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.

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.

DEREK REGENSBURGER*

In United States v. Comprehensive Drug Testing, Inc., the Ninth Circuit recently held that the government may retain copies of drug testing results seized outside the scope of a search warrant because they were intermingled with results which were lawfully seized. The ruling has the potential to impact the way in which computer searches are conducted as well as the privacy of confidential medical records which become the subject of government investigations. This Article provides an in-depth analysis of this decision as well as traces the development of the law surrounding the search and seizure of computer records and files.

I. INTRODUCTION

“What happened to the Fourth Amendment? Was it repealed somehow?” Those are the chilling words of U.S. District Judge James Mahan, echoed by Ninth Circuit Judge Sidney Thomas in his dissent in United States v. Comprehensive Drug Testing, Inc. ("CDT"). The questions are in reference to federal agents’ seizure and subsequent search of confidential medical records in relation to their investigation of the illegal distribution of steroids by the Bay Area Laboratory Cooperative

* The author is the lead instructor in the Legal Studies Department at Everest College in Thornton, Colorado. He is a former Deputy District Attorney in Sterling, Colorado, and a graduate of the George Washington University School of Law.

1 United States v. Comprehensive Drug Testing, Inc. ("CDT"), 473 F.3d 915, 944 (9th Cir. 2006) (Thomas, J., concurring in part, dissenting in part).

2 Id.
The agents had issued subpoenas to and then executed search warrants on two independent testing labs to obtain the steroid testing records of ten Major League Baseball ("MLB") players who had connections to their investigation of BALCO. The Ninth Circuit upheld the agents' seizure and subsequent search of computer files, which contained steroid drug testing results not only for the ten targets of the federal investigation, but countless other athletes inside and outside of baseball.

Because of its connection to steroids and the government's investigation into BALCO and San Francisco Giants' slugger Barry Bonds, the decision received nationwide attention. Bonds's name is inextricably tied to the BALCO investigation, having been linked to BALCO and steroid use in a recent New York Times bestseller. Bonds was recently indicted on perjury and obstruction of justice charges that stemmed from allegedly false statements he made to the federal grand jury investigating illegal steroid distribution at BALCO. It has even been speculated that one of the motivations behind the government's initial investigation of BALCO was a personal vendetta that the government's lead investigator, Jeff Novitsky, had against Bonds.

Apart from its notoriety, the CDT decision is important in several respects. First, it attempts to define the parameters and limitations involved in computer searches, particularly with respect to the seizure and subsequent search of intermingled files. The CDT court held that government agents can seize entire collections of computer data for off-site review where files within the scope of the search warrant are intermingled with irrelevant data on the computer's hard drive. It also permitted the government to browse the contents of computer files to determine if they are within the scope of the warrant, without having to limit such a search to key words or file type. This part of the ruling recognizes the inherent need for flexibility in conducting computer searches.

3 Id. at 922.
4 Id. at 920-22.
5 Id. at 923-24.
7 Dave Sheinin, Home Run King Bonds Charged with Perjury, WASH. POST, Nov. 16, 2007, at A01.
9 CDT, 473 F.3d at 933-35.
10 Id. at 934.
11 Id. at 935.
Second, the decision is also notable for what it does not do—give adequate protection to the privacy concerns of innocent third parties whose records are caught up in the government's dragnet. The case raises a fascinating question: What privacy concerns are implicated when the government obtains confidential medical records from a disinterested third party and what steps have to be taken to ensure that such concerns are not violated? The majority opinion seems to give short shrift to privacy rights, giving the government virtual *carte blanche* to search intermingled data that it seizes. This power is subject to post-seizure review by a magistrate, but this review is only *after* a proper objection has been filed by an aggrieved party. In other words, the government is free to search the seized data until such objection is made. Thus, the ruling affords somewhat uncertain status to the prospect of effective judicial oversight, as there is no mechanism for providing notice to aggrieved third parties that their heretofore confidential records have been seized by the government.

In addition, given the myriad issues present in the case, the decision may serve as the perfect vehicle for the United States Supreme Court (should it be given the opportunity to review the case) to lay out a consistent, uniform set of guidelines for the government to follow in conducting computer searches—something that is sorely lacking in the current jurisprudence on this issue. As will be discussed in Part II of this

---

12 *Id.* at 938.
13 *Id.* at 974 (Thomas, J., dissenting).
14 Petitions for Rehearing before the Panel and a Rehearing *En Banc* were filed in the Ninth Circuit on February 12, 2007. The Ninth Circuit granted the petition for panel rehearing, withdrew its opinion issued on December 27, 2006, and issued a superseding opinion on January 24, 2008. United States v. Comprehensive Drug Testing, Inc., 513 F.3d 1085 (9th Cir. 2008). The petition for rehearing *En Banc* was denied as moot with leave to file a new motion. The Major League Baseball Players Association ("MLBPA") sought an extension of time to file a Petition for Rehearing *En Banc*. That deadline is March 10, 2008, but as of March 7, 2008, a petition had not been filed. It is uncertain at this time whether a Petition for Certiorari will be filed if that motion is filed and is unsuccessful. The Ninth Circuit panel ruled that the government's appeal of the order by Judge Florence-Marie Cooper in the Central District of California, denying reconsideration of her earlier order requiring the government to return property seized from the CDT laboratory in Long Beach, was untimely filed and therefore refused to hear the appeal of that order. *Id.* at 1098-99. However, the Ninth Circuit still had to determine whether the seizures which occurred at CDT were lawful since the MLBPA based its challenge to the search warrant of the Quest Diagnostics lab in Las Vegas on the ground that the CDT files were illegally seized and that the government should be forbidden from using the fruits of an illegal search to form the basis of the warrant to search for files at Quest. *Id.* at 1105. Finding that the government's seizure of the files at CDT was valid, the Ninth Circuit reversed an order by Judge James Mahan in the District of Nevada requiring the government to return property seized from Quest Diagnostics. *Id.* at 1113. Finally, the Ninth Circuit also reversed an order by Judge Susan Illston in the Northern District of California quashing the government's May 6, 2004, subpoenas to CDT and Quest that related to the San Francisco grand jury's investigation of
Article, the rules for conducting computer searches vary dramatically from circuit to circuit. If the decision is reversed, at least in part, then in the ultimate irony of ironies, the Supreme Court will have chastised the Ninth Circuit for having been too conservative when it comes to protecting the liberties and freedoms of individuals.

If nothing else, the CDT decision highlights the need for courts to adopt a more uniform approach to computer searches. The case pitted the two extremes of the current debate against one another. The majority took the position that computer searches require nothing more than an extension of the traditional rules governing searches of documentary evidence to the digital realm.\textsuperscript{15} Conversely, Judge Thomas argued in a boisterous dissent that computer searches require something more. He advocated for magistrate review of intermingled computer files before government investigators could inspect them, and argued that strict limits be placed on the government’s ability to subsequently search that data.\textsuperscript{16}

This Article attempts to clarify the existing law on computer searches and lays out a framework for how such searches should be approached in the future. Part II of this Article examines the current state of the law regarding computer searches and explores the two contrasting approaches to the problem. Next, it addresses what protections are currently available with respect to maintaining the privacy and confidentiality of medical and legal records which are seized in an investigation. It also examines how, and under what circumstances, an aggrieved party may seek return of seized property. Part III provides an in-depth analysis of and commentary on the CDT decision. Part IV discusses how courts view the plain view doctrine’s operation in the digital search realm and addresses whether the doctrine should apply at all in this context. Finally, in Part V, this Article provides some recommendations as to how current search and seizure principles should be applied to govern computer searches in the future.

II. DISCUSSION OF APPLICABLE FOURTH AMENDMENT PROVISIONS TO COMPUTER SEARCHES AND SEIZURES

The current state of the law surrounding computer searches is a bit like parenting. There are lots of ideas as to how it should occur but no clear agreement as to the right answer. Some courts have attempted to analogize computers to closed containers or file cabinets in an attempt to meld

\textsuperscript{15} CDT, 473 F.3d at 935.
\textsuperscript{16} Id. at 965 (Thomas, J. dissenting).
computer searches into existing Fourth Amendment jurisprudence.\textsuperscript{17} Other courts have held that computers require a “special approach” to the question and have imposed new restrictions on such searches which are not present in areas outside this context.\textsuperscript{18} Such legal gymnastics are unwarranted. To borrow a phrase from Todd Bertuzzi, a computer “is what it is.”\textsuperscript{19} Rather than simply being akin to a container or file cabinet, a computer is much more. It is anything and everything a user wants it to be—a file cabinet containing thousands of personal files or business records, a personal accountant, a photo album, a music or movie player, a virtual desk complete with calendar and Rolodex, a research librarian, or a video game machine. In effect, the search of a computer is in some ways no different today than a search of a house or an office desk used to be; it just can be accomplished in one-stop shopping.

Most computer searches occur using a standard protocol. First, the computer is examined to see if it is in proper working order or has any physical damage.\textsuperscript{20} Next, the hard drive is removed, inspected, and connected to a forensic computer for examination.\textsuperscript{21} A write-blocking device is installed between the suspect drive and the forensic computer to prevent the examiner from accidentally writing information onto the suspect drive.\textsuperscript{22} A bitstream copy of the hard drive is then made, including blank space.\textsuperscript{23} The copy of the hard drive information is then analyzed by using software such as EnCase, which allows investigators to examine the contents of each file.\textsuperscript{24}

A. WARRANT SPECIFICITY: PARTICULARITY AND BREADTH

In order to understand the rules governing computer searches, it is first necessary to discuss the basic principles governing execution of search warrants generally. To be reasonable under the Fourth Amendment, a

\textsuperscript{17} See discussion infra United States v. Hill, 322 F. Supp. 2d 1081 (C.D. Cal. 2004).
\textsuperscript{18} See discussion infra United States v. Carey, 172 F.3d 1268, 1275 n.7 (10th Cir. 1999).
\textsuperscript{20} Telephone Interview with Collin Reese, Agent, Colo. Bureau of Investigation (July 2, 2007).
\textsuperscript{21} Id.
\textsuperscript{22} Id.
\textsuperscript{23} Id.
\textsuperscript{24} Id.
warrant must be specific. However, a warrant need only be specific enough to "permit the executing officer to exercise reasonable, rational and informed discretion and judgment in selecting what should be seized." "Specificity has two aspects: particularity and breadth."

