> , 432 U.S. 333 (1977).....	10, 11
<i>Kyllo v. United States</i> , 533 U.S. 27 (2001).....	21, 32
<i>Mainstreet Org. of Realtors v. Calumet City</i> , 505 F.3d 742 (7th Cir. 2007).....	12
<i>Marron v. United States</i> , 275 U.S. 192 (1927).....	27, 29
<i>Michigan v. Chesternut</i> , 486 U.S. 567 (1988).....	30
<i>Minnesota v. Dickerson</i> , 508 U.S. 366 (1993).....	15
<i>NAACP v. Alabama ex rel. Patterson</i> , 357 U.S. 449 (1958).....	10
<i>New York v. Belton</i> , 453 U.S. 454 (1981).....	21, 26
<i>Pennell v. City of San Jose</i> , 485 U.S. 1 (1988).....	10, 11
<i>Rakas v. Illinois</i> , 439 U.S. 128, 132 (1978).....	9
<i>Schneckloth v. Bustamonte</i> , 412 U.S. 218 (1973).....	30
<i>Stanford v. Texas</i> , 379 U.S. 476 (1965).....	30

<i>Thomas v. Arn</i> , 474 U.S. 140 (1985).....	31
<i>Thornton v. United States</i> , 541 U.S. 615 (2004).....	21
<i>Trupiano v. United States</i> , 334 U.S. 699 (1948).....	15, 18
<i>United States v. Adjani</i> , 452 F.3d 1140 (9th Cir. 2006).....	9, 16, 22, 23
<i>United States v. Alexander</i> , 574 F.3d 484 (8th Cir. 2009).....	16
<i>United States v. Arnold</i> , 533 F.3d 1003 (9th Cir. 2008).....	19, 20, 21
<i>United States v. Brookes</i> , No. CRIM 2004-0154, 2005 WL 1940124 (D. VI. June 16, 2005)....	19
<i>United States v. Cardwell</i> , 680 F.2d 75 (9th Cir. 1982).....	29
<i>United States v. Carey</i> , 172 F.3d 1268 (10th Cir. 1999).....	12, 14
<i>United States v. Chan</i> , 830 F. Supp. 531 (N.D. Cal. 1993).....	18
<i>United States v. Comprehensive Drug Testing, Inc.</i> , 579 F.3d 989 (9th Cir. 2009).....	
.....	6, 13, 14, 23–28, 31, 33
<i>United States v. Cote</i> , No. 03CR271, 2005 WL 1323343 (N.D. Ill. May 26, 2006) .....	19
<i>United States v. Curry</i> , No. 07-100-P-H, 2008 U.S. Dist. LEXIS 5438 (D. Me. Jan. 23, 2008)...	19
<i>United States v. Diaz</i> , No. CR 05-0167 WHA, 2006 WL 3193770 (N.D. Cal. Nov. 2, 2006).....	19
<i>United States v. Farlow</i> , No. CR-09-38-B-W, 2009 WL 4728690 (D. Me. Dec. 3, 2009).....	17
<i>United States v. Finley</i> , 477 F.3d 250 (5th Cir. 2007).....	19
<i>United States v. Giberson</i> , 527 F.3d 882 (9th Cir. 2008).....	13, 21–23, 28, 32, 33
<i>United States v. Grubbs</i> , 547 U.S. 90 (2006).....	29, 30
<i>United States v. Grummer</i> , No. 08cr4402-DMS (S.D. Cal.).....	17
<i>United States v. Hay</i> , 231 F.3d 630 (9th Cir. 2000).....	28
<i>United States v. Herndon</i> , 501 F.3d 683 (6th Cir. 2007).....	9, 16
<i>United States v. Hill</i> , 459 F3d 966 (9th Cir. 2006).....	29
<i>United States v. Hunter</i> , No. 96-4259, 1998 WL 887289 (4th Cir. Oct. 29, 1998).....	18

<i>United States v. Ickes</i> , 393 F.3d 501 (4th Cir. 2005).....	20
<i>United States v. Lacy</i> , 119 F.3d 742 (9th Cir. 1997).....	28
<i>United States v. Lynch</i> , 908 F. Supp. 284 (D. Vi. 1995).....	18
<i>United States v. Mann</i> , 389 F.3d 869 (9th Cir. 2004).....	29
<i>United States v. Mercado-Nova</i> , 486 F. Supp. 2d 1271 (D. Kan. 2007).....	19
<i>United States v. Meriwether</i> , 917 F.2d 955 (6th Cir. 1990).....	18
<i>United States v. Miranda</i> , 325 Fed. App’x 858 (11th Cir. 2009).....	12
<i>United States v. Murphy</i> , No. 1:06CR00062, 2006 WL 3761384 (W.D. Va. Dec. 20, 2006).....	19
<i>United States v. Ortiz</i> , 84 F.3d 977 (7th Cir. 1996).....	18
<i>United States v. Parada</i> , 289 F. Supp. 2d 1291 (D. Kan. 2003).....	19
<i>United States v. Payner</i> , 447 U.S. 727 (1980).....	14
<i>United States v. Payton</i> , 573 F.3d 859 (9th Cir. 2009).....	33
<i>United States v. Pickett</i> , No. 07-0374, 2008 WL 4330247 (E.D. La. 2008).....	20
<i>United States v. Raney</i> , 342 F.3d 551 (7th Cir. 2003).....	12
<i>United States v. Reyes</i> , 922 F. Supp. 818 (S.D.N.Y. 1996).....	18
<i>United States v. Romm</i> , 455 F.3d 990 (9th Cir. 2006).....	20
<i>United States v. Scott</i> , 334 Fed. App’x 94 (9th Cir. 2009).....	20
<i>United States v. Singh</i> , No. 07-30421, 2008 WL 4426643 (9th Cir. Sept. 29, 2008).....	20
<i>United States v. Smith</i> , 459 F.3d 1276 (11th Cir. 2006).....	9
<i>United States v. Spilotro</i> , 800 F.2d 959 (9th Cir. 1986).....	29
<i>United States v. Stroud</i> , No. 93-30445, 1994 WL 711908 (9th Cir. Dec. 21, 1994).....	18
<i>United States v. Taketa</i> , 923 F.2d 665 (9th Cir. 1991).....	9
<i>United States v. Turner</i> , 169 F.3d 84 (1st Cir. 1999).....	13, 29
<i>United States v. Valdez</i> , No. 06-CR-336, 2008 WL 360548 (E.D. Wis. Feb. 8, 2008).....	19

<i>United States v. Wilson</i> , 565 F.3d 1059 (8th Cir. 2009).....	9
<i>United States v. Wong</i> , 334 F.3d 831 (9th Cir. 2003) .....	13, 28
<i>United States v. Zamora</i> , No. 1:05 CR 250 WSD, 2006 WL 418390 (N.D. Ga. 2006).....	19
<i>United States v. Zavala</i> , 541 F.3d 562 (5th Cir. 2008).....	9, 12
<i>Veronia School Dist. 47J v. Acton</i> , 515 U.S. 646 (1995).....	15
<i>Zurcher v. Stanford Daily</i> , 436 U.S. 547 (1975).....	30

### Statutes and Rules

Fed. R. Crim. P. 41(g).....	5, 7, 12
Fed. R. Crim. P. 41(f)(1)(B).....	31

### Court Documents

Brief for the United States in Support of Rehearing En Banc by the Full Court, <i>United States v. Comprehensive Drug Testing</i> , Nos. 05-10067, 05-15006, 05-55354 (9th Cir. Nov. 23, 2009).....	14–16, 18, 24– 27, 33
---	-----------------------

