

Nos. 05-10067, 05-15006, 05-55354

**UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT**

UNITED STATES OF AMERICA,

Plaintiff-Appellant,

v.

COMPREHENSIVE DRUG TESTING, INC., et al.,

Defendants-Appellees.

ON APPEAL FROM THE UNITED STATES DISTRICT COURTS FOR
THE NORTHERN DISTRICT OF CALIFORNIA (No. CR Misc. 04-234 SI),
THE CENTRAL DISTRICT OF CALIFORNIA (No. CV 04-2887 FMC (JWJx)),
AND THE DISTRICT OF NEVADA (No. CV-S-04-0707-JCM-PAL)

**BRIEF FOR THE UNITED STATES
IN SUPPORT OF REHEARING EN BANC
BY THE FULL COURT**

ELENA KAGAN
Solicitor General

JOSEPH P. RUSSONIELLO
United States Attorney

MYTHILI RAMAN
Acting Assistant Attorney General

J. DOUGLAS WILSON

ERIKA R. FRICK

BARBARA J. VALLIERE

MICHAEL R. DREEBEN
Deputy Solicitor General

*Assistant United States Attorneys
Northern District of California*

GARY G. GRINDLER
Deputy Assistant Attorney General

TOBY J. HEYTENS
Assistant to the Solicitor General

(counsel continued on next page)

J. CAM BARKER
Attorney
U.S. Department of Justice
Washington, DC 20530

KAREN LOEFFLER
United States Attorney
District of Alaska

DENNIS BURKE
United States Attorney
District of Arizona

GEORGE S. CARDONA
Acting United States Attorney
Central District of California

BENJAMIN B. WAGNER
United States Attorney
Eastern District of California

KAREN P. HEWITT
United States Attorney
Southern District of California

LEONARDO M. RAPADAS
United States Attorney
Districts of Guam and the Northern
Mariana Islands

FLORENCE NAKAKUNI
United States Attorney
District of Hawaii

THOMAS E. MOSS
United States Attorney
District of Idaho

WILLIAM W. MERCER
United States Attorney
District of Montana

DANIEL G. BOGEN
United States Attorney
District of Nevada

KENT ROBINSON
Acting United States Attorney
District of Oregon

JAMES A. MCDEVITT
United States Attorney
Eastern District of Washington

JENNY A. DURKAN
United States Attorney
Western District of Washington

TABLE OF CONTENTS

TABLE OF CONTENTS. i

TABLE OF AUTHORITIES. ii

I. The En Banc Panel’s Decision Violates Basic Norms Of Article III Courts. . . 3

II. The En Banc Panel’s Protocols Conflict With Controlling Authority. 8

III. The Computer Search Procedures Mandated By The En Banc Panel Are
Causing Grave Harm To Effective Law Enforcement. 14

 A. Requiring Plain-View Waivers Frequently Would Result In The Loss
 Of Critical Evidence Of Serious Crimes. 14

 B. The Filter-Team Requirement Is Unworkable. 15

CONCLUSION. 18

CERTIFICATE OF COMPLIANCE WITH RULE 32(a). 21

CERTIFICATE OF SERVICE. 22

TABLE OF AUTHORITIES

FEDERAL CASES

Bank of Nova Scotia v. United States, 487 U.S. 250 (1988)..... 13

Cheney v. United States Dist. Court, 542 U.S. 367 (2004). 8

Dalia v. United States, 441 U.S. 238 (1979).. 10

Greenlaw v. United States, 128 S. Ct. 2559 (2008). 3

Horton v. California, 496 U.S. 128 (1990).. 8

Lo-Ji Sales, Inc. v. New York, 442 U.S. 319 (1979).. 11, 12

Preiser v. Newkirk, 422 U.S. 395 (1975). 5

Princeton Univ. v. Schmid, 455 U.S. 100 (1982). 3

Shadwick v. City of Tampa, 407 U.S. 345 (1972).. 11

Steel Co. v. Citizens for a Better Env't, 523 U.S. 83 (1998). 3, 8

Stormans, Inc. v. Selecky, Nos. 07-36039, 07-36040, 2009 WL 3448435
(9th Cir. Oct. 28, 2009).. 5