First, a warrant is said to be sufficiently particular if it sets forth "general classifications of the items to be seized" which would enable the executing officer to "ascertain and identify with reasonable certainty" the items that he is authorized to seize. Depending upon the complexity of the crimes under investigation, the court's focus should be on whether the warrant is as particular as reasonably could be expected under the circumstances. Given that the search of a hard drive or other storage media is inherently complex, some courts have found warrants to search computers meet the particularity requirement even though they may only generally describe the computer or storage media to be searched. As will be further explored below, this line of decisions recognizes that it is often difficult for officers to precisely pinpoint the location of the desired evidence when it is in digital form. This is because such evidence may be contained in files on the hard drive of the computer or on various storage media such as CD-ROMs or jump drives. It may even be hidden from view entirely by encryption or other security methods. Other courts have followed a different approach, instead requiring that warrants for computer searches be limited more narrowly to specifically defined files or media and to specific types of material and evidence.

Second, breadth is defined as the "requirement that there be probable cause to seize the particular thing named in the warrant." A warrant is thus overbroad if it includes items for which there is no probable cause to

26 United States v. Triumph Capital Group, Inc., 211 F.R.D. 31, 57 (D. Conn. 2002) (finding warrant that sought access to attorney's laptop was sufficiently particular because it detailed the nature of criminal activity and types of files to be seized).
27 In re Grand Jury Subpoenas, 926 F.2d 847, 856 (9th Cir. 1991).
28 United States v. George, 975 F.2d 72, 75 (2d Cir. 1992).
29 Triumph Capital, 211 F.R.D. at 57 (citing Andresen v. Maryland, 427 U.S. 463, 480 n.10 (1976)).
30 United States v. Lacy, 119 F.3d 742, 746-47 (9th Cir. 1997) (upholding general description of computer equipment which authorized blanket seizure of computer equipment where officers knew that the defendant had downloaded images of child pornography but did not know whether they were stored on the hard drive or disks); Triumph Capital, 211 F.R.D. at 58.
31 Interview with Collin Reese, supra note 20.
32 United States v. Riccardi, 405 F.3d 852, 862 (10th Cir. 2005).
33 In re Grand Jury Subpoenas, 926 F.2d 847, 857 (9th Cir. 1991).
In cases involving complex investigations, typified by the need to assemble a “paper puzzle,” courts have been more tolerant of broad warrant provisions. Where an item of interest is contained in a large collection of files or documents, all items in the set may be inspected during a search, provided that “specific guidelines for identifying the documents sought are provided in the search warrant.”

B. THE CAREY/WINICK DOCTRINE

Because of a computer’s massive storage capacity, some courts have been loath to authorize broad searches which allow agents seeming unfettered discretion in deciding what files to seize and how they should be searched. The Tenth Circuit has been the most ardent proponent of this “special approach” to computer searches. The court first outlined this doctrine in United States v. Carey. There, government agents seized two personal computers while conducting a search for evidence of drug possession and drug transactions. After obtaining a second warrant to search the computer files, a detective and a computer technician viewed the directories on the hard drives and then downloaded and printed them. The detective proceeded to use key word searches of text files, which did not produce any evidence related to drug use or drug transactions but did disclose many files with sexually suggestive titles and a .jpg extension. The detective did not know what the jpeg files were, but testified that the image files could have contained evidence relating to the drug charges.

Upon opening the first JPG file, the detective discovered what he believed to be child pornography. He then downloaded 244 more image files and continued to open and view a sampling of them. The Tenth

34 Triumph Capital, 211 F.R.D. at 59 (citing Davis v. Gracey, 111 F.3d 1472, 1478 (10th Cir. 1997)) (finding warrant affidavit contained sufficient allegations of defendant’s illegal campaign finance activities and intent to purge the entire hard drive to establish probable cause for warrant).
35 See United States v. Wuagneux, 683 F.2d 1343, 1349 (11th Cir. 1982).
36 United States v. Tamura, 694 F.2d 591, 595 (9th Cir. 1982). Specifics of the Tamura case are discussed infra note 57.
37 See United States v. Carey, 172 F.3d 1268, 1276 (10th Cir. 1999) (ruling that the search of computer directories containing pornographic image files exceeded the scope of a warrant permitting the search of a computer for evidence pertaining to drug transactions).
38 Id. at 1268.
39 Id. at 1270.
40 Id.
41 Id.
42 Id. at 1270-71.
43 Id. at 1271.
44 Id.
Circuit held that the detective’s search of all but the first image file exceeded the scope of the search warrant.\textsuperscript{45} The court stated that the file cabinet analogy may be “inadequate” in the computer context and noted that a “special approach” is needed instead.\textsuperscript{46} It required that the warrant demonstrate that such mislabeling is anticipated before such a general search of the hard drive would be permitted:

While the scenario is likely, it is not representative of the facts of this case. This is not a case in which ambiguously labeled files were contained in the hard drive directory. It is not a case in which the officers had to open each file drawer before discovering its contents. Even if we employ the file cabinet theory, the testimony of Detective Lewis makes the analogy inapposite because he stated he knew, or at least had probable cause to know, each drawer was properly labeled and its contents were clearly described in the label.\textsuperscript{47}

The court also noted that because the computers had been removed from the home, there were no “exigent circumstances” justifying a general rummaging through the files on the hard drive.\textsuperscript{48} The court found that investigators can generally employ “several methods” such as key word searches or directory or file titles to avoid searching file types not identified in the warrant.\textsuperscript{49} Thus, the court criticized the officers’ failure to use the information gained through the key word search (no evidence of drug transactions) to limit their search appropriately.\textsuperscript{50}

The court’s approach in \textit{Carey} has at its genesis an article written by Raphael Winick in 1994.\textsuperscript{51} Winick theorized that because computers can store “massive quantities” of information, they are fundamentally different from closed containers which frame much of the traditional Fourth Amendment analysis.\textsuperscript{52} Therefore, according to Winick, a “different analysis” under the Fourth Amendment is mandated.\textsuperscript{53} This approach contains two steps. The first requires that officers apply for permission to remove a computer and storage media from the premises.\textsuperscript{54} If that permission is granted, the officers must then obtain a second warrant,

\begin{itemize}
\item \textsuperscript{45} \textit{Id.} at 1276. Based on the officer’s testimony that the discovery of the first pornographic image was inadvertent, the court limited its suppression ruling to the search of all subsequent image files. \textit{Id.} at 1273 n.4.
\item \textsuperscript{46} \textit{Id.} at 1275 n.7.
\item \textsuperscript{47} \textit{Id.} at 1274-75.
\item \textsuperscript{48} \textit{Id.} at 1275-76.
\item \textsuperscript{49} \textit{Id.} at 1276.
\item \textsuperscript{50} \textit{Id.}
\item \textsuperscript{52} \textit{Id.} at 89.
\item \textsuperscript{53} \textit{Id.}
\item \textsuperscript{54} \textit{Id.} at 107.
\end{itemize}
specifying exactly what types of files are to be searched and the precise methods which will be used to search those files.55

The first prong of Winick’s test is essentially an adoption of the intermingled document doctrine, first espoused in United States v. Tamura.56 In Tamura, the court objected to the “wholesale seizure” of entire filing cabinets of records without any efforts to limit the seizure of unrelated material.57 The Tamura court suggested that, where it was necessary to seize intermingled documents, the documents should be “sealed and held pending approval by a magistrate of a further search.”58 Winick proposed a similar procedure for computer searches:

This rule holds that where officers come across relevant documents 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 through the documents. If the officers know prior to the search that transporting large quantities of documents or hardware is likely, they can apply to the magistrate issuing the warrant for permission to remove such material; permission should be granted only when on-site sorting of relevant and irrelevant material is infeasible and no other practical alternative exists.59

If removal of computer equipment and media is warranted, Winick believed officers should not be allowed to conduct a full review of the files contained on the storage media based simply on a “vague allegation” that such review of all files was necessary in all cases.60 Instead, he recommended that officers be forced to use such methods as keyword searches to identify and read through only those files which “there is reason to believe contain relevant information.”61

55 Id. at 108.
56 694 F.2d 591, 595-96 (9th Cir. 1982).
57 Id. at 594-95. In Tamura, the warrant authorized the seizure of three specific categories of business records. To locate the relevant records, the agents had to: (1) review the computer printout, (2) locate the voucher that corresponded to a particular payment recorded on the printout, and (3) find the check that corresponded to the voucher. Id. The agents followed this procedure for a short time but quickly concluded that it would take too long unless the employees helped them. Id. at 595. The agents threatened to seize all of the company’s accounting records for the previous ten years if such assistance was not forthcoming. Id. When the employees refused, the agents seized eleven boxes of printouts, thirty-four file drawers of vouchers, and seventeen drawers of canceled checks. Id.
58 Id. at 595-96.
59 Winick, supra note 51, at 105-06.
60 Id. at 108-09.
61 Id. at 108.
Apart from the Tenth Circuit, only a handful of courts have adopted Winick's two-pronged approach. In *In re the Search of 3817 W. West End*, a magistrate judge for the Northern District of Illinois approved a warrant to seize computers but refused to permit the government to search the computer files until it provided a specific search protocol. The court held that a generalized search of the computer was inappropriate because of the "substantial likelihood" that it contained unrelated personal documents intermingled with those related to tax fraud. The court relied on the fact that computer searches could be limited by key words or to text or graphics files. While noting that these tools are not the "exclusive means" for conducting computer searches, the court found that their existence "demonstrates the ability of the government to be more targeted in its review of computer information than it can be when reviewing hard copy documents in a file cabinet."