### Secondary Sources

Orin S. Kerr, <i>The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution</i> , 102 MICH. L. REV. 801 (2004).....	21
David Krakoff, et. al., <i>New Protocols from the Ninth Circuit</i> , 17 BUS. CRIM. BULL. 1 (2009).....	13
Associated Press, <i>Yahoo, NFL players union settle lawsuit</i> , July 7, 2009, available <a href="http://sports.espn.go.com/nfl/news/story?id=4311049">http://sports.espn.go.com/nfl/news/story?id=4311049</a> .....	11
Colonial Football League Players’ Association—Services Provided, <a href="http://www.cflpa.com">http://www.cflpa.com</a> .....	11
Mark Maske, <i>Hearing Friday in Union Lawsuit</i> , WASH. POST, Dec. 4, 2008, available at <a href="http://views.washingtonpost.com/theleague/nflnewsfeed/2008/12/hearing-friday-in-union-lawsuit-on-suspensions.html">http://views.washingtonpost.com/theleague/nflnewsfeed/2008/12/hearing-friday-in-union-lawsuit-on-suspensions.html</a> .....	11
Verne Kopytoff, <i>Google Reveals Tool That Seeks Similar Images</i> , S.F. CHRON., Apr. 21, 2009, at C3.....	22

## QUESTIONS PRESENTED

- (1) Does a professional sports league which contracted with an independent testing corporation for drug-testing the league's players have standing to sue on behalf of the individual players under Fed. R. Crim. P. 41(g) for return of that corporation's testing records?
- (2) May the government rely on the long-established "plain view" exception to the Fourth Amendment's warrant requirement during execution of a valid warrant to search for digital evidence?
- (3) Must a heightened particularity requirement apply to warrants authorizing computer searches?

OPINIONS BELOW

The opinion of the United States District Court for the District of Wythe, denying Respondent's 41(g) motion for return of property, is unreported and appears in the record. (*See* R. 1–6.)

The opinion of the United States Court of Appeals for the Fourteenth Circuit reversing the district court decision is unreported and appears in the record. (*See* R. 7–19.)

CONSTITUTIONAL PROVISION 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.

## STATEMENT OF THE CASE

In 2003, the Colonial Football League (“CFL”) began requiring its players to submit to drug tests to ensure compliance with state and federal laws and its own athletic-performance standards. (R. 1.) The CFL hired Respondent StarTests, Inc. (“StarTests”), an independent business specializing in administering drug-testing programs for corporations, school districts, and other organizations, to administer the tests. *Id.*

To encourage players to participate in the drug testing, the CFL and StarTests informed players that the tests were strictly to determine the steroid-usage level amongst CFL players. *Id.* If five percent or more of players tested positive, the CFL would make an annual determination of whether to continue drug testing. *Id.* The CFL assured players that their names and test results would be stored at the StarTests facility and would remain confidential, with only the steroid-use percentage being reported to the public. *Id.*

In July 2008, the Federal Bureau of Investigation (“FBI”) began an investigation into the distribution and use of illegal steroids by professional athletes. (R. 1, 7.) The FBI established probable cause that five well-known players from two CFL-franchise teams were major distributors and had tested positive for steroid use, and applied for a search warrant to seize StarTests’ material regarding these five players. (R. 1.) Specifically, the FBI requested permission to seize urine samples, documents, and “all computer records, files, and equipment” related to the StarTests-administered tests. (R. 1–2.) The FBI’s supporting affidavit explained that all computer equipment and files needed to be seized for review at a later date because (1) an “on-site” search would not be possible because of the massive quantity of data sought; (2) file names could be mislabeled or deceptively hidden; and (3) viewing and decoding the data might require software not available at StarTests’ facility. (R. 2.)

The magistrate judge issued a warrant authorizing the FBI to search “computer equipment, storage devices, and—where an on-site search would be impracticable—seizure of either a copy of all data or the computer equipment itself.” *Id.* To limit the scope of the search, the warrant required “law enforcement personnel trained in searching and seizing computer data” to determine whether a computer needed to be seized. *Id.* If computers or other equipment were seized, “appropriately trained personnel” were to review the data, retaining information authorized by the warrant and designating the remainder for return. *Id.* The warrant also limited search and seizure to information “reasonably related to the investigation into the five named players’ illegal steroid use.” *Id.*

The FBI executed the warrant on November 1, 2008. *Id.* StarTests personnel indicated to FBI agents that, because the CFL was one of StarTests’ largest clients and testing had gone on for four years, most computers in the facility included at least one database regarding the CFL drug tests: One computer contained a database recording the players’ personal and health information, another contained a database listing the numbers assigned to players prior to testing, and a third computer held the actual test results, identifying subjects by identification-number only. *Id.* Many of the files were encrypted; others were hidden in H- or S-drives. *Id.*

Because of the complexity of Startests’ computer-system configuration, the search for the five players’ information would have taken a few days. *Id.* As a result, the head agent ordered all computer equipment to be seized or copied, depending on the equipment’s ease of movement. *Id.* Agents took seized documents, specimens, and digital media to the Wythe City FBI office, where computer forensics agents viewed the databases and matched test results to players. *Id.*

While searching for test results for the five named players, computer personnel came across test results of other CFL players who had tested positive for steroid use and a myriad of

other illegal substances, including cocaine, marijuana, and hallucinogens. *Id.* In light of this discovery, the FBI expanded its investigation to include all illegal drug possession and sale in professional football. *Id.* Accordingly, the FBI retained StarTests' databases, copied and inventoried the computer hard drives, then returned the unneeded equipment. *Id.*

StarTests and the CFL filed a motion pursuant to Federal Rule of Criminal Procedure 41(g) in the United States District Court for the District of Wythe seeking return of the copied discs and electronic media. (R. 2.) StarTests and the CFL claimed that all evidence other than the information related to the five players was beyond the scope of the warrant and thus illegally seized. (R. 1, 2.)

The district court denied the motion, finding the search and seizure of StarTests' computer equipment valid in all respects (R. 1, 6.) The court first held that the CFL had standing to sue for return of the seized items under Rule 41(g). (R. 3.) The court then found the warrant facially valid because it restricted the search to information related to the five players' drug-testing information and vested the decision to move computer equipment in trained personnel. (R. 4–5.) Finally, the court agreed with the federal courts of appeals that had encountered the issue, and held that the plain-view exception to the warrant requirement applied to digital-evidence seizures. (R. 6, 9.) Because the FBI was “lawfully present” on StarTests' computers when it accessed the information, the warrant granted the government a “lawful right of access” to the databases, and the criminal character of the positive results was immediately apparent, the plain-view exception permitted the search and seizure in the instant case. (R. 6.)

StarTests and the CFL appealed, arguing that the warrant failed to meet the Fourth Amendment's particularity requirement, and that the plain-view doctrine should not apply to digital evidence. (R. 7.) The United States Court of Appeals for the Fourteenth Circuit first held

that the CFL had standing to challenge the seizure. (R. 10.) On the plain-view issue, the court rejected the reasoning of the Fifth, Seventh, Tenth, and Eleventh circuits, instead following the Ninth Circuit’s decision in *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989 (9th Cir. 2009) (“*CDT*”), and requiring that the government “forswear the use of the plain view doctrine in its warrant application.” (R. 13.)

Although the Fourteenth Circuit held the seizure invalid based upon this new plain-view rule, the court continued on to address the particularity issue. Regarding the particularity requirement, the court adopted the search-warrant issuance and execution requirements created by the Ninth Circuit in *CDT*. (R. 14.) Specifically, the court required that: (1) the segregation and redaction of information from computer documents “be either done by specialized personnel or an independent third party[.]” and personnel “not communicate any information outside the scope of the warrant that they find during the segregation process without separate court approval;” (2) warrants disclose the actual risks of destruction of information and prior efforts to seize that information in other courts; (3) the government’s search protocol be designed to uncover “only the information for which it has probable cause, and only that information may be examined by the case agents;” and (4) the government “destroy or, if the recipient may lawfully possess it, return non-responsive data.” (R. 14–15.) Applying those four prongs, the court held that the warrant was overbroad, and thus the search was invalid. (R. 15.)

Judge Oneida, joined by Judge Whitney, sided with the dissenters in *CDT* and authored a vigorous dissent, arguing that the plain-view exception should not have been eliminated, and that the new particularity guidelines raise significant difficulties in practical application and ignore legitimate public policy concerns. (R. 17–20.)

This Court granted certiorari to determine whether the CFL had standing, whether the plain-view exception should apply to computer searches, and whether a heightened particularity requirement should apply to computer searches. (R. 20.)