Thomas v. Arn, 474 U.S. 140 (1985).. 13

United States v. Brooks, 427 F.3d 1246 (10th Cir. 2005),
cert. denied, 546 U.S. 1222 (2006).. 16

United States v. Grubbs, 547 U.S. 90 (2006). 10

United States v. Grummer, 08cr4402-DMS (S.D. Cal.).. . . . 15

United States v. Payner, 447 U.S. 727 (1980).. 9

Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646 (1995). 10
Zurcher v. Stanford Daily, 436 U.S. 547 (1978). 11

FEDERAL RULES

Federal Rule of Appellate Procedure 32(a)(5). 21
Federal Rule of Criminal Procedure 41(f)(1)(B). 12, 13
Federal Rule of Criminal Procedure 41(g). 4

LOCAL RULES

9th Cir. R. 35-1. 18
9th Cir. R. 35-2. 18
9th Cir. R. 35-3. 18

Nos. 05-10067, 05-15006, 05-55354

**UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT**

UNITED STATES OF AMERICA,

Plaintiff-Appellant,

v.

COMPREHENSIVE DRUG TESTING, INC., et al.,

Defendants-Appellees.

**BRIEF OF THE UNITED STATES
IN SUPPORT OF REHEARING EN BANC
BY THE FULL COURT**

The en banc panel's decision announced sweeping new rules for warrants to search computers that are having an immediate and detrimental effect on law enforcement efforts. In some districts, computer searches have ground to a complete halt, and, throughout the Circuit, investigations have been delayed or impeded. Magistrate judges are uniformly viewing compliance with the newly announced rules as mandatory, but they are implementing those rules in vastly different ways.

All of this was unnecessary. The parties in these cases disagree about the proper resolution of the issues presented for decision, but they agree on one fundamental point: The new rules that the en banc panel announced for the issuance and execution

of warrants to search computers were unnecessary to the issues presented in these cases.

The en banc panel stepped outside the proper role of an Article III court when it set forth detailed protocols that purport to bind, and that are being understood as binding, magistrate and district judges in future cases. The seminal issues surrounding computer searches should be resolved in actual controversies—not through “guidance” that “magistrate judges must be vigilant in observing.” Op. 11891-11892.

On the merits, the detailed protocols announced by the en banc panel conflict with Supreme Court decisions interpreting the Fourth Amendment and the scope of a federal court’s supervisory power. If fully implemented, they also would conflict with amendments to the Federal Rules of Criminal Procedure that are scheduled to go into effect within days.

The United States is mindful that this Court has never granted full court en banc. Indeed, the federal government has never asked the Court to do so. But the broad issues unnecessarily addressed in the en banc panel’s opinion are of surpassing importance and compel that extraordinary action. The full Court should enter an order that vacates the Court’s judgment in these cases and withdraws the en banc panel’s decision. The full Court should then either issue a new opinion limited to the

issues properly before it or, at a minimum, allow the parties to brief the appropriateness of the sweeping new protocols announced by the en banc panel.

I. The En Banc Panel's Decision Violates Basic Norms Of Article III Courts.

Federal courts do “not sit to . . . give advisory opinions about issues as to which there are not adverse parties before [them].” *Princeton Univ. v. Schmid*, 455 U.S. 100, 102 (1982); *see also Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 101-102 (1998). “In our adversary system,” courts “follow the principle of party presentation” and “rely on the parties to frame the issues for decision and assign to courts the role of neutral arbiter of matters the parties present.” *Greenlaw v. United States*, 128 S. Ct. 2559, 2564 (2008). The en banc panel violated those fundamental principles by venturing far beyond the issues presented in these cases and announcing what purport to be, and are being understood as, binding guidelines for future cases involving computer searches. Regardless of the merits of the detailed protocols specified in the en banc panel's opinion, consideration by the full Court is necessary to confine the Court's decision in these cases to the proper performance of the judicial function—*i.e.*, resolution of the issues actually raised on appeal, not issuance of legal rules disposing of issues not before it.