C. A NEW "OLD" APPROACH TO COMPUTER SEARCHES

Winick's approach has come under increasing fire. Criminals have begun using more sophisticated methods of concealing files and data which can defeat the use of simple key word searches. For example, file types or extensions can be changed to hide the true identify or content of the file. Incriminating files may also be deleted or encrypted. One commentator, David Ziff, suggests that the better approach to computer searches is to "import the same rules and standards used for searches of physical records or documents." Ziff argues that any type of file, regardless of whether it is in a small stack of papers or in a computer containing thousands of files, should receive the same level of protection. "If courts have approved of the protection given to individual documents in the stack of twenty, there is no reason to apply a different test simply because the stack has grown."

---

64 Id. at 958.
65 Id. at 959. Of course, this approach assumes that the government investigator must rely on the file name or extension in conducting a computer search, but conversely, be free to disregard such labels when searching a file cabinet.
67 Id.
69 Id. at 869.
Another commentator, Orin S. Kerr, has recently written a series of articles advocating that the Carey/Winick approach be rejected in favor of a more fluid approach which accommodates the interests of both parties.\textsuperscript{70} He notes that computer searches conducted in the virtual world are inherently different from those conducted in the traditional physical sense because “digital evidence searches generally occur at both a ‘logical’ or ‘virtual’ level and a ‘physical’ level.”\textsuperscript{71} According to Kerr, this “distinction between physical searches and logical searches is fundamental in computer forensics.”\textsuperscript{72} He explains the difference between logical and physical searches as follows:

Consider a search for a picture file believed to be evidence of a crime. An examiner might begin by conducting a logical search of the hard drive for files with extensions known to be used for image files, such as “.jpg” . . . .

This procedure sounds easy, but ordinarily does not suffice. It is easy to change the extension of a file. To hide a picture, a user might take a file saved with a “.jpg” extension and resave it with an extension common to a different kind of file, such as “.doc” or “.wpd.” A search for picture files based on the logical file extensions will no longer locate the file. Instead, the analyst will have to conduct a search at a physical instead of a logical level. Software can locate image files at a physical level by searching for file headers characteristic of known types of picture files. . . . The file header remains unchanged regardless of the extension placed on the file, allowing a physical search to uncover picture files that a logical search would not locate.\textsuperscript{73} Consequently, Kerr notes officers are often forced to examine the “entire digital haystack to find the needle.”\textsuperscript{74}

Because files can be mislabeled, hidden, or deleted, a forensic investigator can never be sure ahead of time which type of search may be required. Due to forensic examiners’ inability to forecast accurately what course a digital search will take, Kerr criticizes the logic underlying the Carey/Winick approach as “deeply flawed.”\textsuperscript{75} Instead, he proposes that forensic examiners, not magistrates, are the persons who are best able to dictate the search parameters:

\textsuperscript{71} Kerr, supra note 66, at 544.
\textsuperscript{72} Id. A logical search is based on the contents of the files and the file types found on the hard drive as delineated by the operating system, while a physical search identifies and recovers data “across the entire physical drive without regard to the file system.” Id.
\textsuperscript{73} Id. at 544-45 (footnotes omitted).
\textsuperscript{74} Kerr, Digital Evidence, supra note 70, at 304.
\textsuperscript{75} Kerr, supra note 66, at 572.
It is difficult to know what the particular search requires and what tools are best suited to find the evidence without first taking a look at the files on the hard drive. In a sense, the forensics process is a bit like surgery: the doctor may not know how best to proceed until he opens up the patient and takes a look. The ability to target information described in a warrant is highly contingent on a number of factors that are difficult or even impossible to predict ex ante.

In light of these difficulties, magistrate judges are poorly equipped to evaluate whether a particular search protocol is the fastest and most targeted way of locating evidence stored on a hard drive.\footnote{Id. at 575 (footnotes omitted).}

Another criticism of the Carey/Winick approach is that it does not take into account the need for an officer to exercise his or her judgment in determining the relevance of a file's contents.\footnote{Thomas K. Clancy, The Fourth Amendment Aspects of Computer Searches and Seizures: A Perspective and a Primer, 75 MISS. L.J. 193, 211 (2005) (citing Susan W. Brenner & Barbara A. Frederiksen, Computer Searches and Seizures: Some Unresolved Issues, 8 MICH. TELECOMM. & TECH. L. REV. 39, 60-62 (2002)).} Thomas Clancy points out that search protocols are context insensitive, and as a result, they cannot always predict a document's incriminatory character or relevance to an investigation.\footnote{Clancy cites that if "either the data encoding or the alleged criminal activity is complex in nature, human judgment will be required to determine the evidentiary value of specific electronic documents and whether the documents fall within the scope of the warrant." Id. at 211.} An investigator often must review the contents of a file and compare it to some known standard before forming an opinion as to its usefulness. For example, in the context of a Medicare fraud investigation, a key word search could be used to pull up all files pertaining to a particular diagnosis code or treatment type. However, such a search may cast too wide a net. The officer would still have to examine the contents of each file to determine the authenticity of the injury or reasonableness of the fee charged for the service provided.

Ziff proposes that the discretion of the officer should be checked, not by search protocols, but instead by vigilantly defining and monitoring the scope of the warrant:

\begin{quote}
[T]he ability to examine documents does not give searching officers the authority to read the contents of any given file. Rather, the officers' authority extends only so far as necessary to determine if a given document is within the scope of the warrant. Once the examination reaches the point where it is clear that the document is outside the scope of the warrant, the officer no longer has authority under the warrant to continue reading the document.\footnote{Ziff, supra note 68, at 862 (footnotes omitted).}
\end{quote}

Clancy also rejects the notion that there should be special rules for electronic evidence containers. Otherwise, in his view, filing cabinets,
diaries, books, floppy drives, hard drives, paper bags, and other storage devices would “all require different rules.”

In a recent line of cases, courts outside the Tenth Circuit have generally declined to follow the Carey/Winick “special approach.” These courts have recognized the difficulties inherent in conducting digital searches and thus have been reluctant to tie the hands of investigators by making them comply with rigid, pre-approved search protocols. Instead, the courts have focused on the reasonableness of the government’s actions under the circumstances.

For example, in United States v. Hill, the Ninth Circuit adopted the first prong of the Winick approach (the intermingled document doctrine) to limit the seizure of computer hardware and media, but it refused to adopt the second part to correspondingly limit agents’ search of the data. In Hill, a computer technician tipped off the police to what she believed to be child pornography on the defendant’s computer. The officers sought and obtained a warrant for the computer and all storage media, but the defendant picked up his computer before the warrant could be executed. The police then executed a second warrant on defendant’s home and seized storage media from his bedroom. A subsequent search of the media revealed images of child pornography.
The defendant argued that the search was overbroad because it (1) allowed the seizure of all computer media without requiring inspection at the scene, and (2) it placed no limits or controls on the search methodology the police used in analyzing the seized media. Judge Kozinski, sitting by designation, rejected defendant’s contentions. First, he found that inspection and sorting of the media on site would be impractical because it would: (1) pose a significant burden on smaller agencies to continuously update their technology, (2) pose a serious risk of damaging or compromising the integrity of evidence at the scene, and (3) take an inordinately long time to accomplish. Thus, the court concluded that the police “were not required to examine defendant’s electronic storage media at the scene” for the presence of child pornography, but instead “were entitled to seize all such media and take them to the police station for examination by an expert.”

Judge Kozinski found that Tamura did not require a different result. He concluded that, even in the absence of a specific showing that computer files were difficult to sort on-site, the procedures outlined in Tamura for seizure of intermingled evidence had been complied with:

The warrant here authorized precisely such a seizure of intermingled materials that are difficult and time-consuming to separate on-site. That the officer seeking the warrant did not make a specific showing to this effect is of no consequence: The difficulties of examining and separating electronic media at the scene are well known. It is doubtless with these considerations in mind that the state court judge authorized seizure of all of defendant’s storage media, not merely those containing contraband or evidence of a crime.

The Ninth Circuit did not approve of Judge Kozinski’s conclusion on this point, however. The court held that the warrant was overbroad in the absence of an explanatory affidavit as to why such a blanket seizure of computer equipment was necessary. The court noted that the government does not have an “automatic blank check” in such circumstances but must instead “demonstrate to the magistrate factually why such a broad search and seizure authority is reasonable.” The court noted that the officers’ supporting affidavits play a “critical role” in determining whether this threshold has been met.

---

87 Id. at 1084.
88 Id. at 1089.
89 Id.
90 Id. at 1090.
91 United States v. Hill, 459 F.3d 966, 979 (9th Cir. 2006).
92 Id. at 975.
93 Id. The content of the affidavit seems to be the critical factor in the eyes of the Ninth Circuit. A few weeks earlier, it upheld a similarly broad warrant against an overbreadth
Conversely, the Ninth Circuit did uphold the second part of Judge Kozinski’s opinion, adopting his analysis verbatim. Judge Kozinski rejected defendant’s contention that the search of computer media should have been limited to keywords or file extensions associated with child pornography. Because such photographs can be hidden in all types of files, he found the proposed search methodology to be unreasonable. He likened the situation to forcing officers to ignore plastic bags which contained a white powdery substance suspected of being cocaine simply because they were labeled “flour” or “talcum powder.”

