
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

—————

Team 24

Attorneys for Respondents

QUESTIONS PRESENTED

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

TABLE OF CONTENTS

Questions Presented i

Table of Authoritiesiv

Constitutional and Statutory Provisions Involvedviii

Statement of the Case..... 1

Summary of the Argument..... 3

Argument..... 4

I. CFL HAS STANDING TO BRING THIS CLAIM ON BEHALF OF ITS PLAYERS AS AN ORGANIZATION DEFENDING ITS MEMBERS..... 6

II. THE NINTH CIRCUIT’S GUIDELINES ENSURE THAT THE PARTICULARITY REQUIREMENT IS NOT SACRIFICED TO PRACTICAL CONCERNS RAISED BY COMPUTERS..... 7

 A. Requiring A Search Protocol Limits The Government’s Reach While Providing Highly Effective Law Enforcement Tools. 10

 1. Ex ante search protocols would have prevented the government’s overbroad search. 10

 2. Ex ante search protocols give the government highly effective investigative tools. 12

 3. Generic concerns over search protocols are unnecessary, and they are inapplicable to the Ninth Circuit’s holding because it does not require a specific methodology... 13

 B. The StarTests Warrant Would Not Have Been Overbroad If The Government Had Been Required To Honestly Represent Its Needs In Its Warrant Application..... 16

 C. The Government’s Conduct In The StarTests Search Shows That Overbroad Searches Are Too Likely If Third Party Segregation Is Not Required. 18

 D. The Government Must Not Be Allowed To Keep Illegally Seized Data and Equipment, Because All Other Fourth Amendment Protections Would Be Rendered Ineffective. .20

III. THE COURT SHOULD NOT PERMIT THE GOVERNMENT TO RELY ON THE PLAIN VIEW DOCTRINE TO SANCTION THE SEIZURE OF EVIDENCE AGAINST PLAYERS NOT NAMED IN THE ORIGINAL WARRANT.	22
A. The Plain View Doctrine Should Not Apply To Digital Searches Because The Costs To Fourth Amendment Protections Outweigh The Minimal Gains To Effective Law Enforcement.....	22
1. Because digital searches effectively expose the entire hard drive, every item found can be said to be in “plain view,” thus potentially turning particular warrants in digital searches into unconstitutional general warrants.....	23
2. Police cannot rely on the plain view exception because there are no exigencies that justify dispensing with the warrant requirement, and obtaining a subsequent warrant would promote the objectives of the Fourth Amendment.	25
3. Proposals to limit, but not exclude, the plain view exception in digital searches conflict with established Fourth Amendment principles and are not workable in practice.....	27
B. Even If The Plain View Doctrine Is Applicable To Digital Searches, The Elements Of Plain View Are Not Met In This Case.....	29
1. Investigators were not lawfully present in the place where the evidence could be plainly viewed because the warrant was not valid under the guidelines established in Comprehensive Drug Testing.	30
2. Investigators did not have a lawful right of access to the information because the government violated the terms of the warrant by not segregating the information authorized in the warrant from unauthorized information.....	31
3. That the incriminating character of the database was immediately apparent did not justify the expansion of the search to include evidence not authorized under the warrant.	33
Conclusion.....	34

TABLE OF AUTHORITIES

CASES

Arizona v. Hicks,
480 U.S. 321 (1987)..... 25, 33

Coolidge v. New Hampshire,
403 U.S. 443 (1971)..... 22, 23, 27

Dunkin’ Donuts Franchised Rests. LLC v. Grand Central Donuts, Inc.,
No. CV 2007-4027(ENV)(MDG), 2009 WL 1750348 (E.D.N.Y. June 19, 2009) 14

Frasier v. State,
794 N.E.2d 449 (Ind. Ct. App. 2003)..... 24

Henry v. Quicken Loans, Inc.,
No. 04-40346, 2008 WL 474127 (E.D. Mich. Feb. 15, 2008) 15

Horton v. California,
496 U.S. 128 (1990)..... 28, 29, 31, 34

Johnson v. United States,
333 U.S. 10 (1948)..... 26

Kyllo v. United States,
533 U.S. 27 (2001)..... 5

Minnesota v. Dickerson,
508 U.S. 366 (1993)..... 23, 25, 27, 33

Pannell v. City of San Jose,
485 U.S. 1 (1988)..... 7

Payton v. New York,
445 U.S. 573 (1980)..... 5

Rakas v. Illinois,
439 U.S. 128 (1978)..... 7

Rosa v. Commonwealth,
628 S.E.2d 92 (Va. Ct. App. 2006)..... 24

<i>Russo v. State</i> , 228 S.W.3d 779 (Tex. Ct. App. 2007)	26
<i>Maryland v. Garrison</i> , 480 U.S. 79 (1987).....	5
<i>State v. Hinahara</i> , 166 P.3d 1129 (N.M. Ct. App. 2007).....	24
<i>State v. Schroeder</i> , 613 N.W.2d 911 (Wis. Ct. App. 2000)	24
<i>Treppel v. Biovail Corp</i> , 249 F.R.D. 111 (S.D.N.Y. Apr. 2, 2008)	14
<i>United States v. Angelos</i> , 433 F.3d 738 (10th Cir. 2006)	33
<i>United States v. Burgess</i> , 576 F.3d 1078 (10th Cir. 2009)	passim
<i>United States v. Carey</i> , 172 F.3d 1268 (10th Cir. 1999)	5, 11, 12, 28
<i>United States v. Comprehensive Drug Testing</i> , 579 F.3d 989 (9th Cir. 2009).....	3, 6, 8, 9
<i>United States v. Garces</i> , 133 F.3d 70 (D.C. Cir. 1998).....	33
<i>United States v. Gray</i> , 78 F. Supp. 2d 524 (E.D. Va. 1999)	24, 28
<i>United States v. Hill</i> , 322 F. Supp. 2d 1081 (C.D. Cal. 2004)	25
<i>United States v. Hill</i> , 459 F.3d 966 (9th Cir. 2006).....	passim
<i>United States v. Kim</i> , No. H-09-302, 2009 WL 5185389 (S.D. Tex. Dec. 23, 2009).....	14

<i>United States v. Levato</i> , 540 F.3d 200 (3d Cir. 2007)	5, 20
<i>United States v. Osorio</i> , 66 M.J. 632 (A.F. Ct. Crim. App. 2008).....	26, 31
<i>United States v. Otero</i> , 563 F.3d 1127 (10th Cir. 2009)	8, 19, 20
<i>United States v. Potts</i> , 586 F.3d 823 (10th Cir. 2009).....	14
<i>United States v. Ross</i> , 456 U.S. 798 (1982).....	23
<i>United States v. Sutton</i> , No. 5:08-CR-40(HL), 2009 WL 481411 (M.D. Ga. Feb. 25, 2009)	14
<i>United States v. Tamura</i> , 694 F.2d 591 (9th Cir. 1982).....	passim
<i>Victor Stanley, Inc. v. Creative Pipe, Inc.</i> , 250 F.R.D. 251 (D. Md. 2008)	14
<i>Whren v. United States</i> , 517 U.S. 806 (1996).....	28

STATUTES

28 C.F.R. § 59.4 (1981)	18
-------------------------------	----

SCHOLARLY 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)	5, 17, 26
Orin S. Kerr, <i>Searches and Seizures in a Digital World</i> , 119 Harv. L. Rev. 531 (2005).....	passim
Richard P. Salgado, <i>Fourth Amendment Search and the Power of the Hash</i> , 119 Harv. L. Rev. F. 38 (2005)	12
William J. Stuntz, <i>Local Policing After the Terror</i> , 111 Yale L.J. 2137 (2002).....	28

RULES

Fed. R. Crim. P. 41(g).....20

CONSTITUTIONAL PROVISIONS

U.S. Const. amend. IV4

OPINIONS BELOW

The opinion of the U.S. Court of Appeals for the Fourteenth Circuit is unreported but appears in the record at pages 7-19. The opinion of the U.S. District Court for the District of Wythe is also unreported but appears in the record at pages 1-6.

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

The Fourth Amendment to the Constitution of the United States of America provides that “[t]he 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.