A. The en banc panel concluded that the dispositive legal issues in this case were (1) whether one particular appeal was timely filed, *see* Op. 11870, (2) whether

another appeal was controlled by the preclusive effect of two district court orders, *see* Op. 11875-11876, 11880, 11884-11885, (3) whether the government complied with the terms of various warrants, *see* Op. 11876-11880, (4) whether a district court abused its discretion in ordering a return of property under Federal Rule of Criminal Procedure 41(g), *see* Op. 11882-11886, and (5) whether a district court abused its discretion in concluding that compliance with a certain subpoena would be “unreasonable or oppressive,” Op. 11886-11887. The en banc panel addressed those discrete issues and resolved them in favor of appellees.

B. Throughout its opinion and particularly in a lengthy section captioned “Concluding Thoughts,” however, the en banc panel reached well beyond the issues before it and purported to establish binding new procedures for the issuance and execution of warrants in future cases involving computer searches. Despite finding it unnecessary to decide whether the warrants in these cases were properly issued, the en banc panel identified detailed procedures that the government and magistrates “should” (Op. 11877, 11880, 11892), “must” (Op. 11877, 11881, 11891-11892), or “shall” (Op. 11878) follow in seeking and granting warrants in future cases. The en banc panel also stated that “magistrate judges must be vigilant in observing” various “guidance” set forth in its opinion about the issuance and execution of warrants to search computers, and provided a five-point summary of “procedures” that “will

prove a useful tool for the future.” Op. 11891-11892. In issuing this wide-ranging and detailed “guidance” about subjects that were unnecessary to resolve the particular cases before it, the en banc panel departed from the proper role of an Article III court. *See Preiser v. Newkirk*, 422 U.S. 395, 401 (1975) (“[A] federal court has neither the power to render advisory opinions nor to decide questions that cannot affect the rights of litigants in the case before them.”) (internal quotation marks and citation omitted); *Stormans, Inc. v. Selecky*, Nos. 07-36039, 07-36040, 2009 WL 3448435 at *9 (9th Cir. Oct. 28, 2009) (“Our role is neither to issue advisory opinions nor to declare rights in hypothetical cases, but to adjudicate live cases or controversies consistent with the powers granted the judiciary in Article III of the Constitution.”) (citation omitted).

C. The en banc panel’s departure from basic Article III norms has had immediate and profound legal effects on computer searches.

1. Magistrate and district court judges throughout this Circuit are treating the en banc panel’s “guidance” as binding. For example, the Chief Magistrate Judge for the Western District of Washington recently sent the United States Attorney’s Office for that district a letter stating that “we are all required to follow the requirements set forth in the [en banc panel]’s decision” and enclosing a two-page document outlining detailed procedures they have derived from the opinion that will control all future

computer searches. *See* Ex. A. Judges across the Circuit have reached varied conclusions about which specific procedures are required by the en banc panel's decision: for example, magistrate judges have disagreed about whether the en banc panel's new requirements apply in related contexts, such as searches of cell phones and e-mail accounts. But a widespread consensus has emerged among judges throughout this Circuit that compliance is mandatory.

2. The government is accordingly laboring under the direct effects of this new legal regime. Many United States Attorney's Offices have been chilled from seeking any new warrants to search computers. And all offices within the Circuit report problems in executing warrants in the aftermath of the en banc panel's opinion. In the District of Arizona, for example, an FBI forensic examiner has advised that, to comply with the en banc decision's rules, he will need many months to learn a complex national security case before attempting to segregate responsive and non-responsive data on a seized computer.

The en banc panel's new protocols also have shifted investigations to state authorities who are not bound by those protocols, even in cases involving interstate criminal conduct. In the Western District of Washington, for example, 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.