### SUMMARY OF ARGUMENT

This Court should dismiss plaintiff, the Colonial Football League, for lack of standing, and reverse the Fourteenth Circuit's decision, because the lower court acted without authority in abolishing the plain-view exception to the warrant requirement, and it incorrectly applied a heightened standard for search-warrant particularity.

The CFL cannot establish individual or associational standing to file a Rule 41(g) motion for return of the seized records. The CFL lacks individual standing because it had no interest in the property seized, thus it cannot establish injury in fact. The League's assertion of associational standing based on its players' interests similarly fails because the CFL represents franchise-clubs and owners, not the individual players.

The plain-view exception to the warrant requirement should apply to computer searches. In requiring law-enforcement officers to "forswear reliance" on the plain-view exception, the Fourteenth and Ninth Circuits exceeded their supervisory powers and created a rule that imposes substantial social costs and significantly hampers the government's ability to prosecute crime. Further, the new waiver rule will cause confusion in the lower courts because it conflicts with treatment of computer searches in other Fourth Amendment contexts. Because technology is ever changing, exceptions to the warrant requirement should not be technology specific.

In the same vein, the particularity requirement should not be heightened for computer searches. The "guidelines" established in the Ninth Circuit and adopted in the court below have been interpreted as bright-line tests and have consequently imposed unworkable burdens on law

enforcement. In practical application, these protocols eviscerate law enforcement's ability to search computers and allow criminal activity to escape detection. Additionally, these novel requirements likely require disclosure beyond the government's knowledge.

Moreover, the bright-line test for heightened particularity stands in direct conflict with an extensive body of binding precedent. Bright-line rules have historically been disfavored in Fourth Amendment jurisprudence. The Constitution requires warrants to particularly describe only the place to be searched and persons or items to be seized, and the heightened particularity requirements contradict Rule 41 of the Federal Rules of Criminal Procedure. The Fourteenth Circuit erred in adopting *CDT*'s mandatory protocols, and must be reversed.

## ARGUMENT

The Fourteenth Circuit’s factual findings are reviewed for clear error, but its legal conclusions are reviewed de novo. *See United States v. Wilson*, 565 F.3d 1059, 1065 (8th Cir. 2009); *United States v. Zavala*, 541 F.3d 562, 568 (5th Cir. 2008); *United States v. Herndon*, 501 F.3d 683, 687 (6th Cir. 2007); *United States v. Adjani*, 452 F.3d 1140, 1143 (9th Cir. 2006); *United States v. Smith*, 459 F.3d 1276, 1290 (11th Cir. 2006).

### I. THE CFL LACKS STANDING TO FILE A 41(g) MOTION FOR RETURN OF THE RECORDS SEIZED.

The CFL lacks standing to bring a Rule 41(g) motion because (1) it lacked access, control, and ownership over the records maintained by StarTests, and (2) it may not base its interest in the property on the privacy interests of its individual players. Because the CFL has neither individual nor associational standing, its motion must be dismissed.

A Rule 41(g) motion requires that the moving party has been “aggrieved by an unlawful search and seizure of property or by the deprivation of property.” Fed. R. Crim. P. 41(g). “[A] person aggrieved by an unlawful search and seizure” is either a “victim [or] one against whom the search was directed, as distinguished from one who claims prejudice only through the use of evidence gathered as a consequence of a search or seizure directed at someone else.” *See Rakas v. Illinois*, 439 U.S. 128, 132, 134–35 (1978).

The CFL was neither a victim nor a target of the search in this case. Unlike StarTests, whose computers were seized, the CFL had no access, control, or ownership over the evidence seized. The CFL merely seeks to challenge the search of another party’s office because the evidence is potentially damaging to its business. The CFL cannot piggyback on StarTests’ interests to claim individual standing. *See United States v. Taketa*, 923 F.2d 665, 671 (9th Cir. 1991) (holding defendant lacked standing to challenge a search of another defendant’s office).

Recognizing this failure, the CFL seeks to establish associational standing based on the privacy interests of its individual players whose test results were seized. This claim similarly fails. An association has standing to sue on behalf of its members only when (a) its members would otherwise have independent standing to sue, (b) the interests it seeks to protect are germane to the organization’s purpose, and (c) neither the claim asserted nor the relief requested requires participation of individual members in the lawsuit. *Pennell v. City of San Jose*, 485 U.S. 1, 7 n.3 (1988); *Hunt v. Wash. Apple Adver. Comm’n*, 432 U.S. 333, 343 (1977). The CFL cannot satisfy *any*—let alone *all*—of the three prongs required for associational standing.

First, although associational standing—an exception to the general rule that “a litigant will . . . not be permitted to assert the rights of absent third parties,” *Flast v. Cohen*, 392 U.S. 83, 99 n.20 (1968)—permits organizations to sue on behalf of its members in limited cases, the doctrine is inapplicable to this case because the CFL’s “members” are CFL-franchise clubs and owners, not the individual players.

Associational standing found its footing in *NAACP v. Alabama ex rel. Patterson*, where the Court permitted the National Association for the Advancement of Colored People (“NAACP”) to sue for violations of its members’ First Amendment rights because the NAACP “and its members [were] in every practical sense identical.” 357 U.S. 449, 459 (1958). The doctrine was further fleshed out in *Automobile Workers v. Brock*, 477 U.S. 274, 281–88 (1986), where the Court held that a workers’ union had standing to challenge an agency’s construction of a statute which provided benefits to union workers who lost their jobs, and in *Pennell*, 485 U.S. 1, 6, 7 n.3 (1988), where the Court permitted an unincorporated home-owners’ association “organized for the purpose of representing the interests of the owners and lessors of real property in San Jose” to challenge an ordinance affecting real property in San Jose.

Unlike the associations in *Pennell* and *Brock*, which were established specifically to represent the interests of the workers and property owners affected by the challenged regulations, the CFL's "members" are CFL-franchise clubs and their owners, not the individual players. An association simply cannot sue on behalf of non-member third parties.

It is for this reason that the CFL also fails the second prong for associational standing. Like the National Football League, the National Hockey League, and other professional-sports leagues, the CFL represents the interests of its franchise clubs and owners. It is precisely because the CFL does not represent its players that the CFL Players Association exists. The players' interests are represented by their union, not their league. *See* Colonial Football League Players' Association—Services Provided, <http://www.cflpa.com> (click on "Info," then click "services"); *cf.* Mark Maske, *Hearing Friday in Union Lawsuit*, WASH. POST, Dec. 4, 2008, available at <http://views.washingtonpost.com/theleague/nflnewsfeed/2008/12/hearing-friday-in-union-lawsuit-on-suspensions.html> (reporting suit filed by NFL Players Association to overturn NFL's suspension of five players for testing positive for banned diuretic); Associated Press, *Yahoo, NFL players union settle lawsuit*, July 7, 2009, available <http://sports.espn.go.com/nfl/news/story?id=4311049> (reporting suit by NFL Players Association against Yahoo for use of players' likeness in fantasy football game).

The CFL initiated the drug testing only to ensure compliance with state and federal law and to ensure compliance with its own athletic performance standards. It set out to shield itself from liability and to identify players who are noncompliant with the CFL's performance standards—i.e., to protect its franchise clubs, not its players. The interests the CFL seeks to protect in this suit are simply not germane to the organization's purpose as required by *Hunt* and its progeny.

Finally, even if the individual players did constitute “members” with interests germane to the organization, the CFL would lack standing because the claim requires the presence of the individual players. The results of this seizure have criminal-liability implications for players, but the players are not represented by the CFL. The players’ participation is required either directly or through their union.

The immediate victims of the search and seizure in this case were StarTests and the individual players. The CFL cannot stand on these interests to bring a Rule 41(g) motion. The general prohibition against asserting the rights of third parties should apply, and the CFL’s motion should be dismissed for failure to establish standing. *See Allen v. Wright*, 468 U.S. 737, 751 (1984) (noting that “the general prohibition on a litigant’s raising another person’s legal rights” is a prudential limitation on standing); *Mainstreet Org. of Realtors v. Calumet City*, 505 F.3d 742, 744–46 (7th Cir. 2007) (holding real-estate brokers association lacked standing to challenge an ordinance on behalf of homeowners).