Federal Rule of Criminal Procedure 41(g) provides, in relevant part, “[a] person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property’s return.” Fed. R. Crim. P. 41(g).

STATEMENT OF THE CASE

In the past two decades, computers have emerged as the preferred repository for personal information, as well as a prominent source of evidence of crimes. *See* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531 (2005). Investigators can easily wade through the equivalent of millions of pages of text—the floor of an academic library—in the search of a digital smoking gun on a modestly sized hard drive. *Id.* at 542. Early on November 1, 2008, the FBI executed a warrant to search respondent StarTests’ computers in hopes of finding evidence of five football players using illegal steroids. R. at 1. It found hundreds of individuals’ drug test results, some evidencing illegal drug use, which StarTests’ had assured its client, respondent Colonial Football League (“CFL”), would remain strictly confidential. Since 2005, CFL had been working with StarTests, a drug testing company, to audit its efforts to curb illegal steroid use among its players. *Id.* at 8. Both CFL and StarTests administered urine and blood tests to determine what percentage of players used steroids, *id.* at 1, and both assured players that the results would remain confidential and that only the percentage of positive results would be released to CFL and the public. *Id.* Instead, the government used the results to begin a new investigation into illegal drug use. *See id.* at 16.

StarTests had taken precautions to maintain the confidentiality of CFL’s players: it stored the information for each year of testing on three different computers: one contained a database of players’ personal and health information; a second held a list matching players’ names with an assigned number; and a third held the results of the tests identifying players only by assigned number. *Id.* at 2, 8 n.3. In addition, data was encrypted or hidden on various drives. *Id.* StarTests designed this system to preserve the privacy of each tested player—even against its employees.

Magistrate Judge Leon, who issued the FBI’s warrant, also took steps to protect

StarTests' data. The FBI had established probable cause that five named football players had used illegal steroids, and its warrant affidavit asked to search "all computer records, files, and equipment" related to the drug tests. *Id.* at 8. The affidavit based this broad request on three premises: (1) an on-site search was infeasible because of the large quantity of data; (2) it was possible that file names could be mislabeled or hidden; and (3) data may need to be viewed and decoded using software not available on StarTests' computers. *Id.* at 2. But although Magistrate Judge Leon issued a warrant authorizing the search of "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," the warrant restricted the search and seizure to information "reasonably related to the investigation into the five named players' illegal steroid use." *Id.* It also required "law enforcement personnel trained in searching and seizing computer data" to decide when seizure or removal of computer equipment were necessary, and called for "appropriately trained personnel" to review any seized data, retain *only* the information authorized by the warrant—that is, information relating to the five named players' illegal steroid use—and return the remainder. *Id.*

But this is not how the search transpired. The computer forensics agent did determine that it would be impractical to complete the search on-site and decided to seize all movable computer equipment and copy the hard drives of any non-movable computers. *Id.* at 8-9. But the non-responsive data was never returned, and the weeks-long search that followed was conducted by FBI agents, not computer personnel. *Id.* at 9. This is when the FBI found the hundreds of results it had not known about and launched its new search. *Id.* at 2.

The Fourteenth Circuit found that the FBI had overstepped the warrant, and that the search was unconstitutional. *Id.* at 17. To prevent such abuses in the future, the Fourteenth

Circuit required that search warrants adopt computer search guidelines (the “Guidelines”) recently issued by the Ninth Circuit in *United States v. Comprehensive Drug Testing*, 579 F.3d 989 (9th Cir. 2009). The government appealed this decision.

SUMMARY OF THE ARGUMENT

Computer searches pose Fourth Amendment challenges that must be met by aggressive protections such as the Ninth Circuit’s Guidelines. This search exposed hundreds of CFL players’ private data, ideally situating CFL to bring this claim. CFL satisfies all of the requirements to sue on behalf of its players: (1) the players themselves could have raised the claim because they were the target of the search; (2) testing CFL’s players for steroid use and complying with its contractual duties to keep the steroid tests confidential are germane to CFL’s interests; (3) the players themselves do not need to raise the claim. Additionally, (4) CFL was StarTests’ client and it has its own privacy interest in the tests. Thus CFL can challenge the invasion of its privacy.

The invasion of CFL’s privacy shows the importance of the particularity requirement in computer searches. The Ninth Circuit proposed an effective means to preserve that requirement in *Comprehensive Drug Testing*. Ex ante search protocol requirements can prevent the government from turning a computer search into a general rummaging. Existing search tools give the government highly effective means of finding only the data for which it has probable cause. Concerns that such requirements limit the government’s ability to investigate crimes are unfounded because the Ninth Circuit only requires that the search methodology prevent investigating agents from viewing data for which they do not have probable cause. To accomplish that end, requiring the government to truthfully disclose the risks of data loss allows the issuing magistrate to tailor the warrant as narrowly as the circumstances allow but no

narrower. These are essential steps, but only a requirement that a third party segregate data for which there is not probable cause will actually place a barrier between law enforcement officers and unsearchable data. The government must be required to return illegally seized data or the Fourth Amendment will apply in name only.

Finally, the intermingling of data on StarTests' servers shows why courts should not allow investigators to rely on the plain view exception in digital searches. Because of the increasingly invasive nature of digital searches, specific warrants tend to become general warrants that allow police to riffle through hard drives. Police are often given wide latitude to open and examine every file on a computer, thus bringing its entire contents into plain view so that the exception swallows the rule. Furthermore, the two justifications for the plain view exception are weak in a digital context, since the exception provides minimal gains to law enforcement but seriously imperils the Fourth Amendment's guarantees. Alternatives that merely limit the extent of the plain view exception either conflict with established Fourth Amendment guidelines or are not workable in practice. Even if the plain view exception applies to digital searches, the government cannot establish that it had a lawful right of access to the information in this case, as it was acting outside the scope of the warrant. Further, although the incriminating character of the information was immediately apparent, this fact did not justify the FBI's expansion of the search. Therefore, the plain view exception does not apply under these facts.

ARGUMENT

The Fourth Amendment proscribes "unreasonable searches and seizures," and provides that "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. Warrants must clearly state what they seek and authorize access to only those

places for which probable cause exists. *United States v. Hill*, 459 F.3d 966, 974 (9th Cir. 2006). A warrant becomes an unconstitutional general warrant when it allows the executing authority to conduct an exploratory rummaging in search of criminal evidence. *United States v. Levato*, 540 F.3d 200, 211 (3d Cir. 2007). The primary purpose of the Fourth Amendment is to prevent such indiscriminate searches. See *Maryland v. Garrison*, 480 U.S. 79, 84 (1987) (“The manifest purpose of [the] particularity requirement was to prevent general searches.”); *Payton v. New York*, 445 U.S. 573, 583 (1980) (“[I]ndiscriminate searches and seizures . . . were the immediate evils that motivated the . . . Fourth Amendment.”).

Computer searches inherently challenge this traditional search and seizure paradigm. A computer can accurately be thought of as a filing cabinet, an accountant, a photo album, a music player, a desk, or a librarian. 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, 1155 (2007). And while the similarity between each of these things and computers is apparent, filing cabinets, desks, libraries and accountants’ offices would not each necessarily receive the same Fourth Amendment treatment. Overreliance on analogies to existing searchable items can lead courts to “oversimplify a complex area of Fourth Amendment doctrine[]” *United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999) (discussing risks of reliance on certain analogies and noting that “the file cabinet analogy may be inadequate”).

The risks of over-searching computers are also unparalleled. In the past, this Court has voiced concern about law enforcement discovering “what hour each night the lady of the house takes her . . . bath,” or “the fact that someone left a closet light on.” *Kyllo v. United States*, 533 U.S. 27, 38 (2001). This pales in comparison to what a computer can tell the government: a

given hard drive might contain personal photographs of children, financial records revealing bankruptcy, medical records revealing embarrassing conditions, and love letters or legal pornography revealing an individual's sexual preferences. Computers also store tremendous amounts of "metadata," which is generated without the user's knowledge yet is highly revealing of the user's activities. Kerr, 119 Harv. L. Rev. at 542-43. Computerized recordkeeping intermingles peoples' personal data with strangers' information without those individuals' knowledge or direction. *See Comprehensive Drug Testing*, 579 F.3d at 1005. For this reason, the risk of investigators encountering tremendous quantities of highly personal information is substantial.