3. The irregular manner in which the en banc panel formulated and announced its new protocols has serious consequences for the government's ability to contest the appropriateness of those protocols via the usual course. Many of the issues discussed in the en banc panel's decision were not briefed or argued by the parties in these cases, and so the government has never been heard on them. Going forward, even assuming jurisdiction for an appeal from the denial of a warrant in which the government declined to "waive reliance upon the plain view doctrine," or in which the court ordered "[s]egregation and redaction . . . by specialized personnel or an independent third party," Op. 11892, three-judge panels cannot be expected to address the issues free from the directives issued by the en banc Court in this case. *See* Op. 11891 ("Everyone's interests are best served if there are clear rules to follow . . ."). And mandamus would be an even greater hurdle, because the very existence of the en banc panel's decision could make it impossible for the government to establish a "clear and indisputable" entitlement to relief before a panel of this Court.

Cheney v. United States Dist. Court, 542 U.S. 367, 381 (2004) (citation omitted). At any rate, the government should not be put to the burden of seeking an extraordinary writ to obtain an *initial* opportunity to be heard about many of the critically important issues addressed in the en banc panel's decision.

The judicial power's limitation to actual cases and controversies is "essential" to the separation of powers. *Steel Co.*, 523 U.S. at 101. These cases illustrates that massive harms can occur when courts depart from that principle. Full court review is necessary because the en banc panel's announcement of elaborate standards to guide the conduct of future computer searches by the Executive Branch represents an extreme departure from the usual and proper course of judicial proceedings.

II. The En Banc Panel's Protocols Conflict With Controlling Authority.

Full court review also is warranted because the new standards announced by the en banc panel are legally wrong. They conflict with binding Supreme Court authority and will, within days, conflict with the Federal Rules of Criminal Procedure as well.

Plain-view waiver.—The plain-view exception to the warrant requirement applies when law enforcement officers "have a warrant to search a given area for specified objects, and in the course of the search come across some other article of incriminating character." *Horton v. California*, 496 U.S. 128, 135 (1990). The en banc panel's opinion acknowledged the existence of that well-established doctrine,

see Op. 11876-11877, 11879, but expressed concerns about its implications in the computer-search context. The Court then answered those concerns by requiring the government to waive reliance on the plain-view doctrine as a pre-condition to obtaining a warrant to search a computer. *See* Op. 11888-11892. The en banc panel's waiver rule is unprecedented. The Court did not hold that the Fourth Amendment of its own force imposes this requirement in computer search cases. And it identified no other support for such a mandate.

The en banc panel could not properly rely on supervisory powers as a basis for requiring such waivers. The Supreme Court has made clear that the 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). If the law permits plain-view seizures, courts cannot use supervisory powers to disapprove them. Just as the district court in *Payner* could not invoke supervisory powers to exclude evidence whose collection did not violate the defendant's constitutional rights, the en banc panel could not use its supervisory power to require the government to promise not to introduce such evidence as a condition of obtaining a warrant in the first place. As in *Payner*, such a practice would amount to "a substitution of [a lower court's] judgment for the controlling decisions of [the Supreme] Court." *Id.*

Required use of filter teams.—The en banc panel also went off track in concluding that, in computer search cases, “[s]egregation and redaction [of non-responsive information] must be either done by specialized personnel or an independent third party.” Op. 11892. “Nothing in the language of the Constitution or in [the Supreme Court’s] decisions interpreting that language suggests that, in addition to the [requirements set forth in the text] [of the Fourth Amendment], search warrants also must include a specification of the precise manner in which they are to be executed.” *United States v. Grubbs*, 547 U.S. 90, 98 (2006) (second set of brackets in original; citation omitted). In addition, the Supreme Court has made clear that, subject to the Fourth Amendment’s general protection against unreasonable searches, “it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant.” *Dalia v. United States*, 441 U.S. 238, 257 (1979). The en banc panel’s edict to the government to use a filter team in all cases involving computer searches conflicts with those well-established principles, as well as the Supreme Court’s “repeated[] refus[al] to declare that only the ‘least intrusive’ search practicable can be reasonable under the Fourth Amendment.” *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 663 (1995).