## II. THE PLAIN-VIEW EXCEPTION SHOULD APPLY TO COMPUTER SEARCHES.

Applicability of the plain-view exception to the warrant requirement to computer searches was an issue of first impression in the Fourteenth Circuit (R. 11), but the court was not working from a blank slate; the First, Fifth, Seventh, Tenth, and Eleventh Circuits and the district court below had each recognized that the plain-view exception may apply in digital-evidence cases, just as it has applied to physical-evidence searches for nearly forty years. *See United States v. Miranda*, 325 Fed. App’x 858, 860 (11th Cir. 2009) (per curiam) (applying plain-view exception to computer search); *United States v. Zavala*, 541 F.3d 562, 577 n.5 (5th Cir. 2008) (applying plain-view inquiry to search of cell phone); *United States v. Raney*, 342 F.3d 551, 558 (7th Cir. 2003) (applying plain-view exception to computer search); *United States v. Carey*, 172

F.3d 1268, 1276 (10th Cir. 1999) (recognizing that the plain-view exception may apply to computer searches, but holding it did not apply on the particular facts of the case); *United States v. Turner*, 169 F.3d 84, 89 (1st Cir. 1999) (refusing to apply plain-view doctrine based on scope of defendant’s consent, but making clear decision did not announce any “per se rule on computer searches”). Even the Ninth Circuit previously applied the plain-view exception to a computer search where police, executing a valid search warrant for computer evidence of a murder, stumbled upon child pornography. *United States v. Wong*, 334 F.3d 831, 838 (9th Cir. 2003); *see also United States v. Giberson*, 527 F.3d 882 (9th Cir. 2008) (upholding conviction for possession of child pornography discovered in plain-view during computer search).<sup>1</sup>

The Fourteenth Circuit, however, rejected this guidance, and followed the “renegade Ninth Circuit” (R. 17) decision in *United States v. Comprehensive Drug Testing*, 579 F.3d 989, 998 (9th Cir. 2009) (“*CDT*”)—an *en banc* decision which may soon be reconsidered by the full Ninth Circuit, *see* David Krakoff, et. al., *New Protocols from the Ninth Circuit*, 17 BUS. CRIM. BULL. 1 (Dec. 2009)—holding that the government must “forswear the use of the plain view doctrine” in its warrant applications in computer-search cases (R. 13).

This Court should reverse the Fourteenth Circuit and hold that the plain-view exception applies to computer searches for four primary reasons. First, the Fourteenth and Ninth Circuits had no legal authority to eliminate the plain-view requirement. Second, forswearing reliance on the plain-view exception will significantly hamper law enforcement’s ability to prosecute serious crimes and will work substantial social costs. Third, the plain-view waiver rule will sow confusion because it conflicts with treatment of computer searches in the context of searches at

---

<sup>11</sup> Oddly, the Ninth Circuit’s majority decision in *CDT* failed to even mention its prior decision in *Wong*. Judge Callahan, however, writing in dissent, cited *Wong* for the proposition that “there are. . . contexts where application of the plain view doctrine might be . . . appropriate.” *CDT*, 579 F.3d at 1010 n.4 (Callahan, J., dissenting).

the border and incident to arrest. Finally, exceptions to the Fourth Amendment’s warrant requirement should not be technology specific.

*A. The Fourteenth and Ninth Circuits Exceeded Their Supervisory Powers in Crafting the Plain-View Waiver Rule.*

The Fourteenth Circuit, like the Ninth Circuit in *CDT*, offered no case law which “dictate[d] or suggest[ed] that the plain view doctrine should be entirely abandoned in digital evidence cases,” *CDT*, 579 F.3d at 1013 (Callahan, J., dissenting), yet went beyond the facts of the case before it to craft a sweeping plain-view waiver rule. The prudent course would have been “to allow the contours of the plain view doctrine to develop incrementally through the normal course of fact-based case adjudication,” especially considering that computer-based technology is constantly and rapidly evolving. *Id.* (Callahan, J., dissenting); *see also United States v. Carey*, 172 F.3d 1268, 1274 (10th Cir. 1999).

The panel could not properly rely on its supervisory power to craft such a rule. This Court has made clear that a court’s supervisory power does not empower a court “to disregard the considered limitations of the law it is charged with enforcing.” *United States v. Payner*, 447 U.S. 727, 737 (1980). The Fourth Amendment—as interpreted by this Court—permits plain-view warrantless seizures. *See Coolidge v. New Hampshire*, 403 U.S. 443, 464 (1971). The Fourteenth and Ninth Circuits could not use their supervisory powers to substitute their judgment for the controlling decisions of this Court. (R. 18); Brief for the United States in Support of Rehearing En Banc by the Full Court at 9, *United States v. Comprehensive Drug Testing*, Nos. Nos. 05-10067, 05-15006, 05-55354 (9th Cir. Nov. 23, 2009) [hereinafter *CDT Brief*]. “Despite the difficulty of line-drawing and the novelty of plain view’s application to this area of law,” the court below had no legal ground to entirely eliminate it as a constitutional rule. (R. 18.)

*B. Forswearing Reliance on the Plain-View Exception Will Significantly Hamper Law-Enforcement's Ability to Prosecute Crime and Will Work Substantial Social Costs.*

“It is well established that under certain circumstances the police may seize evidence in plain view without a warrant.” *Coolidge v. New Hampshire*, 403 U.S. 443, 465 (1971); *see also Trupiano v. United States*, 334 U.S. 699, 704 (1948). This plain-view exception applies if “police are lawfully in a position from which they view an object, . . . [the object’s] incriminating character is immediately apparent, and . . . the officers have a lawful right of access to the object.” *Minnesota v. Dickerson*, 508 U.S. 366, 375 (1993); *see also Horton v. California*, 496 U.S. 128, 136–37 (1990).

The Fourth Amendment protects only legitimate expectations of privacy. *Veronia School Dist. 47J v. Acton*, 515 U.S. 646, 654 (1995). The rationale behind the plain-view exception is simple: if contraband is observed by police from a lawful vantage point, there has been no invasion of a legitimate expectation of privacy. With no additional invasion of privacy, no “search” within the meaning of the Fourth Amendment occurred beyond the authorized initial intrusion that gave officers their vantage point. *Dickerson*, 508 U.S. at 375.

While “a plain-view seizure will not turn an initially valid. . . search into a ‘general’ one, . . . the inconvenience of procuring a warrant to cover an inadvertent discovery is great.” *Coolidge*, 403 U.S. at 470. “[A]gainst the minor peril to Fourth Amendment protections [afforded by the plain view doctrine], there is a major gain in effective law enforcement.” *Id.* at 467. It would often be “a needless inconvenience,” and sometimes dangerous to the evidence or to the police themselves, to require police to ignore evidence found in the course of a lawful search until they have obtained a warrant particularly describing it. *Id.* at 467–68.

Computers are ubiquitous in contemporary life; the corollary is that they often contain significant evidence of criminal activity. CDT Brief, at 13. As the Ninth Circuit has recognized,

“[c]omputers are simultaneously file cabinets. . . and locked desk drawers; they can be repositories of innocent and deeply personal information, but also of evidence of crimes. The former must be protected, the latter discovered.” *United States v. Adjani*, 452 F.3d 1140, 1143, 1152 (9th Cir. 2006).