Against this backdrop, the existing Fourth Amendment framework does not offer adequate protections against government overreaching. In *Comprehensive Drug Testing*, the Ninth Circuit devised a workable set of safeguards that ensure against government abuses in digital searches while not hampering effective law enforcement. *Id.* The Court should affirm the Fourteenth Circuit's adoption of the Ninth Circuit's Guidelines because they effectively reign in digital search warrants and prevent them from becoming overly broad. Furthermore, the Court should eliminate the plain view exception to prevent invasive digital searches where every file on a hard drive comes into "plain view."

I. CFL HAS STANDING TO BRING THIS CLAIM ON BEHALF OF ITS PLAYERS AS AN ORGANIZATION DEFENDING ITS MEMBERS.

CFL meets the standing requirements for an organization. An organization has standing to sue on behalf of its members when (1) its members would otherwise have standing to bring the claim, (2) the interest is germane to the organization's purpose, and (3) the claim asserted and relief requested do not require the participation of the individual members of the group. *Pannell*

v. City of San Jose, 485 U.S. 1, 7, 7 n.3 (1988). First, the individual CFL players would have standing to bring this claim. An individual has standing to raise a Fourth Amendment claim when he is the “one against whom the search was directed.” *Rakas v. Illinois*, 439 U.S. 128, 134-35 (1978). Here, the government was investigating individual players, who had a privacy interest in their own urine and blood tests, so they were the target of the search. Second, the players’ drug tests and their privacy interest in the drug tests are germane to CFL’s organizational purpose because it is in CFL’s financial and penal interest to ensure its players are not involved in illegal steroid or drug use, and therefore to perform the tests. The drug tests were conducted at CFL’s insistence. R. at 1. CFL is also contractually bound to protect the privacy of this data as it contracted with its players regarding the confidentiality of the testing, and the nature of CFL’s business relies on its relationship with its players. R. at 3. Third, the individual players do not need to be parties to an action to return the tests to StarTests, when it was CFL that commissioned the tests. *See* R. at 3. CFL also has its own privacy and possessory interest in the test results, sufficient to give it standing. R. at 10. It was CFL who initiated and paid for the tests. Its possessory interest is not diminished simply because the tests contain data about its players. Therefore, CFL has standing on its own and its players’ behalf.

II. THE NINTH CIRCUIT’S GUIDELINES ENSURE THAT THE PARTICULARITY REQUIREMENT IS NOT SACRIFICED TO PRACTICAL CONCERNS RAISED BY COMPUTERS.

The scope of computer searches is at tension with the Fourth Amendment’s particularity requirement. Often it will be obvious that a certain file is stored somewhere on a computer, but it may be impossible to know for sure where it will be, and what innocent data investigators will have to pore over to find it. *See United States v. Burgess*, 576 F.3d 1078, 1092-94 (10th Cir.

2009) (discussing difficulty of finding specific files). Still, even in the context of computers, a search warrant that essentially allows the government to search and seize “everything” is unconstitutionally overbroad. In *Hill*, the court granted a warrant to police investigating allegations of child pornography to search the defendant’s hard drive as well as all storage media belonging to the defendant’s computer or the defendant himself. 459 F.3d at 973. Although the officers had probable cause to suspect the computer contained child pornography, the court held the warrant unconstitutionally broad because the police did not explain why they needed everything they wanted to seize. *Id.* at 975-76; *see also Burgess*, 576 F.3d at 1091 (“If the warrant is read to allow a search of all computer records without description or limitation it would not meet the Fourth Amendment’s particularity requirement.”); *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) (“[A search of] ‘any and all information and/or data’ stored on a computer would be . . . the sort of wide-ranging search that fails to satisfy the particularity requirement.”). The warrant to search StarTests’ computers covered “computer equipment, storage devices . . . [and] *all data* or the computer equipment itself.” R. at 2 (emphasis added). The only thing separating it from the examples of overbroad warrants in *Burgess* and *Otero* were the data segregation restrictions, which the FBI ignored. Thus without affirmative limits on warrants, computer searches necessarily become overbroad.

The question, therefore, is not whether the Fourth Amendment protects computer searches from overbreadth but what protective steps the Fourth Amendment requires. Until recently, government investigators have benefitted from this problem. *Cf. Comprehensive Drug Testing*, 579 F.3d at 999 (“The government agents obviously were counting on the search to bring constitutionally protected data into the[ir] plain view . . .”). But the proper response to a constitutional problem is to solve it, not to profit from it, and logistical difficulties are no excuse

for overstepping the Fourth Amendment. The proper solution is to adopt the Ninth Circuit's Guidelines.

The Ninth Circuit devised the only workable solution to the Fourth Amendment challenges raised by computers when it decided *Comprehensive Drug Testing*. See 579 F.3d at 993-94. As in the present case, the government was investigating steroid use among professional athletes. *Id.* at 993. The FBI received a warrant allowing them to seek “all ‘drug testing records and specimens’ pertaining to Major League Baseball in CDT’s possession.” *Id.* (emphasis in original). Even so, the warrant included restrictions on how the data could be handled. The initial review of the data had to be performed by an agent trained in searching and seizing computer data who would determine whether the data could be searched on-site. *Id.* at 996. This agent would also determine which data fell outside the scope of the warrant and segregate that data. *Id.* Instead of following this instruction, the case agent himself viewed the data on-site and discovered test results of other players for which the government had no probable cause. *Id.* at 997. The Ninth Circuit found the search unconstitutional and announced a series of guidelines that must be followed to prevent future general searches:

- (1) In order to receive a warrant the government must propose a search methodology that will prevent investigators from accessing files for which there is no probable cause.
- (2) The government must disclose the actual risk of destruction of information and prior efforts to seize that information.
- (3) After the search, unauthorized information must be segregated or redacted by a neutral third party so that investigators only see the information for which the warrant was issued.
- (4) The government must destroy or return any data or equipment it seizes but for which it does not have probable cause.

579 F.3d at 1006.

This case shows that the Fourth Amendment can be protected by this combination of measures: (a) the requirement of an ex ante search protocol gives the government highly effective tools to find that data—and *only* that data—for which it has probable cause; (b) the government would not have been given unfettered access to StarTests’ computers if it had disclosed the actual risk of data loss; (c) the government’s search of StarTests’ computers would not have become a general rummaging if investigators followed the data segregation requirement; and (d) none of these protections will mean anything unless the government returns illegally seized equipment and data.

A. Requiring A Search Protocol Limits The Government’s Reach While Providing Highly Effective Law Enforcement Tools.

To prevent an overbroad computer search, the starting point must be a search protocol designed to discover only the information for which the government has probable cause, such as the one Magistrate Judge Leon imposed in this case. Without ex ante search protocols in place (1) there is a real risk of overbroad searches, but, when properly formulated, (2) search protocols give the government highly effective tools to find what they are looking for. Finally, (3) common concerns about the effectiveness of search techniques are unfounded, and irrelevant to the Ninth Circuit’s holding.

1. Ex ante search protocols would have prevented the government’s overbroad search.

When documents are intermingled, as they were on StarTests’ servers, ex ante search protocols are an established and necessary step to curtail government abuse. In *United States v. Tamura*, the government determined that, when executing a warrant, the volume of documents to be searched required that it seize whole file cabinets to search off-site. 694 F.2d 591, 595 (9th Cir. 1982). The Ninth Circuit held that in the future, when documents to be searched are so

intermingled with other documents that they cannot feasibly be sorted on-site, the government must seal them and seek approval for a further search. *Id.* at 595-96. Alternatively, the government may request such permission in advance, but the removal of intermingled documents must be supervised by a detached magistrate. *Id.* at 596; *see also Comprehensive Drug Testing*, 570 F.3d at 996-99 (discussing *Tamura* as applying to computer searches); *Carey*, 127 F.3d at 1275 (“Where officers come across relevant documents [on computers] so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, the officers may seal or hold the documents pending approval by a magistrate of the conditions and limitations on a further search”). These cases contemplate that the measures must be taken *before* the search so that the government knows ahead of time what its limits will be.