Use of court-supervised third parties to review evidence in certain cases.—The en banc panel also announced a “presumption” that, in cases “where the party subject to the warrant is not suspected of any crime, and where the privacy interests of numerous other parties who are not under suspicion of criminal wrongdoing are implicated by the search,” the segregation and redaction of non-responsive information should be performed by “an independent third party under the supervision of the court.” Op. 11877, 11881. The Supreme Court, however, has rejected the idea that different rules are necessary for “‘third party’ search[es]” because “[t]he Fourth Amendment itself has struck the balance between privacy and public need.” *Zurcher v. Stanford Daily*, 436 U.S. 547, 553, 559 (1978).

In addition, for courts to supervise the execution of warrants raises serious constitutional concerns. The Fourth Amendment requires that a warrant be issued by a neutral and detached judicial officer, and the Supreme Court has made clear that “[w]hatever else neutrality and detachment might entail, it is clear that they require severance and disengagement from activities of law enforcement.” *Shadwick v. City of Tampa*, 407 U.S. 345, 350 (1972). In *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319 (1979), the Supreme Court held that a Town Justice failed to “manifest that neutrality and detachment demanded of a judicial officer” when he visited the search scene and made personal determinations about what evidence fell within the scope of the

warrant. *Id.* at 326. The en banc panel never considered how its directive to magistrate judges to “supervis[e]” (Op. 11877) the process of executing warrants to search computers can be squared with *Lo-Ji Sales*.

Nor does use of an outside filter team result in any additional protection to legitimate privacy interests. To find responsive data, *someone* is going to have to see much of what is stored on the hard drive of a computer that is subject to a lawful search. The use of an outside filter team thus would not protect privacy at all; instead, it would simply protect wrongdoers by putting certain incriminating information beyond the reach of law enforcement officers who have legitimate investigatory reasons to examine a computer.

Detailed inventory and destroying government copies.—The en banc panel’s opinion states that, in cases involving warrants to search computers, the government’s return must describe “precisely what data [the government] has obtained as a consequence of the search, and what data it has returned to the party from whom it was seized.” Op. 11881. The en banc panel’s opinion further states that “[t]he government may not retain copies of such returned data, unless it obtains specific judicial authorization to do so.” Op. 11881.

Both of those requirements squarely conflict with amendments to Federal Rule of Criminal Procedure 41(f)(1)(B) that have been approved by the Supreme Court and

are scheduled to take effect on December 1, 2009, just days after this brief is filed. Absent action by Congress, amended Rule 41(f)(1)(B) will provide: (1) that “[i]n 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”; and (2) that the officer who executes the return “may retain a copy of the electronically stored information that was seized or copied.”

The en banc panel’s decision neither mentioned the pending amendments to Rule 41 nor identified the source of its newly announced rules about the nature and contents of a warrant return in cases involving computer searches. To the extent that the en banc panel viewed those rules as required by the Fourth Amendment, its decision appears to conflict with the Supreme Court’s own constitutional judgment in approving the amendments to Rule 41. And to the extent that the en banc panel relied on its supervisory authority, its new warrant-return protocols will soon be superseded. “[E]ven a sensible and efficient use of the supervisory power . . . is invalid if it conflicts with constitutional or statutory provisions,” *Thomas v. Arn*, 474 U.S. 140, 148 (1985), and “federal courts have no more discretion to disregard [a] Rule’s mandate than they do to disregard constitutional or statutory provisions,” *Bank of Nova Scotia v. United States*, 487 U.S. 250, 255 (1988). By failing to identify the

source of the protocols it announced, the en banc panel gave magistrate judges no guidance about whether they should follow the amendments to Rule 41 or the rules announced by this Court.