Other courts have also rejected the use of rigid search protocols. In United States v. Adjani, the Ninth Circuit refused to limit the government’s search of emails to specific email addresses or search terms. The court reasoned that because file names can be easily disguised or renamed, the government “should not be required to trust the suspect’s self-labeling when executing a warrant.” Similarly, in United States v. Gray, the court approved the opening of picture files containing child pornography during an unrelated search of defendant’s computer for evidence pertaining to his unauthorized access of a government computer. Even though investigators did not anticipate finding relevant evidence in the image files, the court approved their inclusion in the search. It reasoned that an agent conducting a search of a computer is entitled to examine “all files on the computer” to determine whether they fall within the scope of the warrant.

challenge in United States v. Adjani, 452 F.3d 1140 (9th Cir. 2006). In contrast to the affidavit in Hill, the court noted that the supporting affidavit attached to the warrant application contained “a detailed computer search protocol, including instructions as to when computers should be searched on-site rather than taken off-site and procedures for screening the data to determine what data could be searched and seized under the terms of the warrant.” Id. at 1149 n.7.

Hill, 459 F.3d at 968.

Hill, 322 F. Supp. 2d at 1088.

Id. at 1089.

Id. at 1090.

See United States v. Maali, 346 F. Supp. 2d 1226, 1245 (M.D. Fla. 2004) (holding that “the lack of a detailed computer ‘search strategy’ does not render the warrant deficient as to the search and seizure of computers”); United States v. Triumph Capital Group, Inc., 211 F.R.D. 31, 47 (D. Conn. 2002) (holding that because computer searches are technical and complex, they cannot be limited to precise, specific steps or only one permissible method); Rosa v. Commonwealth, 628 S.E.2d 92, 96 (Va. Ct. App. 2006) (holding that “officers may glance at files with various extensions in order to ascertain whether or not the files fall within the purview of the warrant”).

452 F.3d 1140, 1149-50 (9th Cir. 2006).

Id. at 1150.


102 Id.

103 Id.
The court likened the situation to the search of voluminous paper records or files, which permits a cursory examination of all files to "determine whether they fall into the category of those papers covered by the search warrant."\textsuperscript{104} Furthermore, despite testimony that it was possible to use the search program to determine whether a file contained pictures or text without opening it, the court concluded that it was "unreasonable" to force the government to always use the most advanced search techniques.\textsuperscript{105}

D. LIMITATIONS ON SEARCHES OF CONFIDENTIAL BUSINESS RECORDS

The search of business computers may require different rules, however, because such searches implicate unique concerns. Business computers may contain thousands of files and records of individuals or entities unrelated to the target of the investigation. This is particularly true of searches of innocent third parties, such as medical or law offices, which are merely the repositories for the records relevant to the investigation. In these situations, special attention needs to be paid by investigators so as to not unnecessarily disturb privacy and confidentiality rights in the unrelated records.

First, law enforcement officers should follow Department of Justice ("DOJ") regulations that dictate that agents should apply for search warrants (in lieu of issuing subpoenas) only in exceptional circumstances.\textsuperscript{106} Second, if a search warrant is necessary, officers should ensure that the affidavit in support of it contains sufficient detail as to what particular files and records are being sought to prevent irrelevant records from being swept up in the search. Finally, special masters or taint teams should be used to review confidential material before it is turned over to investigators.\textsuperscript{107}

1. Department of Justice Regulations

Pursuant to the Privacy Protection Act of 1980, the DOJ has issued regulations aimed at protecting such privacy concerns.\textsuperscript{108} The regulations provide that no federal officer should apply for a search warrant to seize documentary materials believed to be in the possession of "a disinterested

\textsuperscript{104} Id. at 528 (citing United States v. Kufroch, 997 F. Supp. 246, 264 (D. Conn. 1997)).
\textsuperscript{105} Id. at 530 n.8.
\textsuperscript{106} See 28 C.F.R. § 59.4 (1981) and discussion of this regulation infra Part II.D.1.
\textsuperscript{107} A taint team is composed of a different group of agents which is separate and apart from the main group of investigators. The team reviews the seized material and separates those documents which may be subject to privilege. It then turns over to the investigative team only those documents it has determined to be nonprivileged. A "Chinese Wall" is then erected between the taint team and the investigative team. See infra Part II.D.3.
third party” unless the use of less intrusive means of obtaining the documents such as a subpoena would “substantially jeopardize” the availability or usefulness of the information sought.\textsuperscript{109} In determining whether the use of such means would “substantially jeopardize” the availability or usefulness of the materials, the investigator should consider, among other factors, the likelihood of destruction of the material or the immediacy of the government’s need for it.\textsuperscript{110}

A disinterested third party is defined as a person or organization “not reasonably believed to be . . . a suspect” in the criminal offense to which the materials relate or “related by blood or marriage to such a suspect.”\textsuperscript{111} Documentary materials include items such as audio and video tapes, photographs, or materials upon which information is electronically or magnetically recorded.\textsuperscript{112} The regulations also provide that search warrants should not be executed on third-party law offices, medical offices, or clergy, absent similar concerns.\textsuperscript{113} If a search of such persons or offices is

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{109} 28 C.F.R. § 59.4.
\item \textsuperscript{110} Factors to consider whether the use of less intrusive means will “substantially jeopardize” the availability or usefulness of the material include:
\begin{enumerate}
\item Whether it appears the use of a subpoena or other alternative . . . would be likely to result in the destruction, alteration, concealment, or transfer of the materials sought; considerations, among others, bearing on this issue may include:
\begin{enumerate}
\item Whether a suspect has access to the materials sought;
\item Whether there is a close relationship of friendship, loyalty, or sympathy between the possessor of the materials and a suspect;
\item Whether the possessor of the materials is under the domination or control of a suspect;
\item Whether the possessor of the materials has an interest in preventing the disclosure of the materials to the government;
\end{enumerate}
\end{enumerate}
\item The immediacy of the government’s need to obtain the materials; considerations, among others, bearing on this issue may include:
\begin{enumerate}
\item Whether the immediate seizure of the materials is necessary to prevent injury to persons or property;
\item Whether the prompt seizure of the materials is necessary to preserve their evidentiary value;
\item Whether delay in obtaining the materials would significantly jeopardize an ongoing investigation or prosecution . . . .
\end{enumerate}
\end{enumerate}
\item \textsuperscript{111} Id. § 59.2(b)-(b)(1).
\item \textsuperscript{112} Id. § 59.2(c).
\item \textsuperscript{113} Section 59.4(b)(4) provides that warrants should not be issued in such circumstances unless:
\begin{enumerate}
\item It appears that the use of a subpoena, summons, request or other less intrusive alternative means of obtaining the materials would substantially jeopardize the availability or usefulness of the materials sought;
\end{enumerate}
\end{enumerate}
\end{footnotesize}
conducted, it should be executed in a manner so as to "minimize" scrutiny of confidential materials. In addition, the regulations prohibit using a challenge to a subpoena or other legal process as a "legitimate basis" for the procurement of a search warrant. However, failure to comply with the terms of these regulations is not an issue which may be litigated or form the basis for the suppression or exclusion of evidence.

Relatively few cases have explored the limitations these regulations impose on searches of medical or law offices. In Klitzman, Klitzman, and Gallagher v. Krut, the Third Circuit held that a search warrant, which authorized the seizure of hundreds of files and most of a law firm's business records, was overbroad in light of the fact that only one of the firm's attorneys was a suspect. While finding that searches of law offices were not per se unreasonable, the court chastised the government because it made no attempt to limit the seizure of files to materials involving the fraudulent scheme under investigation. Referencing the Privacy Protection Act and the DOJ regulations, the court stated that the government should have followed them instead of acting as if they were "nonexistent." The court suggested that in such situations a special master can be appointed to review in camera any documents that a law firm objects to producing.

Conversely, where adequate protections are put in place to minimize intrusions on privacy, courts have approved the seizure of records from medical and legal offices. For example, in In re Impounded Case, the Third Circuit did uphold the seizure of files and other documents from a law firm. The court distinguished Klitzman on the ground that the warrant specified that only certain types of financial documents were to be seized. It also found that any confidentiality concerns were "sufficiently protected"

---

(iii) The application for the warrant has been approved as provided in paragraph (b)(2) of this section.

Id. § 59.4(b)(2).

118 Id. at 962.

120 Id.
by the procedures requiring the prosecution to seek further leave of court before inspecting the files.\textsuperscript{122}

Florida courts have required that medical records of patients seized during the execution of a search warrant be sealed pending notification of the patients.\textsuperscript{123} In \textit{State v. Viatical Services, Inc.}, the court mandated that if the medical records of innocent third parties are seized pursuant to a warrant, the records must be sealed pending a post-seizure hearing on the issue of the right to privacy.\textsuperscript{124}

\section*{2. Specificity of Warrants}

In such situations where warrants are deemed to be necessary, the warrant must specify what particular medical or legal records are sought. For example, in \textit{United States v. Abrams},\textsuperscript{125} the First Circuit held that a warrant, which permitted seizure of all of a doctor’s Medicare records, was void for lack of particularity because it failed to specify what time period the warrant covered or what specific records were to be seized. The court criticized investigators for failing to make any attempt to separate bona fide records from fraudulent ones.\textsuperscript{126} A division of the Pennsylvania Superior Court reached a similar conclusion in \textit{Commonwealth v. Santner}.\textsuperscript{127} There, the officers seized 3600 files but only fifty were introduced as evidence at trial.\textsuperscript{128} The court found that the officers could have narrowly tailored the warrant because “they had an excellent idea of what specific information they needed, and could easily have made the warrant much less broad.”\textsuperscript{129}

\section*{3. The Use of Taint Teams to Protect Confidentiality}

One somewhat controversial approach to the search of law firm has been the utilization of “taint teams” in lieu of in camera review.\textsuperscript{130} In essence, attorneys and investigators not associated with the main investigation conduct the search of the law office separate and independent from the primary investigators and prosecutors.\textsuperscript{131} The taint team reviews the seized documents for privileged information and separates it from non-
privileged material. The team returns privileged information to the law office but turns over all other material to the investigation. A "Chinese Wall" is then erected between the taint team members and the primary investigation and prosecution team.