Notwithstanding its vocal objections, the government has not given this Court any reason to believe *ex ante* protocols are anything but necessary. The StarTests search vividly illustrates what happens when search protocols are absent or ignored. As in *Tamura*, the data on StarTests’ servers was highly intermingled: by design, the relevant files were stored on separate computers in proximity to innocent data. R. at 2 n.1. Recognizing the risks this posed, Magistrate Judge Leon added the *ex ante* requirement that the data be segregated by a third party, *id.* at 2, and in hindsight it is easy to see how this measure would have prevented exactly the abuse that occurred. In this case as in *Comprehensive Drug Testing*, the government has shown its willingness to ignore limits on its power, with the direct result of a constitutional violation. Furthermore, a common thread among computer searches that were found overbroad was either a missing or ignored *ex ante* search protocol. Thus arguments against *ex ante* protocols ignore the consistent lesson that these protocols are needed to keep the government accountable.

2. *Ex ante search protocols give the government highly effective investigative tools.*

To prevent an unconstitutional search of StarTests' computers, the government had a wide range of tools at its disposal. One common method is to search for specific file extensions.¹ Kerr, 110 Harv. L. Rev. at 544. A file's extension is particular to that type of data, so if investigators are only looking for one type of file, such as a photograph they can search for only extensions associated with that type of data, like ".jpg." *Id.* Investigators can also search for file headers, which are strings of data associated with specific file types but which do not change even if a file's extension is changed. *Id.* at 545. Limiting the warrant to just the file extensions and headers associated with database files might have prevented the government's wholesale copying of StarTests' data. Another technique is to perform a key word search, which ignores data that does not contain certain words or phrases. *See, e.g., Carey*, 172 F.3d at 1276. The government could have restricted itself to files containing the names of the steroids they were investigating and the word "positive," for instance.

Depending on what was known about StarTests' database, the government could have relied on "hashing." Hashing is a process that uses complex mathematical algorithms to generate a numerical hash value that unambiguously identifies that file. *See* Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 Harv. L. Rev. F. 38 (2005), <http://www.harvardlawreview.org/forum/issues/119/dec05/salgado.pdf> (last visited Dec. 31, 2009). There are extensive databases containing the hash values of specific computer programs and viruses, as well as known exemplars of contraband such as child pornography. *Comprehensive Drug Testing*, 579 F.3d at 999; Saldago, 119 Harv. L. Rev. F. at 40 n.14, 41. Hash searches can be automated, making a search for known hash values a hands-off method to

¹ A file extension is a one to five character suffix appended to a file's name, which instructs a computer's operating system as to what kind of file it is. *Burgess*, 576 F.3d at 1093 n.16.

effectively and efficiently pinpoint only data for which probable cause exists. *Id.* at 43. The combination of extension and header, key word, and hash searches, makes it possible to significantly limit the government's exposure to data it does not have a right to see, and the inclusion of a search protocol merely ensures that the government remains honest in adhering to those techniques.

3. *Generic concerns over search protocols are unnecessary, and they are inapplicable to the Ninth Circuit's holding because it does not require a specific methodology.*

Concerns over requiring ex ante search protocols are unjustified. Many courts are hesitant to require search protocols when issuing warrants because they are afraid of interfering with law enforcement's effectiveness. In the present case, Judge Oneida worried that investigators cannot decide which search methods are most effective "until a computer technician sits down before the computer screen and analyzes the system." R. at 18; *see also Comprehensive Drug Testing*, 579 F.3d at 1013 ("[T]he majority's new guidelines are troubling because they are overbroad and restrict how law enforcement personnel can carry out their work") (Callahan, J., concurring in part and dissenting in part); *id.* at 1019 ("[T]he majority's guidelines raise substantial practical problems") (Bea, J., concurring in part and dissenting in part); *Burgess*, 576 F.3d at 1094 ("[I]t is folly for a search warrant to attempt to structure the mechanics of the search and a warrant imposing such limits would unduly restrict legitimate search objectives."); Kerr, 119 Harv. L. Rev. at 575 ("[I]dentifying the best technique usually must wait until the search occurs.").

This anxiety is unfounded, however. The courts in *Hill* and *Burgess* failed to consider hash searching, which is more effective than the techniques they rejected. Further, in *Burgess*, the court later implies limits to its own broad claims, noting "there *may* be no practical substitute

for actually looking in many (perhaps all) folders and *sometimes* at the documents contained within those folders” 576 F.3d at 1095 (emphasis added). Some concern over search protocols is based on a misunderstanding of available technology. In *Hill* the court thought “[t]here is no way to know what is in a file without examining its contents.” 459 F.3d at 978. This is either false or irrelevant, however, because hash values identify precisely what is in a file without showing it to a human, and if that counts as “examining” a file’s contents, then clearly a file can be examined without investigators seeing what it contains, making it a moot point that the file must be “examined.”

The best indication that search protocols will not harm the administration of justice is that they have not done so yet. *See, e.g., United States v. Potts*, 586 F.3d 823, 834 (10th Cir. 2009) (upholding warrant which included ex ante search protocol); *United States v. Kim*, No. H-09-302, 2009 WL 5185389, at *14 (S.D. Tex. Dec. 23, 2009) (invalidating warrant for failure to follow Ninth Circuit’s *Comprehensive Drug Testing* requirements even though not bound by Ninth Circuit); *United States v. Sutton*, No. 5:08-CR-40(HL), 2009 WL 481411, at *3 (M.D. Ga. Feb. 25, 2009) (upholding warrant requiring third party data segregation). Computer search protocols are considered an effective and indispensable component of civil discovery, where they are used to limit exposure to privileged documents. *See Victor Stanley, Inc. v. Creative Pipe, Inc.*, 250 F.R.D. 251, 256-58 (D. Md. 2008) (describing effective search protocol techniques for privilege search); *see also Dunkin’ Donuts Franchised Rests. LLC v. Grand Central Donuts, Inc.*, No. CV 2007-4027(ENV)(MDG), 2009 WL 1750348 (E.D.N.Y. June 19, 2009) (ordering parties to devise search protocol); *Treppel v. Biovail Corp*, 249 F.R.D. 111, 120 (S.D.N.Y. Apr. 2, 2008) (criticizing failure to devise effective search protocol); *Henry v. Quicken Loans, Inc.*, No. 04-40346, 2008 WL 474127, at *1-*2 (E.D. Mich. Feb. 15, 2008) (describing parties’ search

methodology). Thus far, search protocols have not brought the wheels of justice to a halt but kept them turning smoothly.

All the government's exhortations really prove is that not every search technique is appropriate in every instance. But as will be elaborated below, the Ninth Circuit solved this problem by requiring the government to accurately describe what difficulties it will encounter in the search. Moreover, the techniques found in proposed methodologies were all originally designed to make law enforcement's task easier by helping them find files without wading through irrelevant data. Techniques do not become any less effective because they happen to serve the dual purpose of limiting the government's reach. Alarm over *ex ante* search protocols is based on conjectural problems that have not transpired in practice.

Generic worries about specific search techniques do not apply to the Guidelines, because they do not require a specific search methodology, just that a methodology exist. The Ninth Circuit merely said that the search protocol must prevent *case agents* from seeing information to which they are not entitled, but which they have repeatedly shown they will try to access anyway. 579 F.3d at 1000 (requiring "a protocol for *preventing agents* . . . from examining or retaining any data other than that for which probable cause is shown") (emphasis added). This requirement is easy to satisfy even in the hypothetical case where the only effective method involves a human search of files. *See id.* ("The procedure might . . . [require] that the segregation be done by specially trained computer personnel who are not involved in the investigation."). Even if identifying the best search technique "must wait until the search occurs," Kerr, 119 Harv. L. Rev. at 575, a search protocol that "prevents agents . . . from examining or retaining any data other than that for which probable cause is shown" might simply involve letting someone *else* manually search every file without "disclos[ing] . . . any information other than that which is the

target of the warrant,” *id.* at 1007. Thus *Comprehensive Drug Testing* fully contemplates a search protocol in which not so much as a single hash value is specified in advance, if the circumstances actually dictate such a result.