III. The Computer Search Procedures Mandated By The En Banc Panel Are Causing Grave Harm To Effective Law Enforcement.

A. Requiring Plain-View Waivers Frequently Would Result In The Loss Of Critical Evidence Of Serious Crimes.

Computers are ubiquitous in contemporary life. The corollary is that they often contain significant evidence of criminal activity. Because computer searches often lead to the discovery of vital evidence that falls squarely within the plain-view doctrine, requiring the government to “forswear reliance on” it (Op. 11877) as a condition of obtaining a warrant prevents investigators from discovering information about serious and ongoing or imminent criminal activity. A search of a computer for evidence of fraud, for example, could reveal evidence of a planned terrorist attack or a search aimed at drug trafficking could reveal evidence of an ongoing violent crime or sexual abuse. Requiring plain-view waivers also could result in the loss of highly probative evidence about the very crime under investigation, such as when a warrant contains a date restriction but the resulting search turns up evidence that the crime began or continued after officers previously had reason to believe. Evidence discovered in plain view during a search under warrant is, by definition, the fruit of constitutionally permissible activity. Accordingly, compelling law enforcement to

forswear the use of such evidence sacrifices the compelling societal interest in prosecuting crime without serving a countervailing privacy interest.

These concerns are not hypothetical. In one recent case, an agent examining a computer pursuant to a warrant to search for evidence of environmental crimes related to the sale of DDT discovered evidence that the defendant possessed large quantities of child pornography, had taken videos of his 13-year-old stepdaughter naked, and had file-sharing software on his computer that made his child pornography available to others. *See United States v. Grummer*, 08cr4402-DMS (S.D. Cal.). If the government had been required to waive reliance on the plain-view doctrine as a condition of obtaining the initial warrant, it might have been impossible to prosecute the defendant for that conduct.

B. The Filter-Team Requirement Is Unworkable.

Without the benefit of briefing on how computer searches typically are conducted, the en banc panel crafted a filter-team requirement that presupposes that warrants to search computers usually authorize the seizure of discrete and easy-to-identify files. But the computer searches performed thousands of times annually in terrorism, computer hacking, fraud, identity theft, drug distribution, child pornography, and other types of investigations often seek particular information to answer more general questions, such as who used a computer, when they did so, and

the purpose and manner of that use. Such searches “can be as much an art as a science,” *United States v. Brooks*, 427 F.3d 1246, 1252 (10th Cir. 2005), cert. denied, 546 U.S. 1222 (2006), and they often require detailed knowledge about the participants in and practices surrounding the suspected criminal activity in order to determine whether particular information is relevant and falls within the scope of a warrant.

1. The procedures mandated by the en banc panel will be grossly inefficient, lead to delays in obtaining time-sensitive evidence, and heighten the risk that important information will be missed. Before a search commences, case agents will need 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. Even after receiving such a crash course, filter team members will be unlikely to know a case as well as the case agents, with the result that at least some responsive and potentially case-critical information will go unrecognized. 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.

2. The en banc panel's filter-team requirement also will strain scarce government resources. Computer forensics labs often faced substantial backlogs even before the en banc panel's decision, and they generally lack the personnel to absorb the burden of learning entire cases in order to segregate responsive from non-responsive information. In addition, the government will need to devote additional resources to documenting compliance with the filter-team requirement in order to address future motions to suppress that allege lack of compliance with that requirement.

3. The difficulties identified above will only be magnified in cases where the filter team consists of "independent third parties not affiliated with the government." Op. 11881. The cost of hiring such third parties often will be prohibitive. In previous cases where the government has had to employ special masters to separate legally privileged materials on electronic storage devices, costs have run into the hundreds of thousands of dollars.

Mandating use of third parties to conduct computer searches also would risk the integrity and security of evidence. The en banc panel's decision could result in the loss of admissible evidence if a third-party searcher failed to protect against evidence contamination, network security breaches, or employee misconduct. The use of an outside filter team also could threaten the security of investigations, particularly those in which an examiner must know the identity of a confidential informant or have

access to classified information in order to have a full understanding of what he is seeing. It is entirely inappropriate to require the government to entrust the viability of its cases and the security of highly sensitive information to private contractors whose employees the government does not hire, fire, or supervise.

CONCLUSION

The full Court should enter an order that vacates the judgment and withdraws the en banc panel's decision. Consistent with this Court's procedures for granting limited rehearing en banc of a three-judge panel decision, the order should provide that the en banc panel's decision "shall not be cited as precedent by or to this court or any district court of the Ninth Circuit, except to the extent adopted by the" full court sitting en banc. 9th Cir. R. 35-1 to 35-3, advisory committee's note para. 3. The full Court should then issue a revised opinion confined to the issues that are necessary to resolve these particular appeals or, at a minimum, allow the parties to file briefs addressing the appropriateness of the sweeping new protocols announced by the en banc panel.