In theory, the use of a taint team has some distinct advantages. It relieves the trial court of much of the burden of sifting through the entire record to look for privileged information. Instead, the court may only have to review a few disputed documents for privilege. The obvious drawback to this approach is that it exposes potentially confidential information to the eyes of the taint team. It also relies heavily on the integrity of the personnel involved not to breach the Chinese Wall.

For these reasons, court response has been equivocal to the use of taint teams. In In re Search of 5444 Westheimer Road, a Southern District of Texas court reasoned that the use of a taint team was a reasonable accommodation to the problem of separating confidential information from law office records. There, the FBI seized 118 boxes of information and imaged four computer hard drives from a corporate office. The court found that the use of a taint team would "sufficiently protect any potentially privileged documents" and would allow for expeditious review of all seized documents. It noted that its decision was based on the presumption that government investigators will "conduct themselves with integrity."

---

132 Id.
133 Id.
134 Id. A Chinese Wall is essentially a self-imposed gag order. In theory, individuals on the taint team and investigation team do not talk to one another regarding details of the case. Such arrangements are often used to prevent attorneys transferring from one law firm to another from talking about cases they had previously handled at their old firms.

135 See Hicks v. Bush, 452 F. Supp. 2d 88, 103 (D.D.C. 2006) (finding exigent circumstances existed justifying use of taint team where government had legitimate interest in quickly reviewing materials of suicidal prisoners held at Guantanamo Bay facility); In re Search of 5444 Westheimer Road, H-06-238, 2006 WL 1881370, at *3 (S.D. Tex. July 6, 2006) (finding use of taint team approved to sort privileged material from corporate files seized pursuant to warrant). But see United States v. Stewart, 02CR396JGK, 2002 WL 1300059, at *8 (S.D.N.Y. June 11, 2002) (finding search of criminal defense attorney's office raises Sixth Amendment concerns not present in the search of the offices of a civil litigation attorney so the use of a Chinese Wall is "highly questionable" and should be discouraged in the context of a criminal prosecution); In Re Search Warrant of Law Offices, 153 F.R.D. 55, 59 (S.D.N.Y. 1994) (noting the use of taint teams in criminal prosecutions is "highly questionable").

136 2006 WL 1881370, at *3.
137 Id. at *1.
138 Id. at *3.
139 Id. (quoting United States v. Grant, No. 04 CR 207BSJ, 2004 WL 1171258, at *3 (S.D.N.Y. May 25, 2004)).
In contrast, in *United States v. Neill*, the District Court for the District of Columbia heavily criticized the use of taint teams. While it declined to hold that the government’s invasion of the attorney-client privilege rose to the level of a constitutional violation, it did find that the government’s interference with the privilege was intentional:

Where the government chooses to take matters into its own hands rather than using the more traditional alternatives of submitting disputed documents under seal for *in camera* review by a neutral and detached magistrate or by court-appointed special masters (citations omitted), it bears the burden to rebut the presumption that tainted material was provided to the prosecution team.141

However, while the court noted that the use of taint teams is “unwise” and creates an “appearance of unfairness,” it found their use does not offend the Constitution absent a showing of harm resulting from disclosure of the privileged information.142

The Sixth Circuit summed up the problems associated with taint teams as follows:

[T]aint teams present inevitable, and reasonably foreseeable, risks to privilege, for they have been implicated in the past in leaks of confidential information to prosecutors. That is to say, the government taint team may also have an interest in preserving the privilege, but it also possesses a conflicting interest in pursuing the investigation, and, human nature being what it is, occasionally some taint team attorneys will make mistakes or violate their ethical obligations. It is thus logical to suppose that taint teams pose a serious risk to holders of the privilege, and this supposition is supported by past experience.143

In particular, the court referenced an incident where a taint team turned over tapes of attorney-client conversations, which were obviously protected by attorney-client privilege, to members of the investigating team.144 The court noted this incident highlights the obvious flaw in the taint team procedure: “[T]he government’s fox is left in charge of the appellants’ henhouse, and may err by neglect or malice, as well as by honest differences of opinion.”145

Courts have distinguished the use of taint teams to review documents produced under subpoena as opposed to those seized under exigent circumstances such as a search warrant. In *Neill*, the court concluded that where the government officials have already obtained possession of the documents pursuant to a warrant, the use of a taint team to “sift the wheat

---

141 *Id.* at 840-41.
142 *Id.* at 841 n.14.
143 *In re* Grand Jury Subpoenas, 454 F.3d 511, 523 (6th Cir. 2006).
144 *Id.* at 523 (citing United States v. Noriega, 764 F. Supp. 1480 (S.D. Fla. 1991)).
145 *Id.*
from the chaff’ is “respectful of, rather than injurious to,” the attorney-client privilege. In *Hicks v. Bush*, the court held that the use of a taint team was appropriate where the government was investigating the suicidal deaths of three detainees. The court found that the government’s legitimate penological interests of maintaining inmate safety and thwarting prison further disruption outweighed the relatively minor chilling effect on the attorney-client privilege. It concluded that no other alternative such as magistrate review or the appointment of a special master could accomplish the necessary review in a reasonable amount of time.

Even where the use of taint teams has been approved, courts still require the government to provide some procedure for review and challenge of the non-privileged documents before they are turned over to prosecutors. For example, in *United States v. SDI Future Health, Inc.*, the court doubted that (had it been challenged) the government’s taint team procedure would have been approved because it failed to provide notice to the defendant of the taint team’s privilege decisions or to afford it an opportunity to challenge them in court before the documents were provided to the prosecution team. Conversely, in approving the use of a taint team, the *Westheimer* court pointed to the fact that the defendant would have an opportunity to challenge the government’s privilege determinations before any material was turned over to the prosecution team.

E. RULE 41(G) MOTIONS FOR RETURN OF PROPERTY

Once the government has seized computer files and records pursuant to a search warrant, the next question that must be answered is what remedy, if any, the aggrieved party has to seek return of that information. A party who alleges that property was unlawfully seized during execution of a search warrant has two basic options. He may file a motion to suppress the evidence (assuming it is incriminatory and being offered against him in a criminal case), or he may move for its return. An aggrieved party may

---

146 Id. at 522 (citing United States v. Abbell, 914 F. Supp. 519 (S.D. Fla. 1995)).
148 Id.
149 Id.
152 See FED. R. CRIM. P. 12 (2006); FED. R. CRIM. P. 41(g) (2006). Those individuals who have not yet been charged with a crime or who are disinterested third parties (i.e., they are not the target of the investigation) have only one option—seeking return of the property pursuant to rule. As discussed below, in such a case the movant must demonstrate that equitable principles favor him before such a motion will be heard.
also seek return of lawfully seized property on the ground that he is being unreasonably deprived of it. While Rule 12 of the Federal Rules of Criminal Procedure governs motions to suppress, Rule 41(g) provides for motions for return of property as follows:

A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return. The motion must be filed in the district where the property was seized. The court must receive evidence on any factual issue necessary to decide the motion. If it grants the motion, the court must return the property to the movant, but may impose reasonable conditions to protect access to the property and its use in later proceedings.\(^{153}\)

Many states have a similar provision.\(^{154}\) A Rule 41(g) motion may be filed either prior to indictment, or after charges have been filed, and it may be filed independently of any pending criminal or civil case.\(^{155}\)

### 1. History of Rule 41

A brief examination of the history of Rule 41 is helpful to understanding the intent behind the current rule and its practical operation. The rule has been in existence in some form since the adoption of the Federal Rules of Criminal Procedure in 1944. In 1972, the then-Rule 41(e) was first amended. The Advisory Committee Comment to the 1972 Amendments noted that the rule “provides for return of the property if (1) the person is entitled to lawful possession and (2) the seizure was illegal.”\(^{156}\) The Rule was again substantially amended in 1989.\(^{157}\) The Advisory Committee Comments to that 1989 Amendment are instructive. The primary purpose of that amendment was to address the harm that may result from “the interference with the lawful use of property by persons who are not suspected of wrongdoing.”\(^{158}\) The Committee also noted that the prior rule did not explicitly recognize the right of a property owner to obtain return of lawfully seized property where the government could protect its interests in the property through other means, such as photocopying or conditioning return on future access.\(^{159}\) Thus, the amended

---

\(^{153}\) The Rule was amended most recently in 2003. The amendments were cosmetic. The Rule was re-lettered as 41(g), and the last sentence of the prior rule, regarding treatment of post-indictment motions filed in the district of trial as motions to suppress, was deleted. Rule 41(h) now encapsulates that sentence, however, providing that a defendant may move to suppress evidence in the district of trial. *See In re Search of Law Office*, 341 F.3d 404, 408 n.3 (5th Cir. 2003).

\(^{154}\) See, e.g., COLO. R. CRIM. P. 41(e) (2006).


\(^{156}\) FED. R. CRIM. P. 41(g) advisory committee's comment, 1972 Amendment.

\(^{157}\) FED. R. CRIM. P. 41 advisory committee’s comment (1989).

\(^{158}\) FED. R. CRIM. P. 41(g) advisory committee’s comment, 1989 Amendment.