B. The StarTests Warrant Would Not Have Been Overbroad If The Government Had Been Required To Honestly Represent Its Needs In Its Warrant Application.

A magistrate judge cannot issue a warrant with the specificity required by the Fourth Amendment unless the government is honest about the likelihood of data being hidden or destroyed. Certainly, computers allow criminals to effectively conceal data, and dire accounts of these risks often make their way into warrant affidavits and court opinions. *See, e.g., Comprehensive Drug Testing*, 579 F.3d at 995 (noting that the warrant affidavit claimed “data might be erased or hidden; there might be booby traps that ‘destroy or alter data . . . ’ ”); *Burgess*, 576 F.3d at 1094 n.18 (recounting “computer files . . . describ[ing] pay-owe sheets as ‘auto repair bills,’ marijuana as ‘green paint,’ and cocaine as ‘white paint’ ”); *Hill*, 459 F.3d at 978 (noting “[t]he ease with which child pornography images can be disguised—whether by renaming sexyteenyboppersxxx.jpg as sundayschoollesson.doc, or something more sophisticated . . . ”). But these are worst-case scenarios which often bear no resemblance to the facts of a specific search.

None of these risks were present on StarTests’ servers, and the government did not need the broad latitude it sought. As noted in *Burgess*,

As the description of . . . places and things becomes more general, the method by which the search is executed becomes more important—the search method *must be tailored to meet allowed ends*. And those limits must be functional. For instance, unless specifically authorized by the warrant there would be little reason for officers searching for evidence of drug trafficking to look at tax returns

576 F.3d at 1094 (emphasis added); *see also id.* at 1093 (“[O]fficers must be clear as to what it is they are seeking on the computer and conduct the search in a way that avoids searching files of types not identified in the warrant.”) (quoting *United States v. Walser*, 275 F.3d 981, 986 (10th Cir. 2001)). Thus there is no Fourth Amendment justification for granting investigators broader leeway than necessary when they are searching for discrete files that are not likely to be hidden or destroyed, like the databases on StarTests’ servers. But it is impossible for a magistrate judge to know the difference and to tailor the warrant to meet the allowed ends unless the government is required to “fairly disclose the *actual* degree of such risks.” *Comprehensive Drug Testing*, 579 F.3d at 998 (emphasis in original); *see also Hill*, 459 F.3d at 975 (“[T]he government must still demonstrate to the magistrate *factually* why such a broad search and seizure authority is reasonable in the case at hand.”) (emphasis in original).

The Ninth Circuit’s requirement would have prevented the government’s unfettered search of StarTests’ servers. The government obtained its broad warrant in part by citing concerns about data concealment. But unlike drug dealers and child pornographers, StarTests is a legitimate business that was not engaged in any illegal activity. StarTests possessed incriminating data because it was paid to perform drug tests, not because it was complicit in any criminality. It concealed data on its servers only to protect its clients’ anonymity and there is nothing to suggest StarTests would have obstructed justice out of a mere commercial duty to its clients. *See generally* Regensburger, 97 J. Crim. L. & Criminology at 1165-72 (discussing substantial differences between searching business’ records and searching criminal suspects’ computers). The government also knew or should have known in advance that the entirety of the information it sought was contained in a handful of discrete files which, for privacy reasons, were not duplicated. Assuming a business has an interest in being able to find its own records, a

StarTests employee could have easily located the three files and given only those files to the government,² at which point the government would be entirely certain its search was complete. Instead, it sought permission to search “ ‘all computer records, files, and equipment’ related to the StarTests-administered tests” R. at 8. The gulf between the warrant the government asked for and the warrant the government needed³ was immense, but the issuing magistrate had no way of knowing this because the government dishonestly represented its needs. Likewise, in *Comprehensive Drug Testing*, the warrant emphasized only theoretical risks of data loss and neglected to mention that CDT had agreed to keep its data intact. 579 F.3d at 998. The court held that omitting “highly relevant information altogether is inconsistent with the government’s duty of candor . . . [and] shall bear heavily against the government” *Id.* In this case, the government received an unconstitutionally broad warrant by omitting the fact that the generic risks associated with criminals’ computers did not apply to the servers of a law abiding company. The Ninth Circuit’s honesty requirement is needed to make sure the government does abuse courts’ trust.

C. The Government’s Conduct In The StarTests Search Shows That Overbroad Searches Are Too Likely If Third Party Segregation Is Not Required.

The Fourth Amendment cannot protect computer searches unless investigators are prevented from seeing information for which they do not have probable cause. Once investigators come across data for which there is no probable cause, a constitutional violation has already occurred. Although all of the Ninth Circuit’s guidelines are needed to prevent

² Or, depending on how the database was saved, an even more restrictive measure could be possible. *Comprehensive Drug Testing* details how investigators could have copied and pasted only the specific database entries they sought into a new Microsoft Excel spreadsheet, limiting their view only to a particular portion of a particular document. *See* 579 F.3d at 1016 (Bea, J., concurring in part and dissenting in part). If StarTests’ databases were similar, then the narrowest possible search is even further removed from the one the government executed.

³ If it needed a warrant at all. Under Department of Justice guidelines, “[a] search warrant should not be used to obtain documentary materials . . . [from a] disinterested third party unless it appears that the use of . . . other less intrusive . . . means . . . would *substantially jeopardize* . . . [the search].” 28 C.F.R. § 59.4 (1981) (emphasis added).

indiscriminate, general searches, only the third party segregation requirement actually places a barrier between investigators and the data they are not allowed to see. Such a barrier is needed before it is too late. In *Otero*, a warrant did not restrict the government to searching files created within the dates as to which probable cause existed. 563 F.3d at 1130. Without such limitations, investigators viewed every file the computer search turned up, including false hits. *Id.* As a result the court found the warrant was unconstitutionally overbroad. *Id.* at 1133. In *Hill*, a warrant was overbroad when it exposed investigators to all computer storage media without any indication that a blanket search was necessary. 459 F.3d at 977-78. In *Carey*, a search was invalidated because the warrant allowed officers to open files to determine if they were relevant, and in doing so they found documents for which they did not have probable cause. 172 F.3d at 1273. In the present case, FBI agents violated the Fourth Amendment when they searched StarTests' computers, without performing third party segregation required by the warrant. None of these violations could have occurred if limits were placed on what the investigators could see.

The appropriate affirmative limit to what investigators see is neutral third party data segregation. This is a proven solution. In *Tamura*, the court held that, if the government must over-seize, then “[t]he essential safeguard required is that wholesale removal must be monitored by the judgment of a neutral, detached magistrate.” 694 F.2d at 596. Courts have had no trouble extending this requirement to computer searches. The magistrate judge in *Comprehensive Drug Testing* required the initial search and segregation of CDT's computers be conducted by specially trained computer personnel, not the case agent. 579 F.3d at 995. The Fourth Amendment problem in that case is not that this restriction was *imposed* but that it was *ignored*. In the present case, Magistrate Judge Leon also included a third party segregation requirement in light of the risk of the government stumbling across innocent data. Thus, dating back to *Tamura*,

the notion of third party segregation is the accepted approach to searching intermingled data, and it is easily imported to the computer context.

The fundamental protection of the particularity requirement is to prevent investigators from conducting an exploratory rummaging. *E.g.*, *Otero*, 563 F.3d at 1131-32; *Levato*, 540 F.3d at 211. Seizure of records not described in a warrant for later examination is “the kind of investigatory dragnet that the [F]ourth [A]mendment was designed to prevent.” *Tamura*, 694 F.2d at 595 (quoting *United States v. Abrams*, 615 F.2d 541, 543 (1st Cir. 1980)). Thus the core concern of the Fourth Amendment reduces to preventing officers from seeing documents unless there is probable cause.

D. The Government Must Not Be Allowed To Keep Illegally Seized Data and Equipment, Because All Other Fourth Amendment Protections Would Be Rendered Ineffective.