The Fourteenth Circuit’s plain-view-waiver rule, however, will prevent evidence of crime from ever being discovered. For example, a computer search for evidence of fraud could reveal evidence of a planned terrorist attack—evidence which could not be used for any purpose under the Fourteenth Circuit’s rule. *See* CDT Brief, at 13. The plain-view waiver could even result in the loss of highly probative evidence about the very crime under investigation. *Id.* If, for example, a warrant contained a date restriction and the resulting search revealed evidence that the crime began or continued at dates later than that which officers previously had reason to believe, the unprecedented waiver rule would not permit police to seize or use such information for any purpose. *Id.*

These situations are not merely hypothetical. In *United States v. Alexander*, a computer forensic analyst discovered child pornography while executing a valid warrant to search for digital and other evidence of illicit taping of adult females engaged in sexual acts. 574 F.3d 484, 491 (8th Cir. 2009). The analyst stopped his review and directed officers to get a second warrant based on his inadvertent discovery of child pornography. *Id.* at 487. The resulting search turned up VHS tapes and photographs of child pornography. *Id.* Under the plain-view prohibition adopted below, police would not have been able to use the pornography discovered in plain view during the initial search in seeking the second warrant.

Similarly, in *United States v. Herndon*, a probation officer came across thumbnails of child pornography while lawfully searching Herndon’s computer for evidence of internet activity

in violation of the terms of his probation. 501 F.3d 686 (6th Cir. 2007). When the detective arrived on the scene, he saw twelve images of prepubescent females on Herndon's computer screen in plain view. *Id.* at 692–93. The detective sought and received a warrant to examine the computer and its external drives based upon this information. *Id.* The resulting search revealed approximately 58,000 images and 3,000 videos of child pornography involving prepubescent children. *Id.* at 686. The Sixth Circuit applied the plain view exception and affirmed the district court's denial of Herndon's motion to suppress. *Id.* at 694. Under the Fourteenth Circuit's sweeping rule, Herndon would have gone free while possessing tens of thousands of images of child pornography.

These cases are just the tip of the iceberg. *See, e.g., United States v. Grummer*, No. 08cr4402-DMS (S.D. Cal.) (agent examining a computer pursuant to a warrant to search for evidence of environmental crimes related to sale of DDT discovered large quantities of child pornography, including a tape showing Grummer's 13-year old stepdaughter naked, which he shared with others via file-sharing software). The court in *United States v. Farlow* recently recognized this point:

In *CDT*, the ill-gotten evidence was of baseball players' use of steroids, certainly a matter of notoriety, but relatively benign in the scope of federal criminality. [In *Farlow*], the evidence in plain view . . . [wa]s child pornography, the possession of which is a serious federal felony. In a future case, the evidence in plain view could be profoundly serious, ranging from photographs of a kidnapped child to plans to commit acts of terrorism. The judicial directive to forswear in advance the plain view doctrine, placed in a different context, is equivalent to demanding that a DEA investigative team engaged in the search of a residence for drugs promise to ignore screams from a closet or a victim tied to a chair. To require the government before every computer search to forswear the plain view doctrine, which itself has its own constraints, seems unwise.

No. CR-09-38-B-W, 2009 WL 4728690, at \*6 n.3 (D. Me. Dec. 3, 2009).

In short, “compelling law enforcement to forswear the use of such evidence sacrifices the compelling societal interest in prosecuting crime without serving a countervailing privacy interest.” CDT Brief, at 13. The plain-view waiver rule simply does not “leav[e] adequate room for the necessary processes of law enforcement.” *Trupiano*, 334 U.S. at 709.

*C. The Plain View Waiver Rule Will Sow Confusion Because it Conflicts with Treatment of Computer Searches in the Border Search and Search Incident to Arrest Contexts.*

“The ‘plain view’ exception is intimately linked with the search-incident [to arrest] exception[.]”<sup>2</sup> *Coolidge*, 403 U.S. at 481–82. United States district and circuit courts have already been called on to address the applicability of the search-incident-to-arrest exception to an array of technological devices.

The district court in *United States v. Chan* denied defendant-Chan’s motion to suppress information obtained from activation of his pager’s memory found in a search incident to Chan’s arrest, concluding that all containers—including electronic containers—can be searched incident to lawful arrest. 830 F. Supp. 531, 535 (N.D. Cal. 1993). Other courts followed suit, treating pagers just like any other “container” in a Fourth Amendment search. *See, e.g., United States v. Hunter*, No. 96-4259, 1998 WL 887289, at \*4 (4th Cir. Oct. 29, 1998) (upholding retrieval of numbers from a pager incident to arrest); *United States v. Ortiz*, 84 F.3d 977, 984 (7th Cir. 1996) (same); *United States v. Stroud*, No. 93-30445, 1994 WL 711908, at \*2 (9th Cir. Dec. 21, 1994) (same); *United States v. Meriwether*, 917 F.2d 955, 958 (6th Cir. 1990) (“[T]he digital display pager, by its very nature, is nothing more than a contemporary receptacle for telephone numbers.”); *United States v. Reyes*, 922 F. Supp. 818, 833 (S.D.N.Y. 1996) (upholding retrieval of numbers from a pager); *United States v. Lynch*, 908 F. Supp. 284, 287 (D. Vi. 1995) (same).

---

<sup>2</sup> Incident to arrest, officers may search an arrestee and areas under his immediate control without suspicion, subject to minor spatial and temporal limitations. *Chimel v. California*, 395 U.S. 752 (1969); *United States v. Robinson*, 414 U.S. 218, 235 (1973).

The Fifth Circuit has taken a similar view of cell phones, finding no conceptual difference between searching physical containers for drugs and searching electronic equipment for digital information. See *United States v. Finley*, 477 F.3d 250, 259–60 (5th Cir. 2007). A handful of district courts have similarly admitted evidence seized from cell phones incident to arrest. See, e.g., *United States v. Valdez*, No. 06-CR-336, 2008 WL 360548, at \*1, \*4 (E.D. Wis. Feb. 8, 2008) (upholding search of cell phone’s address book and call logs incident to arrest); *United States v. Curry*, No. 07-100-P-H, 2008 U.S. Dist. LEXIS 5438, at \*30–31 (D. Me. Jan. 23, 2008) (upholding search of cell phone for call logs from drug informant); *United States v. Mercado-Nova*, 486 F. Supp. 2d 1271, 1279 (D. Kan. 2007) (upholding search of cell phone for numbers of outgoing and incoming calls); *United States v. Zamora*, No. 1:05 CR 250 WSD, 2006 WL 418390, at \*5 (N.D. Ga. 2006) (same); *United States v. Murphy*, No. 1:06CR00062, 2006 WL 3761384, at \*4 (W.D. Va. Dec. 20, 2006) (upholding search of cell phone’s text messages); *United States v. Diaz*, No. CR 05-0167 WHA, 2006 WL 3193770, at \*5 (N.D. Cal. Nov. 2, 2006) (upholding recording of names and numbers in address book and recording messages); *United States v. Cote*, No. 03CR271, 2005 WL 1323343, at \*6 (N.D. Ill. May 26, 2006) (upholding search of cell phone’s call log, phone book, and wireless web inbox); *United States v. Brookes*, No. CRIM 2004-0154, 2005 WL 1940124, at \*3 (D. VI. June 16, 2005) (upholding search of numbers in cell phone and pager); *United States v. Parada*, 289 F. Supp. 2d 1291, 1303–04 (D. Kan. 2003) (upholding search of stored numbers to prevent destruction of evidence).

Computers and other digital-evidence receptacles have met a similar fate in the border-search context. Even the Ninth Circuit—which crafted its unprecedented plain-view-waiver rule for computers in *CDT*—held in *United States v. Arnold* that laptops qualify as containers and

thus can be searched at the border without any suspicion at all. 533 F.3d 1003, 1007 (9th Cir. 2008). *Arnold* came on the heels of *United States v. Romm*, 455 F.3d 990, 997(9th Cir. 2006), in which the Ninth Circuit held that laptop searches were permissible at the border on less than probable cause, and *United States v. Ickes*, 393 F.3d 501, 507–08 (4th Cir. 2005), in which the Fourth Circuit upheld a border agent’s search of defendant-Ickes’ laptop as he crossed into the United States which revealed child pornography.