\(^{159}\) *Id.*
rule provided that "an aggrieved person may seek return of property that has been unlawfully seized, and a person whose property has been lawfully seized may seek return of property when aggrieved by the government's continued possession of it."\(^{160}\)

2. Pre-Indictment Motions to Return Property

Pre-indictment motions are to be treated as interlocutory in nature; in other words, it is "really only a request for the modification in the terms of the warrant which was issued by the magistrate judge in the first instance."\(^{161}\) Such motions are not intended to be dispositive matters and are subject to further review if the government pursues criminal charges.\(^{162}\) As a result, federal magistrate judges have jurisdiction to hear motions for return of property, just as they have jurisdiction to issue the original search warrant.\(^{163}\) Where the movant sufficiently alleges facts which enable the court to conclude that a substantial claim is presented, an evidentiary hearing must be set. It is an abuse of discretion for the court to refuse to hold a hearing "if factual issues are sufficiently raised."\(^{164}\)

Pre-indictment motions for return of property are treated as civil equitable proceedings and the court, therefore, must exercise "caution and restraint" before assuming jurisdiction to hear them.\(^{165}\) In determining whether to exercise equitable jurisdiction, courts must consider whether the movant would suffer "irreparable injury" by deprivation of the property and whether the movant has an "adequate remedy at law."\(^{166}\) Some circuits require consideration of two additional factors: (1) whether the government displayed a callous disregard for the constitutional rights of the movant; and (2) whether the movant has an individual interest in and need for the seized property.\(^{167}\)

Courts have declined to find irreparable injury, absent extraordinary circumstances. Threat of imminent indictment does not demonstrate

\(^{160}\) Id.
\(^{161}\) In re Search of 4330 N. 35th St., 142 F.R.D. 161, 164 (E.D. Wis. 1992).
\(^{162}\) Id.
\(^{165}\) In re Search of Kitty's East, 905 F.2d 1367, 1370 (10th Cir. 1990).
\(^{166}\) Id. at 1371.
\(^{167}\) Ramsden v. United States, 2 F.3d 322, 325 (9th Cir. 1993); In re Search of 4801 Flyer Ave., 879 F.2d 385, 390 (8th Cir. 1989); Richey v. Smith, 515 F.2d 1239, 1243 (5th Cir. 1975). Some jurisdictions have dropped the callous disregard requirement because proof of illegality of the search is no longer required to bring a motion under Rule 41. Kitty's East, 905 F.2d at 1371.
“irreparable harm” for purposes of a pre-indictment Rule 41(g) motion.\textsuperscript{168} Such a threat would merely be an “ordinary injury” everyone has the chance of suffering rather than an extraordinary one requiring equitable relief.\textsuperscript{169} Courts have also held that the retention of original business documents does not constitute irreparable injury if copies of the seized items are provided to the business.\textsuperscript{170} They have held, however, that the irreparable injury test is satisfied where the seizure impairs First Amendment free speech rights.\textsuperscript{171} Courts are split whether an alleged invasion of the attorney-client privilege is sufficient to satisfy this prong.\textsuperscript{172}

In order to satisfy the second prong (no adequate remedy at law), a movant must show that he will not have a fair opportunity to subsequently litigate the issue; the mere existence of a possible remedy is not sufficient to deny equitable relief.\textsuperscript{173} However, an adequate remedy will be found to exist where criminal charges are imminently pending because the propriety of the seizure can be challenged in a motion to suppress.\textsuperscript{174} Where the seized property is subject to a civil forfeiture action, an adequate remedy will be found as well because the forfeiture action provides an opportunity for the movant to be heard.\textsuperscript{175} Conversely, no adequate remedy exists where claimants are either innocent third parties who are not targets of the investigation, or who were targets, but against whom charges are not forthcoming.

\textsuperscript{168} Kitty’s East, 905 F.2d at 1371. The Fifth Circuit used to hold to the contrary, but it recently fell in line with other circuits, noting that the focus of an irreparable harm determination should be on the loss suffered from deprivation of the property, not the fact of the indictment. In re Search of Law Office, 341 F.3d 408, 415 (5th Cir. 2003).


\textsuperscript{170} Ramsden, 2 F.3d at 326.

\textsuperscript{171} Kitty’s East, 905 F.2d at 1371 (the seizure of x-rated videotapes constituted an irreparable injury because free speech rights were directly infringed).

\textsuperscript{172} Law Office, 341 F.3d at 414; In re Search of 5444 Westheimer Rd., H-06-238, 2006 WL 1881370 (S.D. Tex. July 6, 2006). In Law Office, the government seized files and records from an attorney’s home and office. 341 F.3d at 407. The court found that the defendant failed to prove it would suffer an irreparable injury because the warrant affidavit provided that a “taint team” would seize the files subject to defendant’s inspection for potentially privileged documents. Id. The court noted that defendant failed to provide any proof substantiating its allegations that the taint team viewed extensive amounts of privileged information during the search. Id. at 414. But see In re Search of 636 South 66th Terrace, 835 F. Supp. 1304, 1306 (D. Kan. 1993) (finding seizure of materials protected by the attorney-client privilege gives rise to irreparable injury because confidentiality of the materials may be lost if they are allowed to remain in the hands of investigators).

\textsuperscript{173} Interstate Cigar Co. v. United States, 928 F.2d 221, 223 (7th Cir. 1991).

\textsuperscript{174} Angel-Tores v. United States, 712 F.2d 717, 718-19 (1st Cir. 1983).

In order to satisfy the third prong, some illegality in the search usually must be found. For example, the Ninth Circuit has held that the seizure of evidence pursuant to a warrantless search, which is not justified by exigent circumstances, constitutes callous disregard. Another court declined to find callous disregard, however, where the allegations were insufficient to prove that the agent knowingly relied on false statements in submitting his affidavit for a search warrant. The final prong is satisfied where the movant can demonstrate a pressing interest in or need for return of the evidence such as where the seized documents are integral to the operation of movant’s business.

3. What Is the Proper Remedy Under Rule 41(g)?

If the court does find that it should entertain the Rule 41 motion, then it must determine what the proper remedy should be. While the Rule does not contain a standard to help determine whether property should be returned, the courts have noted that the spirit of Rule 41(g) is “one of compromise.” The comments to the Rule state that “reasonableness under all the circumstances” is the proper standard for determining the outcome of such a motion. The Committee stated that where the government has “a need for the property in an investigation or prosecution,” retention of the property is “generally reasonable,” but where its interest can be satisfied by other means, retention would be “unreasonable.” This spirit of compromise is intended to avoid an all-or-nothing approach whereby the government either is entitled to keep everything seized or ordered to return everything, including copies. Thus, the Rule is intended to allow room for return of documents that are relevant to ongoing or contemplated investigations by permitting the government, in most circumstances, to retain copies of the seized information for future use.

176 Ramsden v. United States, 2 F.3d 322, 325 (9th Cir. 1993).
178 Black Hills Inst. of Geological Research v. U.S. Dep’t of Justice, 967 F.2d 1237, 1240 (8th Cir. 1992) (holding landowner had interest in preservation of dinosaur fossil seized during criminal investigation into violations of the Antiquities Act); In re Singh, 892 F. Supp. 1, 3 (D.D.C. 1995) (ruling movant demonstrated such a pressing need where its principal business was preparation of tax returns and IRS had seized business equipment and business files); cf. Hiller v. Murphy, 600 F. Supp. 14, 18 n.2 (D. Ga. 1984) (finding no pressing need for property where movant filed for return of property two years after search was executed and property was seized).
179 Ramsden, 2 F.3d at 327.
180 FED. R. CRIM. P. 41(g) advisory committee’s comment, 1989 Amendment.
181 Id.
a. Suppression v. Return of Property

After the 1989 amendments, the Advisory Committee noted that “Rule 41(e) is not intended to deny the United States the use of evidence permitted by the fourth amendment and federal statutes, even if the evidence might have been unlawfully seized.” The Committee found it significant that language in the prior version of the Rule, relating to the suppression of returned property, had been deleted in response to Supreme Court precedent which permitted the use of illegally seized evidence for other purposes. In particular, in United States v. Calandra, the Supreme Court held that the exclusionary rule could not be used to preclude grand jury testimony based on illegally seized evidence. As an extension of that holding, the court noted that Rule 41(g) is not intended to be a “statutory expansion of the exclusionary rule.”

In In re Southeastern Equipment Search Warrant, the U.S. District Court for the Southern District of Georgia cautioned, however, that Calandra should not be interpreted too broadly. It noted that Calandra only addressed the issue of whether a witness could invoke the exclusionary rule during grand jury questioning and did not address the issue of whether illegally seized evidence could be returned while a grand jury proceeding was underway. Thus, the district court determined that “it is apparent that the Court [in Calandra] did not intend to prohibit the use of a Rule 41(e) motion during a grand jury proceeding to seek the return of illegally seized property.”

Since the 1989 amendment to the rule precluded suppression as a de facto result of an order to return property, the district court reasoned that Rule 41 provides for return of illegally seized property, while at the same time reserving the determination of whether such evidence should be excluded from trial under the exclusionary rule. Thus, a distinction needs

---

183 Fed. R. Crim. P. 41(g) advisory committee’s comment, 1989 Amendment.
185 414 U.S. at 348-49.
186 Id. at 349 n.6.
188 Id. at 1571. In Calandra, the Supreme Court had left open the possibility that a party, who was unable to seek suppression of the evidence under its ruling, could seek return of property under Rule 41(e). 414 U.S. at 354 n.10.
190 Id. at 1571-72.
to be made between suppression of evidence and the court’s power to order its return under Rule 41(g). Ordinarily, the court may only suppress evidence pursuant to a Rule 41(g) motion if it treats the motion as a post-indictment motion to suppress under Rule 12.191 In the context of a motion to suppress, the general rule is that properly seized evidence will remain admissible and only that which is improperly seized will be suppressed.192 Conversely, blanket suppression of evidence is warranted where the agents executing the warrant exhibit “flagrant disregard” for the terms of the warrant.193 Such conduct is found where the government effects a “widespread seizure” of items which clearly are not within the scope of the warrant.194

Thus, the Fifth Circuit concluded that the target of a grand jury investigation could not use Rule 41(g) to “prevent the grand jury from having access to illegally obtained evidence.”195 This ruling is essentially a recognition of the fact that the exclusionary rule only applies to the prosecution’s case-in-chief; illegally seized evidence can be used in other contexts, including for impeachment, sentencing, and before the grand jury. An order for return of property that also had the effect of suppression would therefore be premature at this stage of the proceedings because the court cannot predict what the government’s intended use of the property is going to be. As the Fifth Circuit pointed out in In re Search of Law Office, the only exception to this rule is where complete suppression of all seized evidence is warranted upon a “substantial showing of irreparable harm.”196 Return of the property and suppression of its use for any purpose are proper in such a situation because the court would likely order blanket suppression of the evidence for use at trial anyway.

b. The Government’s Retention of Copies of Returned Property

Another question that arises in the context of a Rule 41 motion is whether the government should be permitted to retain a copy of seized materials where the original documents are ordered to be returned (or vice versa). This issue is a particularly thorny one. The Advisory Committee comments are again instructive. The Committee specifically rejected the idea that the government has to return photocopies of business records it has lawfully seized and intimated that copies of illegally seized evidence

191 FED. R. CRIM. P. 41(h).
193 United States v. Hamie, 165 F.3d 80, 83-84 (1st Cir. 1999).
194 Triumph Capital, 211 F.R.D. at 61.
195 In re Search of Law Office, 341 F.3d 408, 412 (5th Cir. 2003).
196 Id. at 413-14.
could be retained in certain circumstances as well. The Committee noted that the return or destruction of all copies of seized records is warranted only where “equitable considerations” justify such an approach.