Returning seized data for which there is no probable cause prevents the government from profiting from an illegal search as it is attempting to do now. This requirement is a natural concomitant both of the particularity requirement’s restriction on what the government can see, and on Federal Rule of Criminal Procedure 41(g) which allows a party to move for the return of improperly seized property. Fed. R. Crim. P. 41(g). Although Rule 41(g) allows for the return of improperly seized data, it does not go far enough in the context of computer searches. Even if a Rule 41(g) motion is granted, the government may still use illegally seized information as evidence. *See Comprehensive Drug Testing*, 579 F.3d at 1023 (Bea, J., concurring in part and dissenting in part). In this case, the government’s reward for ignoring the terms of its warrant is that it is able to launch a new investigation sparked purely by its illegal search. R. at 16. In the process, it is interfering with the legitimate operation of StarTests’ business. *Id.*; *see also Comprehensive Drug Testing*, 579 F.3d at 1002 (noting that seizure of CDT’s data “interferes

with the operation of its business”). The constitutionally required protections announced by the Ninth Circuit will be reduced to a nullity if the government is allowed to use StarTests’ data and equipment as if legally obtained.

In his dissent in *Comprehensive Drug Testing*, Judge Bea objected to the Ninth Circuit’s requirement that the government return CDT’s equipment, because a Rule 41(g) motion cannot exceed the scope of the exclusionary rule. *Id.* at 1021 (Bea, J., concurring in part and dissenting in part). But if investigators follow the Guidelines, and execute the warrant in good faith, the only way they will find data beyond what they are searching for is through plain view. For reasons that will be elaborated below, that exception can no longer apply to computer searches. Thus no Fourth Amendment exception would protect the discovery of additional data, and the Ninth Circuit’s rule would not extend past the exclusionary rule.

Additionally, the usefulness of some illegally seized data in a criminal investigation does not justify retaining StarTests’ computer equipment which contains no useful evidence. The government cannot possibly have use for StarTests’ physical equipment and the legitimate business records it keeps. If the government is not forced to return this equipment, the Fourth Amendment will amount to nothing more than a “best practice” without any consequences.

The government’s illegal search of StarTests’ computers occurred when it disregarded instructions designed to protect StarTests’ and CFL’s rights. This callous abuse shows that the only way to ensure the Fourth Amendment is not vitiated in the digital world is to impose the Ninth Circuit’s four-part search guidelines on any computer search. These guidelines leave law enforcement with highly effective resources to investigate crime while ensuring that the government is kept honest and the Fourth Amendment is taken seriously.

III. THE COURT SHOULD NOT PERMIT THE GOVERNMENT TO RELY ON THE PLAIN VIEW DOCTRINE TO SANCTION THE SEIZURE OF EVIDENCE AGAINST PLAYERS NOT NAMED IN THE ORIGINAL WARRANT.

The “distinct objective” of the warrant requirement is that “those searches deemed necessary should be as limited as possible.” *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). The plain view exception, as applied to physical searches, is “consistent” with this objective because it “does not convert the search into a general or exploratory one.” *Id.* In the context of digital searches, however, this is simply no longer true.

Computer searches are increasingly invasive, and police are often given wide latitude in determining the scope of a search—more so than would be tolerated in physical searches. This Court should prevent potentially limitless and virtually unrestricted access to confidential and often personal information stored on computers by excluding digital searches from the scope of the plain view exception. To hold otherwise would threaten individual privacy and undo the constitutional protections to keep one’s effects personal.

A. The Plain View Doctrine Should Not Apply To Digital Searches Because The Costs To Fourth Amendment Protections Outweigh The Minimal Gains To Effective Law Enforcement.

The unique nature of digital searches precludes application of the plain view doctrine to digital searches for two reasons: (1) use of the plain view exception creates a danger that specific warrants will become general warrants because every file on a hard drive could be said to be in “plain view”; and (2) the two justifications for the plain view exception are weak in a digital search context, such that minimal gains to law enforcement do not justify the costs to Fourth Amendment protections.

1. *Because digital searches effectively expose the entire hard drive, every item found can be said to be in “plain view,” thus potentially turning particular warrants in digital searches into unconstitutional general warrants.*

In the digital search context, plain view exception swallows the Fourth Amendment rule against warrantless searches, as it is more convenient for the government to conduct invasive and expansive computer searches. In *Minnesota v. Dickerson*, this Court warned against “the danger . . . that officers will enlarge a specific authorization, furnished by a warrant or an exigency, into the equivalent of a general warrant to rummage and seize at will.” 508 U.S. 366, 378 (1993). Because of this concern, the plain view doctrine “may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges.” *Coolidge*, 403 U.S. at 466. Nevertheless, digital searches “tend to be unusually invasive” in ways that physical searches are not. Kerr, 119 Harv. L. Rev. at 569. Invasive searches are becoming the norm in the digital context for two reasons. First, computers lower the cost and inconvenience to the government of invasive searches. *Id.* at 569-70. Second, current limitations on searches are tailored to the realities of physical searches. These limitations become ineffective in a digital context, and police are often given virtually unlimited authority to rummage through hard drives. As a result, every file on a hard drive could be said to be in plain view.

Fourth Amendment jurisprudence limits physical searches by restricting the search to “places in which there is probable cause to believe that [the evidence] may be found.” *United States v. Ross*, 456 U.S. 798, 824 (1982). For example, police may not search for undocumented aliens in a suitcase. *Id.* As discussed above, this limitation does not translate well to digital searches, however. In theory, this rule could be modified so that police would be limited to searching for the *type* of file in which evidence is expected to be found. Police accurately note, however, that criminals can disguise image files by changing the file extension or file name;

police then use this concern to argue that investigators must open a file to know its contents. *See Frasier v. State*, 794 N.E.2d 449, 466 (Ind. Ct. App. 2003) (noting that, because files can be mislabeled, files “must necessarily be ‘opened’ in some way to ascertain [their] contents”). This argument, when taken to its natural conclusion, gives police an enormous right of access to individuals’ information and results in highly invasive searches. In fact, several cases have gone so far as to hold that investigators may meticulously open and inspect every file on a suspect’s hard drive. *See, e.g., United States v. Gray*, 78 F. Supp. 2d 524, 528 (E.D. Va. 1999) (holding that “[i]n searching for the items listed in the warrant, [the officer] was entitled to examine all of defendant’s files”); *State v. Hinahara*, 166 P.3d 1129, 1135 (N.M. Ct. App. 2007) (holding that the search pursuant to warrant did not violate the Fourth Amendment where police opened every file on a suspect’s hard drive); *Rosa v. Commonwealth*, 628 S.E.2d 92, 102 (Va. Ct. App. 2006) (noting that the officer was “entitled to examine all of appellant’s files to determine whether they contained items that fell within the scope” of the warrant); *State v. Schroeder*, 613 N.W.2d 911, 917 (Wis. Ct. App. 2000) (noting that in digital searches “investigators necessarily must look at all files”).

Such unfettered police access to the equivalent of millions of pages of private information would have been unthinkable in years past. In *Tamura*, for example, the seizure of 11 boxes of papers, 34 file drawers of vouchers, and 17 drawers of cancelled checks was considered a broad seizure. *Comprehensive Drug Testing*, 579 F.3d at 1004 (calling seizure “broad”); *Tamura*, 694 F.2d at 595 (listing contents of seizure). Today, the seizure in *Tamura* does not hold a candle to the expansiveness of the search and seizure of the average hard drive. When police have the authority to open every file on a hard drive, and when every opened file comes into plain view as a result, what information on a hard drive is not in plain view? It hardly

seems fitting to call this wide net the plain view “exception” when, in fact, individuals’ privacy is no better protected than it was under the general warrants of centuries past. The plain view doctrine must not be permitted to effectively eliminate all existing Fourth Amendment privacy protections.

Investigators, left to their own devices, hold the potential to uncover virtually unlimited personal information through digital searches, creating an unprecedented opportunity for overreaching. Therefore, because digital searches are unusually invasive, and because every file on a hard drive could be said to be in “plain view,” this Court should disallow reliance on the plain view exception in digital searches.

2. Police cannot rely on the plain view exception because there are no exigencies that justify dispensing with the warrant requirement, and obtaining a subsequent warrant would promote the objectives of the Fourth Amendment.