*Arnold* went further than both *Ickes* and *Romm* and permitted a laptop search in which a customs agent looked through Arnold’s luggage, found a laptop, turned it on, clicked on icons labeled “Kodak” and “Kodak Memories,” and read the data therein, all without any suspicion that Arnold was carrying contraband of any kind. 533 F.3d at 1005. The Ninth Circuit analogized laptop searches to searches of briefcases, luggage, wallets, purses, pictures, and the like, and rejected Arnold’s argument that a laptop search is so intrusive as to be nonroutine under the border search doctrine. *Id.* at 1008. *Arnold* has been cited favorably not only in subsequent Ninth Circuit decisions, *see, e.g., United States v. Singh*, No. 07-30421, 2008 WL 4426643 (9th Cir. Sept. 29, 2008) (holding argument that a border search officer should have a reasonable suspicion to search defendant's laptop was foreclosed by *Arnold*), but also by district courts outside the Ninth Circuit, *see, e.g., United States v. Pickett*, No. 07-0374, 2008 WL 4330247, at \*3 (E.D. La. 2008).

The Ninth Circuit even reaffirmed *Arnold* subsequent the computer-specific rule it announced in *CDT*. *See United States v. Scott*, 334 Fed. App’x 94, 95 (9th Cir. 2009) (unpublished) (affirming denial of defendant’s motion to suppress evidence of child pornography found during a border search in which officials searched his laptop and CDs).

The Ninth Circuit’s inconsistent treatment of computer searches illustrates the problems with crafting a rule specific to computers. In the border-search and search incident to arrest contexts, the court treats computers as any other container for the purposes of the Fourth Amendment. But in the plain-view and particularity contexts (discussed below), the court crafted special rules for computers based on the very reasons it declined to do so in *Arnold* without regard to reasonableness.

Such inconsistent treatment runs squarely against the recognized need for “clear rule[s], readily understood by police officers.” *Thornton v. United States*, 541 U.S. 615, 623 (2004); *see also New York v. Belton*, 453 U.S. 454, 459 (1981), *rev’d on other grounds in Arizona v. Gant*, 129 S. Ct. 1710 (2009) (recognizing that police officers must be afforded “a straightforward rule, easily applied and predictably enforced”).

*D. Fourth Amendment Exceptions Should Not Be Technology Specific.*

“Fourth Amendment exceptions and distinctions based solely on a type of technology are ‘unwise[ ] and inconsistent with the Fourth Amendment.’” *United States v. Giberson*, 527 F.3d 882, 887 (9th Cir. 2008) (quoting *Kyllo v. United States*, 533 U.S. 27, 41 (2001) (Stevens, J., dissenting)).

Technology changes. Not every change in technology necessitates changing the rules of constitutional criminal procedure to be more protective of individuals. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 858–59 (2004). “Judges cannot readily understand how the technologies may develop, cannot easily appreciate context, and often cannot even recognize whether the facts of the case before them raise privacy implications that happen to be typical or atypical.” *Id.*

Recognizing this fact and the Supreme Court’s sound disavowal of technology-specific Fourth Amendment rules, the Ninth Circuit in *Giberson* explicitly declined to craft a special rule governing computer searches. 527 F.3d at 887. The court found no persuasive reason to treat computers differently from storage mediums such as file cabinets and briefcases, concluding:

[N]either the quantity of information, nor the form in which it is stored, is legally relevant in the Fourth Amendment context. While it is true that computers can store a large amount of material, there is no reason why officers should be permitted to search a room full of filing cabinets or even a person’s library for documents listed in a warrant but should not be able to search a computer. [The] purported exception would also create problems in analyzing devices with similar storage capacities. . . . If we do not permit computers to be searched, what about a USB flash drive or other external storage device?

. . . .

[A]ttempting to limit Fourth Amendment searches based on the format of stored information would be arbitrary. We have already held that microcassettes, which store data differently from traditional paper, are seizable in a search for ‘records.’ There is no reason why material stored digitally on a computer should not also be searchable. Once again, [the] purported exception generates more questions than answers: If we permit a person’s Day-Timer to be searched, what about one’s Black-Berry? The format of a record or document should not be dispositive to a Fourth Amendment inquiry.

*Id.* at 888. The court in *Adjani* similarly declined to craft a special rule for computers based upon the potentially-massive quantity and intermingling of data on computers. *See Adjani*, 452 F.3d at 1152 n.9 (“The fear that agents searching a computer may come across . . . personal information cannot alone serve as the basis for excluding evidence of criminal acts.”). In short, “the potential intermingling of materials does not justify an exception or heightened procedural protections for computers beyond the Fourth Amendment’s reasonableness requirement.” *Giberson*, 527 F.3d at 889.

If new technology were to develop which permitted police to more narrowly tailor their searches to minimize collateral intrusions of privacy, *see, e.g.*, Verne Kopytoff, *Google Reveals Tool That Seeks Similar Images*, S.F. CHRON., Apr. 21, 2009, at C3 (noting that Google

“introduced an experimental tool Monday [April 20, 2009] that allows users to narrow their search results to photographs that are alike in terms of their content, perspective and color”), the Fourteenth Circuit’s sweeping rule would *still* prevent police from relying upon the plain view exception—they would not even be able to use the evidence discovered in plain view as a basis for a future search warrant. This makes little sense given that technology may be developed to assist law-enforcement officers in conducting narrowly-tailored computer searches.

Moreover, such a bright-line rule will create major problems in implementation it becomes increasingly difficult to discern what constitutes a “computer.” For example, iPhones and Blackberrys—unquestionably “phones”—also permit users to access the internet, store e-mails, conduct banking, and perform various other functions; does the Fourteenth Circuit’s rule apply to such devices? Police simply have no way to answer that question, leaving them with little guidance when obtaining and executing search warrants for new technological devices.

### III. COMPUTER-SEARCH WARRANTS DO NOT REQUIRE A HEIGHTENED PARTICULARITY REQUIREMENT.

The Fourteenth Circuit replaced the long-settled “reasonableness” test for search-warrant particularity with an impractical, burdensome, bright-line test adopted from a circuit with inconsistent Fourth Amendment rulings. (*See* R. 14–15); *compare United States v. Giberson*, 527 F.3d 882, 888 (9th Cir. 2008) (rejecting bright-line tests for computer searches), *with United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989, 1006 (9th Cir. 2009) (“*CDT*”) (creating five-prong bright-line test for computer searches). Both the Fourteenth and Ninth Circuits ignored binding precedent and the Federal Rules of Criminal Procedure. Accordingly, this Court should overturn the Fourteenth Circuit and reinstate the well-settled reasonableness test for Fourth Amendment particularity.

*A. The Requirements Promulgated in Comprehensive Drug Testing and Adopted in StarTests Impose an Unworkable Burden on Law Enforcement.*

The Ninth Circuit in *CDT* overreacted to “an obvious case of overreaching by the government” and created a bright-line test that mandates specific procedural burdens in warrants authorizing the search of computer-based data. *See CDT*, 579 F.3d at 1000, 1006. Specifically, the Ninth Circuit mandated that: (1) the segregation and redaction of information from computer documents “be either done by specialized personnel or an independent third party[,]” and personnel “not communicate any information outside the scope of the warrant that they find during the segregation process without separate court approval;” (2) warrants disclose the actual risks of destruction of information and prior efforts to seize that information in other courts; (3) the government’s search protocol be designed to uncover “only the information for which it has probable cause, and only that information may be examined by the case agents;” and (4) the government “destroy or, if the recipient may lawfully possess it, return non-responsive data.” *Id.* at 1006.

In the wake of *CDT*, “[m]agistrate and district court judges throughout [the Ninth] Circuit are treating the en banc panel’s ‘guidance’ as binding.” Brief for the United States in Support of Rehearing En Banc by the Full Court at 5, *United States v. Comprehensive Drug Testing*, Nos. 05-10067, 05-15006, 05-55354 (9th Cir. Nov. 23, 2009) [hereinafter *CDT Brief*]. However, disagreement persists about application of the rules. “For example, magistrate judges have disagreed about whether the . . . new requirements apply in related contexts, such as searches of cell phones and e-mail accounts.” *Id.* at 6. The uncertainty generated by *CDT* has resulted in undesirable outcomes. For example,

In the Western District of Washington . . . federal agents received information from their counterparts in San Diego that two individuals had filmed themselves raping a four-year-old girl and

traded the images via the internet. The agents did not obtain a warrant to search the suspects' computers, however, because of concerns that any evidence discovered about other potential victims could not be disclosed by the filter team. The agents therefore referred the case to state authorities, who continued the investigation using warrants obtained from state magistrate judges.