Courts have generally held that the government may retain copies of the seized evidence, absent “extreme circumstances.” For example, in *Ramsden*, the Ninth Circuit approved the government’s retention of copies of documents seized without a valid warrant because it advanced a “legitimate law enforcement interest”—namely that of assisting the British government with an ongoing investigation of the defendant. On similar grounds, the Fifth Circuit refused to uphold a district court order requiring return of all copies of documents taken from a law office. The court noted that the Advisory Committee comments caution that “even in cases of illegally seized property, ‘[i]f the United States has a need for the property in an investigation... its retention of the property generally is reasonable.’”

Taken at face value, this statement implies that the government could keep copies of any documents and records that it seizes, regardless of the legality of their seizure, simply by alleging that it has some “legitimate interest” in their retention. While it is true that Rule 41(g) cannot expand the scope of the exclusionary rule, it is axiomatic that it cannot restrict it either. A more narrow definition of “legitimate government interest” is needed to prevent such a perverted result.

In order to retain items seized outside the scope of a warrant, the government must demonstrate that the items have some connection or nexus to the underlying investigation. To hold otherwise would eliminate

---

197 The Committee summed up its findings as follows:

As amended, Rule 41(e) avoids an all or nothing approach whereby the government must either return records and make no copies or keep originals notwithstanding the hardship to their owner. The amended rule recognizes that reasonable accommodations might protect both the law enforcement interests of the United States and the property rights of property owners and holders. In many instances documents and records that are relevant to ongoing or contemplated investigations and prosecutions may be returned to their owner as long as the government preserves a copy for future use.

FED. R. CRIM. P. 41(g) advisory committee’s comment, 1989 Amendment.

198 FED. R. CRIM. P. 41(g) advisory committee’s comment, 1989 Amendment. The Committee cited to *Paton v. LaPrade*, 524 F.2d 862, 867-69 (3d Cir. 1975) as an example of such extenuating circumstances. This citation is vague and, frankly, confusing. *Paton* dealt with an expungement of a closed criminal case, not a Rule 41(e) motion. *Id.* at 867. The Ninth Circuit found the citation unhelpful as well. *Ramsden v. United States*, 2 F.3d 322, 327 n.3 (9th Cir. 1993).

199 Grimes v. Comm’r, 82 F.3d 286, 291 (9th Cir. 1996).

200 2 F.3d at 327.

201 *In re Search of Law Office*, 341 F.3d 404, 412 (5th Cir. 2003).

202 *Id.*
any incentive for the government to refrain from engaging in widespread fishing expeditions. For example, assume the government has a warrant to search a house for evidence of stolen property. During the search, the government seizes stolen electronics (related to the investigation) and evidence of an assault (unrelated to the investigation) from a location not authorized by the warrant. Under this analysis of the rule, while both types of evidence are illegally seized, the government would be able to retain the stolen electronics but not the evidence related to the assault.

Several courts have limited the language of Rule 41(g) in this fashion. In *Interstate Cigar Co. v. United States*, the Seventh Circuit held that in order to retain possession of seized property, the government “must demonstrate a specific nexus between the seized property and the continuing criminal investigation.” In *In re Search Warrant for K-Sports Imports, Inc.* refused to extend the government’s right to retain documents and property which were unrelated to the topic of the warrant. There, customs agents seized illegal Chinese machine guns, records, and other documents pertaining to their purchase, as well as other unrelated weapons, records, and computer data. The court held that the government could only retain items related to illegal machine gun purchase:

Government, in this case, has a legitimate interest in documents and computer records/discs related to the purported machine guns because of the pending forfeiture proceeding; but does not have a legitimate interest regarding documents and computer records/discs unrelated to the purported machine guns. Government’s interest may be accommodated by returning all original documents and computer records/discs to K-Sports after Government has had an opportunity to review them and to photocopy or otherwise duplicate those items relating to the purported machine guns. This resolution achieves the “reasonable accommodation” favored by the Ninth Circuit.

Finally, in *Maali*, the court refused to permit the government to keep all of the information found on eighty-three hard drives containing some three million files it had seized during the search of a business. The government had sought to keep all of the documents, claiming that they were part of a separate, on-going grand jury investigation. The court held that the government could not keep documents which were not “within the scope of the warrant” and which it “did not intend to introduce at trial.”

---

203 928 F.2d 221, 224 (7th Cir. 1991).
205 Id. at 596.
206 Id. at 598 (emphasis added).
208 Id. at 1266.
209 Id.
III. DISCUSSION OF United States v. Comprehensive Drug Testing, Inc.

The CDT decision is important in the law of computer searches because it addresses most of the areas touched on above. Unlike many cases which only involve the search of a defendant's personal computer, the CDT case implicates wide-ranging privacy concerns, involving the search of third-party medical records. The following is an in-depth analysis of the decision and its potential to influence future decisions in this area.

A. FACTS AND PROCEDURAL HISTORY

In CDT, the federal government served the search warrants in question as part of an ongoing investigation into the activities of BALCO.\footnote{473 F.3d 915, 919-20 (9th Cir. 2006).} The government began its investigation in 2002 and eventually developed probable cause that at least ten major league baseball players had obtained steroids from BALCO.\footnote{Id. at 920.} Shortly thereafter, the Major League Baseball Players Association ("MLBPA") agreed that, as part of its collective bargaining agreement with MLB, the players would be anonymously tested for steroid use in 2003.\footnote{Id. at 944-45 (Thomas, J., concurring in part and dissenting in part).} Pursuant to the agreement, the results would be used only to determine the extent of the steroid problem in baseball and the results of the tests would be kept confidential.\footnote{In 2003, 1198 MLB players were tested for steroids pursuant to the new collective bargaining agreement that had gone into effect the previous fall. Two hundred forty players were randomly selected for a second round of tests. Gordon Edes, Baseball Gets Tougher over Steroid Use, BOSTON GLOBE, Nov. 14, 2003, available at http://www.boston.com/sports/baseball/articles/2003/11/14/baseball_gets_tougher_over_steroid_use/. Pursuant to the agreement, the identities of those who tested positive an initial time were to be kept confidential. \textit{Id.} The league announced that 5-7% of the 1438 anonymous, unannounced tests had tested positive for steroids, triggering a new round of testing and sanctions for 2004. \textit{Id.}}

The government in early 2004 then subpoenaed the testing records for all MLB players from the independent testing labs which had performed the tests—Comprehensive Drug Testing, Inc. ("CDT") in Long Beach, California and Quest Diagnostics, Inc. ("Quest") in Las Vegas, Nevada.\footnote{CDT, 473 F.3d at 920. After the initial subpoena was met with resistance, the government then issued a narrower subpoena on March 3, 2004, limited to the testing records for only the eleven players with BALCO connections. \textit{Id.}} CDT and Quest both resisted producing any material under the subpoenas. On March 3, 2004, the government issued new subpoenas, seeking information related only to the ten players with BALCO connections.\footnote{Id.} The MLBPA filed motions to quash the subpoenas. While the motions to
quash were still pending, the government applied for warrants to search the
two labs in the federal districts where they were located.\textsuperscript{216} The warrants
authorized the seizure of the drug testing records and specimens for the ten
named players connected to the BALCO investigation as well as any other
materials detailing and explaining the testing process.\textsuperscript{217} The warrants also
authorized the agents to search computer equipment and storage devices,
and where an on-site search would be impracticable, to seize either a copy
of the data or the computer equipment itself.\textsuperscript{218} Additionally, the warrant
allowed the agents to rely on the advice of a computer expert to choose the
proper course of action to capture the data sought.\textsuperscript{219}

The warrants were executed on April 8, 2004.\textsuperscript{220} Initially, the agents’
search of CDT was met with resistance.\textsuperscript{221} The agents threatened to seize
all of CDT’s computers for up to sixty days unless the directors assisted
them in locating the evidence.\textsuperscript{222} After lengthy negotiations with CDT
directors and their counsel, the federal agents were informed that two
particular computers contained the information relevant to the search
warrant.\textsuperscript{223} During the search, agents discovered a hard copy document
which contained names and identifying numbers for all MLB players,
including some of the ten BALCO players.\textsuperscript{224} One of the agents faxed the
document to another agent for preparation of a third search warrant to seize
testing specimen samples from Quest based on the identifying numbers.\textsuperscript{225}

After observing the agent fax the document, one of CDT’s directors
opened a locked drawer and provided the agent with a document that
contained the testing results for the ten named BALCO players.\textsuperscript{226} Another
CDT director then identified a computer directory (the “Tracey” directory)

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{216} Id. at 921. The affidavit for the warrant for CDT referenced the fact that CDT
intended to challenge the subpoena. Id. at 946. The affidavit for the warrant to search Quest
apparently did not reference the fact a subpoena had been issued or that a motion to quash
had been filed. Id. at 947 (Thomas, J., concurring in part and dissenting in part).
\item \textsuperscript{217} Id. at 921.
\item \textsuperscript{218} Id.
\item \textsuperscript{219} Id.
\item \textsuperscript{220} Id. at 921-22.
\item \textsuperscript{221} Id. at 922.
\item \textsuperscript{222} Id.
\item \textsuperscript{223} Id.
\item \textsuperscript{224} Id.
\item \textsuperscript{225} Id. The agents who executed the initial search warrant at Quest’s Las Vegas lab were
unable to locate the specimens to be seized because the samples were identified by number
only and the identifying numbers were kept at an off-site location. Pursuant to the third
warrant, the agents seized the then-identifiable BALCO players’ specimens. Id. at 922 n.13.
The MLBPA’s motion for return of property was based solely on the conduct of the agents
during their search of CDT, however. Id. at 923.
\item \textsuperscript{226} Id.
\end{itemize}
\end{footnotesize}
for the agents which contained all of the computer files for the company's sports drug testing programs. A forensic computer expert then recommended copying of the entire directory for off-site analysis due to the time and intrusiveness involved in searching the entire directory on site. A copy of the directory was then made and seized for analysis. Agents seized additional hard copy documents, including a twenty-five page master list of all MLB players tested during the 2003 season and a thirty-four page list of positive drug testing results for eight of the ten BALCO players, which was intermingled with positive test results for twenty-six other players.