This Court has provided two justifications for the use of the plain view exception to the warrant requirement: first, abandoning a search to seek a warrant may be impractical and inconvenient or may pose a risk to the officer or to the preservation of the evidence; second, seeking a warrant for the seizure of an object in plain view would do little to promote the objectives of the Fourth Amendment. *Dickerson*, 508 U.S. at 375; *Arizona v. Hicks*, 480 U.S. 321, 327 (1987). In the context of digital searches, neither of these justifications applies.

Practical concerns such as police safety, preservation of evidence, time constraints, and convenience support the role of the plain view doctrine in mitigating exigent circumstances in physical searches. The nature of digital searches, however, significantly reduces or eliminates these concerns. First, investigators often seize a suspect’s hard drive before beginning a search because an on-site search proves to be impractical. *See United States v. Hill*, 322 F. Supp. 2d 1081, 1088-89 (C.D. Cal. 2004). Once police seize the hard drive and analyze it in a secure

location, only minimal concerns for police safety or preservation of evidence remain. Police often make an identical copy of the hard drive, which further reduces the preservation concern. *See Russo v. State*, 228 S.W.3d 779, 800 (Tex. Ct. App. 2007) (noting that making an identical copy of a hard drive prior to a search is “protocol for forensic computer examination”). In addition, there are significantly fewer time constraints in digital searches. For example, week-long physical searches would be considered an impermissible invasion of privacy. Yet, as in this case, investigators typically spend weeks searching hard drives and analyzing data. *See United States v. Osorio*, 66 M.J. 632, 634 (A.F. Ct. Crim. App. 2008) (noting that investigators did not begin to prepare the suspect’s hard drive for analysis until eleven days after it was seized); *see also* Kerr, 119 Harv. L. Rev. at 537-38 (noting police may begin a search weeks or months after seizing a hard drive, and the search could take weeks to complete). Because investigators have ample time to conduct a search, they can also spare the time to seek a second warrant. Furthermore, in digital searches, “the additional step of applying for a second warrant to seize new evidence creates a minimal burden.” Regensburger, 97 J. Crim. L. & Criminology at 1207. For these reasons, there are no exigencies which would make it impossible or impractical for police to pause a search and seek a second warrant.

Second, seeking a second warrant would do much to promote the objectives of the Fourth Amendment. Because it is increasingly more convenient for police to conduct invasive digital searches, requiring that police seek a second warrant would place a much needed check on police overreaching. As an acknowledgement that police have an incentive to cut corners, the protection provided by the Fourth Amendment “consists in requiring that [evidentiary] inferences be drawn by a neutral and detached magistrate” and not “zealous officers” who are “engaged in the often competitive enterprise of ferreting out crime.” *Johnson v. United States*, 333 U.S. 10, 14 (1948).

As this Court has recognized, police “simply cannot be asked to maintain the requisite neutrality with regard to their own investigations.” *Coolidge*, 403 U.S. at 451. This is, perhaps, even more true when the plain view doctrine has been applied to give police essentially unlimited access to every file on a suspect’s hard drive. Judge Kozinski has noted the danger that “everything the government chooses to seize will . . . automatically come into plain view” and that this unrestrained access will “create a powerful incentive for them to seize more rather than less” *Comprehensive Drug Testing*, 579 F.3d at 998. This is not merely an abstract possibility. In *Comprehensive Drug Testing*, the FBI admitted that the “idea behind” seizing one of the computer directories was to “later briefly peruse it to see if there was anything *above and beyond that which was authorized for seizure in the initial warrant.*” *Id.* at 1011 n.5 (emphasis added). Whereas in a physical search the requirement that police obtain a warrant before seizing contraband in plain view would be a meaningless exercise, here it would ensure that police do not abuse their unfettered access to a suspect’s hard drive and that a specific warrant does not become “the equivalent of a general warrant to rummage and seize at will.” *Dickerson*, 508 U.S. at 378.

Therefore, because the gains to law enforcement in dispensing with the warrant requirement are slight, and because requiring an additional warrant would greatly advance the objectives of the Fourth Amendment, the application of the plain view doctrine to digital searches is unjustified.

3. Proposals to limit, but not exclude, the plain view exception in digital searches conflict with established Fourth Amendment principles and are not workable in practice.

There are two alternative means of limiting the application of the “plain view” doctrine. *See Kerr*, 119 Harv. L. Rev. at 577-82. The first is to focus on the subjective intent of officers

conducting the search. *See, e.g., Carey*, 172 F.3d 1268. The second is to focus on future uses of the evidence obtained, such as distinguishing between the use of the evidence in terrorism cases and other less compelling cases. *See William J. Stuntz, Local Policing After the Terror*, 111 Yale L.J. 2137, 2184 (2002). Neither of these options, however, presents acceptable alternatives.

This Court has rejected a focus on the subjective intent of the officers when determining the constitutionality of a search or seizure under the plain view doctrine, *Horton v. California*, 496 U.S. 128, 137 (1990), and has explicitly stated that “[s]ubjective intentions play no role in ordinary, probable-cause Fourth Amendment analysis,” *Whren v. United States*, 517 U.S. 806, 813 (1996). Even so, several recent cases have focused on intent. In *Carey*, the Tenth Circuit adopted an “inadvertence” requirement in digital searches and held that an officer’s decision to pause the original search and begin a warrantless search for child pornography turned the search into a general search that exceeded the scope of the warrant. 172 F.3d at 1276. Similarly, *Gray* focused on the subjective intent of the officer but held that inadvertently discovered evidence could be admitted because the officer did not divert the original search to begin looking for evidence not authorized by the warrant. 78 F. Supp. 2d at 529. An officer’s intent may be impossible to discern, however, and it would unnecessarily hamper law enforcement to strike down an officer’s objectively reasonable actions on the basis of his or her less discernible intent. In addition, computer analysts often conduct searches according to an established policy. Kerr, 119 Harv. L. Rev. at 578. An analyst’s ability to claim that he was following procedure in continuing a search can mask his intent further.

Likewise, a focus on the future uses of evidence is problematic because there must be some agreement on what constitutes a “compelling” case. Some would draw the line at terrorism and child pornography cases; others would include homicide or large-scale computer hacking.

Even if there were some agreement, this is a policy decision better left to Congress. Congress, however, has an incentive to “expand the list of eligible offenses over time, watering down the protection,” as it has done with federal wiretapping authorizations. *Id.* at 581. For that reason this approach is ill-advised.

Because these options conflict with Fourth Amendment jurisprudence or are unworkable in practice, the Court should not adopt them. Concerns that eliminating reliance on the plain view exception in digital searches would exclude all evidence outside that authorized by the warrant are overstated, as police may still rely on other warrantless seizure doctrines such as the inevitable discovery and independent source rules.

B. Even If The Plain View Doctrine Is Applicable To Digital Searches, The Elements Of Plain View Are Not Met In This Case.

Even if the Court holds that the plain view exception may be applied in digital searches, the plain view exception does not sanction the seizure of evidence in this case. A warrantless seizure is legal under the plain view doctrine when: (1) the officer is lawfully present in the place where the evidence can be plainly viewed; (2) the officer has a lawful right of access to the object itself; and (3) the incriminating character of the object is “immediately apparent.” *Horton*, 496 U.S. at 136-37. The government has failed to establish the first two of these elements because the warrant was not valid under the guidelines established in *Comprehensive Drug Testing* and because investigators exceeded the scope of the warrant. In addition, because the plain view doctrine does not justify the expansion of the search to evidence not covered by the warrant, the search and seizure was not lawful.

1. Investigators were not lawfully present in the place where the evidence could be plainly viewed because the warrant was not valid under the guidelines established in Comprehensive Drug Testing.

Contrary to the Guidelines, the warrant failed to prevent the government from seeing unauthorized information and was premised upon inadequate governmental disclosure of the risk of data loss and concealment. Therefore the warrant was invalid.

The warrant first directed that “appropriately trained personnel” were to review the seized data, retain whatever information was authorized by the warrant, and return the unauthorized information. R. at 8. As discussed earlier, this provision meets the first requirement under *Comprehensive Drug Testing*.