*Id.* at 6–7.

By adopting the *CDT* protocols (R. 14–15), the Fourteenth Circuit will amplify the confusion created in the Ninth Circuit. Treating these guidelines as a bright-line test is not only damaging to effective law enforcement, but also unnecessary to ensure protection of Fourth Amendment rights.

1. The heightened scrutiny required by *Comprehensive Drug Testing* eviscerates law enforcement's ability to search electronic storage and protects criminal activity.

In practice, the heightened particularity requirements bar law enforcement's ability to search electronic formats. Neither requiring specially-trained personnel to execute all computer-based searches nor barring disclosure of any information outside the warrant's scope is founded on any authority. Further, these mandates impose a costly and potentially unsustainable drain on scarce public financial and personnel resources. *CDT*, 579 F.3d at 1013 (Callahan, C.J., dissenting); *CDT* Brief, at 17. "To comply, an agency would have to expand its personnel, likely at a significant cost, to include both computer specialists who could segregate data and forensic computer specialists who could assist in the subsequent investigation . . . [or] use an independent third party consultant, which no doubt carries its own significant expense." *CDT*, 579 F.3d at 1013 (Callahan, C.J., dissenting). Indeed, past use of independent third parties has cost "into the hundreds of thousands of dollars." *CDT* Brief, at 17. Absent additional personnel, already

substantial backlogs will become even more clogged and staff will be forced to spend time documenting compliance to avoid losing future suppression motions. *Id.*

The new guidelines require that “specially trained computer personnel” or “independent expert[s] or special master[s]” determine whether data falls within the scope of the warrant; information beyond the scope of the warrant cannot be disclosed to investigators. *CDT*, 579 F.3d at 1000. But the Ninth and Fourteenth Circuits failed to define “specially trained.” It is unclear whether these persons need legal training, training in computer-search techniques, or other unforeseen expertise. Legal training may be required if they must distinguish between data within the scope of the warrant and data beyond those bounds. Lack of specificity regarding filter-team training renders the requirement too vague for uniform and predictable application. *Cf. New York v. Belton*, 453 U.S. 454, 459 (1981), *rev’d on other grounds in Arizona v. Gant*, 129 S. Ct. 1710 (2009) (recognizing that law-enforcement officers must be afforded “a straightforward rule, easily applied and predictably enforced”).

Additionally, the guidelines contain no provision for review of filter-team determinations. *Id.* If a “special master” wrongly determines that information is not within the scope of the warrant, its existence will remain undisclosed, and potentially valuable evidence will be lost. *Id.* A similar risk of evidence loss or corruption also exists if private parties retained to execute third-party searches “fail to protect against evidence contamination, network security breaches, or employee misconduct.” *CDT Brief*, at 17.

Essentially, under this requirement, the effectiveness of law enforcement depends upon the judgment of one person or a few people of uncertain training, working without review. Mitigating these risks requires “case agents [to] spend days, weeks, or even months teaching

both the underlying law and the specifics of the particular case to members of a filter team,” further straining public resources. CDT Brief, at 16.

The Ninth and Fourteenth Circuits also failed to guide magistrate judges on the conflict that might arise when an independent filter team is required for searches involving a highly secure investigation. To search effectively, the filter team will need to be given information—identities of confidential informants or classified information—that it may be legally barred from possessing. CDT Brief, at 17–18.

Although valid warrants should leave nothing in the discretion of law-enforcement personnel, *Marron v. United States*, 275 U.S. 192, 196 (1927), the “specially-trained computer personnel” required by the Ninth and Fourteenth Circuits will have unreviewable discretion—discretion which may be difficult or impossible to exercise consistently. For cases concerning straight-forward crimes such as child pornography or animal cruelty, it might be easy enough to distinguish evidence of the crime from information protected from disclosure. However, applying this requirement to more complex crimes such as insider trading, corporate fraud, or national security violations demonstrates the extensive and unreviewable discretion vested in “specially trained computer personnel.” *CDT*, 579 F.3d at 1000.

These concerns will be particularly acute in cases involving national security, because spies and terrorists often receive specialized training about concealing their tracks and because the ability to spot important information may require not only a deep knowledge of the subjects of the investigation but also access to highly classified information or possession of rare language skills.

CDT Brief, at 16.

Finally, this bright-line rule creates a zone of permissiveness for criminal activity that endangers society. No matter how obvious the photos of child pornography may be, a “special

master” searching for evidence of drug dealing is barred from disclosing the existence of a separate crime. Criminals such as Frank Giberson and Raymond Wong would sleep well under such a regime, knowing that they have an extra-Constitutional layer of protection. *See United States v. Giberson*, 527 F.3d 882 (9th Cir. 2008) (upholding conviction for possession of child pornography after it was discovered on his computer during a search for evidence of another crime); *United States v. Wong*, 334 F.3d 831 (9th Cir. 2003) (upholding conviction for possession of child pornography found on his computers while agents searched for evidence of a murder).

2. Requiring the government to disclose the actual risks of data-destruction exceeds the scope of knowledge available to the government.

The first-half of the second requirement—that search warrants disclose the actual risk of data-destruction—compels authorities to provide information that they probably cannot ascertain. Because agents assigned to the *CDT* investigation “created the false impression that, unless the data was seized at once, it would be lost,” the Ninth Circuit required the government to disclose more than just the theoretical risks of data destruction; it demanded that “the government . . . fairly disclose the *actual* degree of such risks . . .” *CDT*, 579 F.3d at 998 (italics in original).

Without intimate knowledge of the computer system in question, the software used, methods of encryption, and existing booby-traps, agents cannot possibly disclose the *actual* degree to which data is at risk of destruction. This requirement places the cart before the horse in seeking information prior to a search that can only be revealed *after* a search. The government’s ability to obtain a search warrant cannot hinge upon its production of information that it cannot possess. *See United States v. Hay*, 231 F.3d 630, 637 (9th Cir. 2000); *United States v. Lacy*, 119 F.3d 742, 746 (9th Cir. 1997).

*B. The Bright-Line Test for Heightened Particularity Stands in Direct Conflict with an Extensive Body of Binding Precedent.*

The Fourth Amendment requires that a search warrant particularly describe the place to be searched and the items sought. *U.S. Const.* amend. IV. The standard for determining the validity of search warrants is objective. *United States v. Grubbs*, 547 U.S. 90 (2006); *Marron v. United States*, 275 U.S. 192 (1927).

The Constitution requires the warrant to specify only two matters: “the place to be searched and the persons or things to be seized.” *Grubbs*, 547 U.S. at 97. The place to be searched must be described “with ‘sufficient particularity to enable law enforcement officers to locate and identify the premises with reasonable effort,’” while guarding against “any reasonable probability . . . that the officers may mistakenly search” elsewhere. *United States v. Mann*, 389 F.3d 869, 876 (9th Cir. 2004). Likewise, “[t]he description [of the items to be seized] must be specific enough to enable the person conducting the search reasonably to identify the things authorized to be seized” without sanctioning “general, exploratory searches and indiscriminate rummaging through a person’s belongings.” *Id.* at 877; *United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986). These standards are evaluated for reasonableness considering the totality of circumstances. *United States v. Hill*, 459 F.3d 966, 974 (9th Cir. 2006); *United States v. Cardwell*, 680 F.2d 75, 78 (9th Cir. 1982).