Respectfully submitted,

Dated: November 23, 2009

ELENA KAGAN
Solicitor General

MICHAEL R. DREEBEN
Deputy Solicitor General

MYTHILI RAMAN
Acting Assistant Attorney General

GARY G. GRINDLER
Deputy Assistant Attorney General

TOBY J. HEYTENS
Assistant to the Solicitor General

J. CAM BARKER
Attorney
Department of Justice,
Washington, DC 20530

/s/
JOSEPH P. RUSSONIELLO
United States Attorney

J. DOUGLAS WILSON
ERIKA R. FRICK
BARBARA J. VALLIERE
Assistant United States Attorneys
Northern District of California

KAREN LOEFFLER
United States Attorney
District of Alaska

DENNIS BURKE
United States Attorney
District of Arizona

GEORGE S. CARDONA
Acting United States Attorney
Central District of California

BENJAMIN B. WAGNER
United States Attorney
Eastern District of California

KAREN P. HEWITT
United States Attorney
Southern District of California

LEONARDO M. RAPADAS
United States Attorney
Districts of Guam and the Northern
Mariana Islands

FLORENCE NAKAKUNI
United States Attorney
District of Hawaii

KENT ROBINSON
Acting United States Attorney
District of Oregon

THOMAS E. MOSS
United States Attorney
District of Idaho

JAMES A. MCDEVITT
United States Attorney
Eastern District of Washington

WILLIAM W. MERCER
United States Attorney
District of Montana

JENNY A. DURKAN
United States Attorney
Western District of Washington

DANIEL G. BOGEN
United States Attorney
District of Nevada

EXHIBIT A

Oct 01 09 03:22p

Strombom

2538823891

P. 1



UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON

CHAMBERS OF
KAREN L. STROMBOM
CHIEF UNITED STATES MAGISTRATE JUDGE

U.S. COURTHOUSE
1717 PACIFIC AVENUE
TACOMA, WA 98402

(253) 882-3890

October 1, 2009

Robert Westinghouse
Assistant United States Attorney
U.S. Department of Justice
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271

Re: Warrant Requirements under *United States v. Comprehensive Drug Testing*

Dear Mr. Westinghouse:

In a letter dated September 21, 2009, you outlined your office's position regarding the application of *United States v. Comprehensive Drug Testing Inc.*, ___ F.3d ___, 2009 WL 2605378 (9th Cir. August 26, 2009) (en banc) to warrants authorizing searches of electronically stored information. A copy of your letter was provided to the Magistrate Judges in this district. We met, discussed your office's position, and the *Comprehensive Drug Testing* decision to determine the impact and requirements of the decision.

The decision significantly affects the manner in which searches of electronically stored information may be conducted. It specifies that the "plain view" doctrine does not apply to such a search. It imposes additional requirements on the government in requesting a warrant, and on Magistrate Judges in issuing the warrants, with relation to the risk of destruction of data, the scope of the warrants, and procedures to be used in seizing and searching devices containing electronically stored information. It requires the government to provide a return certifying that the data or devices seized have been returned or destroyed.

The Magistrate Judges understand the United States disagrees with the majority decision in *Comprehensive Drug Testing* but as Judge Bea states in his dissent "the establishment of guidelines which are little more than dicta . . . are nonetheless binding precedent in this circuit." *Id.* at *24. Therefore, we are all required to follow the requirements set forth in the majority's decision.

Oct 01 09 03:23p

Strombom

2538823891

P.2

Robert Westinghouse
October 1, 2009
Page 2

Accordingly, attached is a two page outline entitled SEARCH WARRANT REQUIREMENTS FOR ELECTRONICALLY STORED INFORMATION which sets forth what we have concluded *Comprehensive Drug Testing Inc.* requires of the United States and Magistrate Judges for warrants seeking the seizure and search of electronically stored information. This outline has also received the approval of the district judges.