Second, the warrant did not discuss the search protocol in great detail, though it did require that a third party segregate the data and that the search be limited to information “reasonably related to the investigation into the five named players’ illegal steroid use.” *Comprehensive Drug Testing*, 579 F.3d at 1006-07. Although the warrant limited the search to information reasonably related to the investigation, it did not successfully prevent the government from staying beyond this restriction as the Ninth Circuit requires. Whether this was due to a defect in the search protocol or bad faith on the investigators’ part, the search did not satisfy the Ninth Circuit’s ultimate requirement that the case agents only see the specific data for which they have probable cause, and therefore was invalid.

Third, the warrant was based on the FBI’s inadequate descriptions of the risk of data loss and concealment, a fatal flaw which undermines the validity of the warrant. As discussed earlier, the FBI failed to emphasize that StarTests is a legitimate business, not suspected of any wrongdoing, and one which has no incentive to thwart a government investigation. In order to meet the requirement, investigators should have modified their list of potential challenges to fit

the particular circumstances of the search. Instead, the FBI pointed to “difficulties common to all computer searches,” including the possibility that files would be mislabeled or “deceptively” hidden. *Id.* For these reasons, the FBI’s failure to fully disclose the risks of data loss and concealment rendered the warrant invalid.

Therefore, because the warrant did not specifically outline a search protocol, and because the FBI did not fully disclose the risk of destruction or concealment of information in its warrant application, the warrant was invalid.

2. *Investigators did not have a lawful right of access to the information because the government violated the terms of the warrant by not segregating the information authorized in the warrant from unauthorized information.*

Even if the warrant was valid, investigators’ actions exceeded its scope, and evidence obtained as a result was not in plain view. For evidence to be lawfully seized under the plain view doctrine, police must have a “lawful right of access” to the evidence. *Horton*, 496 U.S. at 137. When the scope of a search “exceeds that permitted by the terms of a validly issued warrant,” the resulting seizure is unconstitutional. *Id.* at 141. In *Osorio*, the court held that the government could not rely on the plain view doctrine where the government agent discovered pictures after she began a search that exceeded the scope of the warrant. 66 M.J. at 637. The warrant authorized the search and seizure of pictures stored on a hard drive and pertaining to a sexual assault the government was investigating. *Id.* at 634. When copying the hard drive, however, the agent began opening unrelated files to determine whether the images were of child pornography. *Id.* at 635. Because the search exceeded the scope of the warrant, the court denied the government’s argument that the images were in plain view.

In this case, the warrant required that police use trained personnel to segregate information authorized in the warrant from unauthorized information and then return the

unauthorized information. R. at 2. The warrant further required that police restrict their search and seizure to information regarding the illegal steroid use of five named players. *Id.* Despite these clearly defined restrictions, the FBI violated the terms of the warrant in two regards by expanding the scope of the search beyond that permitted in the warrant. First, police did not direct “appropriately trained personnel” to review the data, segregate authorized information, and return the unauthorized information. The FBI may have used “computer personnel” to review the data, but the FBI never segregated the information authorized by the warrant—that is, the information regarding the illegal steroid use of the five named players for whom the FBI had probable cause—from information not authorized by the warrant. *Id.* Instead, as the district court opinion notes, the FBI “thoroughly cop[ied] and inventor[ied] the computer hard drives,” *id.*, actions which are inconsistent with segregating and returning data not authorized by the warrant.

Second, the FBI did not restrict its search and seizure to information regarding the five named players’ illegal steroid use, as the warrant required. The FBI violated this restriction in two regards: by seeking information on other players, and by seeking information on all illegal substance use. *Id.* As in *Osario*, the FBI intentionally exceeded the authority in the warrant and began a new, unauthorized search. Although the FBI spent weeks copying, inventorying, and searching the hard drives, and although the FBI presumably had ample time to apply for a second warrant, R. at 9, investigators never sought a magistrate’s approval prior to its rogue search.

For these reasons, the FBI’s search and seizure of information unrelated to the illegal steroid use of the five named players exceeded the scope of the warrant. Therefore, investigators did not have a lawful right of access to the information, and the information was not lawfully seized under the plain view doctrine.

3. That the incriminating character of the database was immediately apparent did not justify the expansion of the search to include evidence not authorized under the warrant.

The incriminating character of an object is immediately apparent when police have probable cause to believe that an object is contraband “without conducting some further search of the object” *Dickerson*, 508 U.S. at 375. The purpose of this requirement is to “obviate prolonged, warrantless rummaging” in order to determine whether evidence is incriminating. *United States v. Garces*, 133 F.3d 70, 76 (D.C. Cir. 1998) (quoting *United States v. Szymkowiak*, 727 F.2d 95, 98 (6th Cir.1984)). In *United States v. Angelos*, police discovered bags of marijuana in a basement while executing a “limited” warrant authorizing the search of only a car and a safe located in a basement. 433 F.3d 738, 744, 746 (10th Cir. 2006). Despite this narrow authorization, police expanded the search upon finding the marijuana and seized numerous other items found throughout the house. *Id.* at 744. The court held that the bags of marijuana were in plain view but that police were not authorized to exceed the scope of the warrant and search the entire house. *Id.* at 746. The court emphasized that, with a simple phone call, police could have sought “authorization to expand the scope of the search to include the entire premises” but failed to do so. *Id.*

Similarly, in this case, the database showed test results for illegal substances, and the incriminating character of this information was immediately apparent to investigators. This fact, however, only entitled police to *seize* the information. *See Hicks*, 480 U.S. at 326 (noting that the plain view doctrine, if applicable, would have “sustained a seizure of the equipment”). The FBI had already seized the database, however. Because the plain view exception permits a warrantless seizure, but not a warrantless search, the presence of incriminating information did not permit the FBI to expand its search beyond what was permitted in the warrant. *Horton*, 496

U.S. at 136 (“the ‘plain view’ doctrine may not be used to extend a general exploratory search from one object to another”) (quoting *Coolidge*, 403 U.S. at 466). Just as the discovery of marijuana in a basement in *Angelos* did not authorize police to expand their search to the entire house, the discovery of test results in this case did not give the FBI the authorization to expand its search beyond the limits prescribed by the warrant. And just as police in *Angelos* were required to contact the issuing judge to receive the authority to expand their search, the FBI was required to seek a second warrant or the permission of the magistrate judge to expand the search to include players and illegal substances not named in the warrant. The FBI makes no claim that the exigencies of the search required that it dispense with seeking a second warrant, and no such claim could be supported by the record, as police spent weeks analyzing StarTests’ databases. R. at 9.

Therefore, because the presence of incriminating evidence only permits the seizure of that evidence but does not support the unauthorized expansion of a search beyond the scope of the warrant, the FBI may not rely on the plain view exception to sanction the expansion of its search to include players and substances not included in the warrant.

Accordingly, the Court should hold that the plain view doctrine does not apply to digital searches and that it does not sanction the seizure of evidence beyond the warrant’s authorization.

CONCLUSION

The prevalence and complexity of computers make it likely that any computer search will expose investigators to intimate personal details about a person. The Ninth and Fourteenth Circuits have shown that law enforcement concerns cannot and need not justify this result. The Guidelines take the realities of computer searches as a starting point and strike the right balance between promoting law enforcement and protecting the Fourth Amendment. Government abuses

in *Comprehensive Drug Testing* and the present case cannot occur when the government is required to honestly disclose its investigatory needs in advance and a search protocol tailored to those needs is devised to prevent overreaching. Search protocols give the government effective tools and are endorsed by scores of criminal and civil courts. The government's abuse of the terms of the StarTests warrant, however, shows that search protocols are no substitute for a third party segregation requirement that prevents investigators from seeing more than they are allowed to see. These measures will prevent the government from overstepping the Fourth Amendment, as long as the plain view exception does not apply. This Court should not allow another abusive government search to confirm what is already evident from the facts of this case and others like it: without strong but fair affirmative restrictions such as imposed by the Ninth and Fourteenth Circuits, the government will turn computer searches for discrete files into unconstitutional general searches.

For the reasons outlined above, this Court should affirm the U.S. Court of Appeals for the Fourteenth Circuit.