1. Bright-line rules are disfavored in the Fourth Amendment context.

“[R]easonableness is the touchstone of the Fourth Amendment.” *Florida v. Jimeno*, 500 U.S. 248, 250 (1991) (citing *Katz v. United States*, 389 U.S. 347, 360 (1967)). For nearly 40 years, this Court has favored fact-specific contextual inquiries over bright-line tests which rigidly define Fourth Amendment boundaries. *See, e.g., Florida v. Bostick*, 501 U.S. 429 (1991) (striking down *per se* rule that questioning individuals aboard a bus constitutes a seizure);

*Michigan v. Chesternut*, 486 U.S. 567, 572–73 (1988) (disavowing “bright-line rule[s] applicable to all investigatory pursuits” in favor of the Court’s “traditional contextual approach”); *Florida v. Royer*, 460 U.S. 491, 506 (1983) (rejecting “litmus-paper test” due to the “endless variations in the facts and circumstances” that concern the Fourth Amendment); *Schneckloth v. Bustamonte*, 412 U.S. 218 (1973) (rejecting *per se* rule that consent to search was invalid unless defendant knew of his right to refuse the request).

This Court in *Zurcher v. Stanford Daily* explicitly rejected a heightened particularity requirement for third-party searches. 436 U.S. 547, 554 (1975). Because “[i]t is an understatement to say that there is no direct authority in this or any other federal court for [such a] . . . sweeping revision of the Fourth Amendment,” *id.*, the Fourteenth Circuit’s decision in *StarTests* should be reversed.

2. The Fourth Amendment requires warrants to particularly describe only the place to be searched and items to be seized, not the precise manner in which warrants are to be executed.

In order to comport with the Fourth Amendment, a search warrant need only particularly describe the place to be searched and items to be seized. *Grubbs*, 547 U.S. at 97. This Court has refused to read additional specificity requirements into the particularity requirement. *See, e.g., Grubbs*, 547 U.S. at 98 (“Nothing in the language of the Constitution or in this Court’s decisions interpreting that language suggests that, in addition to the [requirements set forth in the text], search warrants also must include a specification of the precise manner in which they are to be executed.”); *Dalia v. United States*, 441 U.S. 238, 255 (1979) (rejecting requirement that agents gain explicit permission for covert entry of a suspects’ premises in order to place an electronic surveillance “bug”); *Zurcher*, 436 U.S. at 560–61 (rejecting heightened standards for third-party

searches); *Veronia School Dist. 47J v. Acton*, 515 U.S. 646, 652–53, 663 (1995) (refusing to limit searches to their least intrusive means).

This Court has made clear that warrants need only particularly describe two enumerated interests—particularity of place, and person or thing to be searched. The Ninth and Fourteenth Circuit decisions failed to regard this precedent and imposed additional requirements—requirements which should now be rejected.

### 3. The Heightened Particularity Requirements Run Afoul of Rule 41 of the Federal Rules of Criminal Procedure.

On August 26, 2009, the Ninth Circuit issued its holding in *CDT*, either unaware or in disregard of recent changes in the Federal Rules for Criminal Procedure which nullify part of its ruling. The revised version of Rule 41(f)(1)(B) (“Rule 41”), which took effect on December 1, 2009, stands in direct conflict with two mandates in *CDT*. *CDT* requires that the government state, precisely, what data it obtained from the search, and that non-responsive data either be destroyed or returned to the owner, if its possession is legal. *CDT*, 579 F.3d at 1000–01. By contrast, Rule 41 provides:

In a case involving the seizure of electronic storage media or the seizure or copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied.

Fed. R. Crim. P. 41(f)(1)(B).

Procedural rules sanctioned by this Court supersede lower court decisions. *Thomas v. Arn*, 474 U.S. 140, 148 (1985); *Bank of Nova Scotia v. United States*, 487 U.S. 250, 255 (1988). Because the requirements created by the Ninth and Fourteenth Circuits conflict with Rule 41, they must be discarded.

4. The Fourteenth Circuit erred in adopting *CDT*'s mandatory protocols.

The Ninth Circuit's Fourth Amendment jurisprudence is erratic. In *United States v. Adjani*, the court applied traditional reasonableness standards to uphold the search and seizure of a "computer belonging to . . . [co-defendant] Reinhold . . . even though she had not at that point been identified as a suspect and was not named as a target in the warrant." 452 F.3d 1140 (9th Cir. 2006). The court reasoned that, because "the level of detail necessary in a warrant is related to the particular circumstances and the nature of the evidence sought," requiring "a pin-pointed computer search, restrict[ed] to . . . an email program or to specific search terms, would likely have failed to cast a sufficiently wide net to capture the evidence sought." *Id.* at 1147, 1149–50.

Under *CDT*'s guidelines, *Adjani* would have resulted in a different outcome. First, because Reinhold was a third party, independent contractors and not government agents would have conducted her laptop search. Second, the search protocol would have been strictly limited—a circumstance that the *Adjani* court found threatening to the recovery of critical evidence. Use of the *CDT* protocols in *Adjani* would have resulted in failure to detect and successfully prosecute an extortion and conspiracy scheme.

In 2008, the Ninth Circuit in *Giberson* followed *Adjani* and applied the traditional reasonableness test and rightly rejecting heightened scrutiny for computer searches, because "exceptions and distinctions based solely on a type of technology are 'unwise [ ] and inconsistent with the Fourth Amendment.'" *Giberson*, 527 F.3d at 887–88 (quoting *Kyllo v. United States*, 533 U.S. 27, 41 (2001) (Stevens, J., dissenting)). The *Giberson* panel acknowledged that

[t]echnology changes. To be acceptable, *Giberson*'s argument must be based on a principle that is not technology-specific. Though *Giberson* offers several rationales for treating computers differently from storage mediums such as filing cabinets and briefcases, none is persuasive.

*Id.* The court found no legal relevance in either the quantity or format of information being searched. *Id.* at 888. Additionally, the *Giberson* panel anticipated the issues with which the Ninth Circuit’s magistrate judges struggle in the wake of *CDT*. “[W]hat about a USB flash drive or other external storage device. . . . If we permit a person's Day-Timer to be searched, what about one's BlackBerry?” *Id.*; see also, *CDT* Brief, at 5–6. In *Giberson*, the Ninth Circuit concluded that “the format of a record or document should not be dispositive to a Fourth Amendment inquiry.” 527 F.3d 882, 888 (9th Cir. 2008).

However, just fourteen months later, a different Ninth Circuit panel backtracked from its unequivocal language in *Giberson*. The court in *United States v. Payton* reasoned that “[t]here is no question that computers are capable of storing immense amounts of information. . . . Searches of computers therefore often involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches of other containers.” 573 F.3d 859, 862 (9th Cir. 2009). The *Payton* court held that “the search of Payton’s computer without explicit authorization in the warrant exceeded the scope of that warrant and did not meet the Fourth Amendment standard of reasonableness illustrated by *Giberson*.” *Id.* at 864.

Though the *Payton* and *Giberson* courts both applied the reasonableness standard, the *Payton* court advocated a bright-line rule requiring “officers to seek explicit judicial authorization for searches of computers.” *Id.* Because “the nature of computers makes such searches so intrusive” and “it is important to preserve the option of [magistrate judges] imposing . . . conditions . . . [on the] search of computers,” the *Payton* court held that it is not reasonable to search computers without express authorization in the warrant. *Id.*

Only one month after *Payton*, the Ninth Circuit abandoned the reasonableness standard altogether in *CDT*. See *CDT*, 579 F.3d at 1006. Perhaps recognizing this mistake, “the Ninth

Circuit on Nov. 4 [2009] issued an order inviting the parties to submit briefs addressing whether the decision of the 11-member en banc panel should be reconsidered by all of the court's 27 active judges." David Krakoff, et. al., *New Protocols from the Ninth Circuit*, 17 BUS. CRIM. BULL. 1 (Dec. 2009). Meanwhile, the Fourteenth Circuit stepped onto volatile legal ground with its substitution of *CDT*'s mandatory protocols for the settled test of reasonableness. This Court should reverse that decision.

### CONCLUSION

For the reasons stated above, this Court should dismiss the CFL for lack of standing and reverse the Fourteenth Circuit's decision. Because computers are not materially different from other containers, the United States respectfully requests that this Court sanction application of the plain-view doctrine in the computer-search context, and remind lower courts that Fourth Amendment particularity requirements are subject to an objective test considering the totality of the circumstances.

Respectfully submitted,

Team 21  
Attorneys for Petitioner

January 11, 2010