We expect that warrant applications for electronically stored information will comply with the requirements set forth in the attached outline. Additionally, we expect that any Assistant U.S. Attorney who submits a warrant application that deviates from these requirements will highlight those deviations to the Magistrate Judge at or before the time the application is submitted for approval. The Magistrate Judges in this district will either modify or reject any provision that does not comply with these requirements.

Thank you for your work on this matter. If you have any additional questions or concerns, please feel free to contact us.

Sincerely,



Karen L. Strombom
Chief U. S. Magistrate Judge

enc.

cc: Chief Judge Robert S. Lasnik

SEARCH WARRANT REQUIREMENTS FOR ELECTRONICALLY STORED INFORMATION

Pursuant to *United States v. Comprehensive Drug Testing, Inc.*, ___ F.3d __ WL 2605378 (9th Cir. 2009), search and seizure warrants of devices containing electronically stored information ("ESI") must meet the following requirements:

THE SCOPE OF WARRANT

1. The scope of the warrant shall be limited to the device(s) and ESI for which the government has shown probable cause.
2. The government shall set forth a protocol for sorting, segregating, decoding and otherwise separating seizable ESI (as defined by the warrant) from all other ESI. This protocol will include a requirement that any such segregating be done either by a reasonably reliable third party who possesses the device(s) or ESI that is the subject of the warrant (such as an internet service provider) or by specially trained computer personnel who are not involved in the investigation (hereafter "Filter Team")
3. The warrant shall disclose the actual risk of destruction of ESI for which it has probable cause, as well as ~~prior efforts to seize the ESI in other judicial fora.~~
4. The government shall forswear reliance on the "plain view" doctrine for any ESI that it seeks to review in the enforcement of the warrant and agree that the Filter Team will not communicate any information outside the scope of the warrant that they learn during the segregation process, absent further approval of the court.

SEIZURE PROCEDURES

1. If the ESI that is subject to seizure is held by a reasonably reliable third party, the third party shall provide to the Filter Team a forensic copy of the ESI described in the warrant.
2. Otherwise, a forensic copy of ESI shall be made on-site by the Filter Team, if it is safe and reasonable to do so. The actual device(s) containing ESI shall not be taken off-site unless it contains ESI that is unlawful to possess, e.g. child pornography, or the device(s) was used to commit a criminal offense, i.e. an instrumentality.
3. If it is unsafe or unreasonable to make a forensic copy of the ESI on-site, the device(s) described in the warrant may be taken off-site. The Filter Team shall then make a forensic copy of the contents of the device(s) off site.

SEARCH PROCEDURES AND LIMITATIONS

1. Only the Filter Team may search the device(s) or forensic copies containing ESI that is outside the scope of the warrant. The Filter Team will then segregate and extract only ESI that falls within the scope of the warrant.
2. Once segregated and extracted, the ESI that is within the scope of the warrant will be copied to separate storage media. Absent further order by the issuing judicial officer, only ESI that has been segregated and extracted to separate storage media and is within the scope of the warrant will be provided to investigative agents and the United States Attorney. The Filter Team shall not disclose ESI outside the scope of the warrant or use it as the basis to seek additional search warrants or to perform additional searches of the seized devices.

RETURN PROCEDURES

1. As soon as practicable, but in any event no later than within 60 days of seizure (absent further order of the issuing judicial officer), the government must provide the issuing judicial officer with a return containing a sworn certificate that:
 - (a) certifies precisely what ESI it has obtained;
 - (b) certifies what ESI it has returned;
 - (c) certifies it has returned the actual device(s) seized; and
 - (d) certifies it has destroyed any copy made of the ESI that is outside the scope of the warrant.
2. The government may retain ESI outside the scope of the original warrant or the device(s) seized for a longer time period only if the government makes application to the issuing judicial officer, establishing a need to retain the ESI or device(s) seized, and obtains supplemental authorization from the issuing judicial officer for continued retention.