On April 30, 2004, the government sought a search warrant in the Northern District of California for all electronic data retained by CDT pertaining to the drug testing of all MLB players located within the Tracey directory, a copy of which was in the possession of the IRS in San Jose, California. The affidavit sought authorization to conduct a “thorough review” of all the MLB-related drug testing data and to seize “all data pertaining to illegal drug use by any member of major league baseball.” The affidavit also averred that it was “logical to assume” that such a review would “provide additional evidence of the use of similar performance-enhancing drugs which could establish a link to the charged defendants in the charged [BALCO] case.” The affidavit for the warrant did not disclose the ongoing litigation surrounding the seizure of the same material from the CDT lab on April 7th.

On May 5, 2004, the agents applied for new search warrants of CDT and Quest based on the information obtained from the Tracey directory seized from CDT. The new warrants authorized seizure of all specimens and records relating to all of the other non-BALCO MLB players who had

---

227 Id. at 947 (Thomas, J., concurring in part and dissenting in part). The directory contained over 2900 files. Certain subdirectories pertained to the MLB drug test results; many others contained test results for other sports and business organizations. Id.
228 Id.
229 Id. at 923 (majority opinion).
230 Id. Copies of all seized documents were provided to CDT directors several days later. Id. at 923 n.15.
231 Id. at 923 n.16.
232 Id. at 948 (Thomas, J., concurring in part and dissenting in part).
233 Id.
234 Id. at 949. A motion for return of property was subsequently filed and granted by Judge Illston on August 9, 2004. The government did not challenge the ruling, but instead asserted that it had the right to review the same information under the April 7 warrants. Id. at 923 n.16 (majority opinion).
235 Id. at 923-24.
tested positive for steroids in 2003.  The government executed the warrants a day later and simultaneously issued grand jury subpoenas for the same information.  The MLBPA then filed Rule 41(g) motions for return of property seized pursuant to both the April and May warrants.  It also filed motions to quash the May subpoenas.  Without holding evidentiary hearings, the trial courts in each district granted the motions for return of property.  The courts ordered that all property seized which was not connected to the ten BALCO players must be returned.  Judge Illston also issued an order quashing the May 6, 2004 subpoena directed at CDT.

B. NINTH CIRCUIT DECISION

The Ninth Circuit reversed the decision of the trial courts to grant the motions for return of property and to quash the subpoenas, finding that their decisions constituted an abuse of discretion.  The court reviewed the Ramsden factors for determining whether an exercise of the court’s equitable power to entertain a pre-indictment motion for return of property was justified.  Although it ultimately ruled that the equities weighed in the MLBPA’s favor, the panel held that the lower courts had erred in finding that the government’s execution of the warrants evidenced a “callous disregard” for the players’ constitutional rights.

1. The Lower Courts’ Findings That Issuance of the Search Warrants Constituted Callous Disregard Were Erroneous

   a. The Simultaneous Issuance of Subpoenas and Search Warrants Did Not Constitute Callous Disregard

   First, the court rejected the players’ argument that the government’s simultaneous issuance of search warrants and subpoenas for the same information constituted “callous disregard,” stating “[w]e are aware of no

---

236 id.
237 id. at 924.  Quest complied with the subpoena, but the government deferred CDT’s compliance until the search warrant litigation was resolved.  On August 31, 2004, the government revoked the indefinite deferral and the MLBPA filed a motion to quash in the Central District of California on September 13, 2004.  Id. at 925.
238 id. at 924.
239 id. at 925.
240 id. at 924.
241 id.
242 id. at 925.
243 id. at 938.
244 id. at 929-36.
245 id. at 936.
authority that the simultaneous pursuit of search warrants and subpoenas in aid of an ongoing grand jury investigation constitutes a violation of the Fourth Amendment.\textsuperscript{246} The court recognized the difference between the two tools, noting that warrants may only be obtained upon a showing of probable cause, whereas subpoenas may be issued any time a prosecutor feels the information may assist a grand jury with its investigation.\textsuperscript{247} Thus, it concluded that even had the initial subpoenas been quashed, the government still could have applied for search warrants to obtain the requested material.\textsuperscript{248}

This conclusion goes counter to the DOJ guidelines which state that search warrants should not be issued in lieu of subpoenas (where practical), or issued where a challenge to the use of a subpoena has been made.\textsuperscript{249} Although Judge Thomas raised this issue in his dissent,\textsuperscript{250} the majority dismissed his argument on the ground that such guidelines do not give rise to substantive rights, and as such, do not dictate what is “reasonable” under the Fourth Amendment.\textsuperscript{251} Judge Thomas noted that such guidelines do, however, “form a baseline from which to judge the reasonableness of unjustified deviations from the standard practices they outline.”\textsuperscript{252}

Judge Thomas’ reasoning is more persuasive. While it is true that such guidelines should not be used to delineate the floor for determining which procedures are, at a minimum, constitutionally required, the trial courts were not using the government’s deviation to prove defendant’s constitutional Fourth Amendment rights had been violated (and thus to order suppression of evidence). Rather, they were using it to determine whether the court’s equitable powers should be exercised to entertain a Rule 41(g) motion for return of property.

For example, in the lower court’s ruling on the Motion for Return of Property in the Central District of California, Judge Cooper noted some “special concerns” that she had with the government’s actions in this case:

The documents presented to the Court in connection with this Motion reveal extremely troubling conduct on the part of the Government. The picture painted is one of almost desperate effort to acquire evidence by whatever means could be utilized. The Government negotiated with movants’ attorneys over the breadth of the grand jury subpoenas; received assurances in writing that the records of the ten athletes would be secured while the Court resolved the issue, and the day after the

\begin{flushleft}
\textsuperscript{246} Id. at 930.
\textsuperscript{247} Id.
\textsuperscript{248} Id.
\textsuperscript{249} See discussion of 28 C.F.R. § 59.4 supra notes 107-15.
\textsuperscript{250} CDT, 473 F.3d at 959 (Thomas, J., concurring in part and dissenting in part).
\textsuperscript{251} Id. at 938 n.42 (majority opinion).
\textsuperscript{252} Id. at 959 (Thomas, J., concurring in part and dissenting in part).
\end{flushleft}
issue was presented to a Court, went to another district and sought a search warrant. . . . Four days after Movants filed a motion before Magistrate Judge Johnson for return of property, the Government obtained a further warrant from a Magistrate Judge in the Northern District of California. And while a motion for return of that property was pending, the Government obtained two more warrants in the Central District of California (not from Magistrate Judge Johnson) and in Nevada. The image of quickly and skillfully moving the cup so no one can find the pea would be humorous if the matter were not so serious.  

Thus, in his dissent, Judge Thomas concluded that the district judges were entitled to find that the government's simultaneous issuance of subpoenas and search warrants constituted callous disregard because it "undertook this action in an attempt to prevent the Players Association and CDT from litigating the merits of their objections to the grand jury subpoenas."  

b. The Warrants Were Not Used as a Pretext to Search for Evidence of Unrelated Crimes

The MLBPA had also argued that the government was using the warrants (aimed at the BALCO test results) as a pretext to obtain the records of the other non-BALCO players who had also tested positive for steroids.  

It attempted to analogize the facts of its case to United States v. Rettig, where the Ninth Circuit had suppressed evidence seized as a result of "egregious police misconduct." There, the police had obtained a warrant to search a house for marijuana paraphernalia a day after failing to obtain a warrant to search it for evidence of a cocaine-smuggling conspiracy. During the subsequent search of the home, the officers demanded that the suspect's wife "tell us where [the cocaine] is so we don't have to mess up your house."  

The CDT court properly rejected that comparison. Since the agents were lawfully on the property and were authorized to seize records of the ten BALCO players, the court found that the seizure of the records of the non-BALCO players was not improper simply because they happened to be

---

253 Id. at 953-54 (quoting Judge Cooper's October 1, 2004 order granting the motion for return of property) (emphasis in original). The image Judge Cooper describes is perhaps even more humorous given her pun in the context of a drug testing case.

254 Id. at 959-60.

255 Id. at 932 (majority opinion).

256 Id.

257 United States v. Rettig, 589 F.2d 418, 422-23 (9th Cir. 1978).

258 Id. at 422 n.1.

259 The MLBPA did not challenge the validity of the warrants so the court presumed there was probable cause to support issuance of the warrants. CDT, 473 F.3d at 929.
intermingled with the relevant records. "Because the agents saw that the spreadsheet clearly contained information within the scope of the warrant, they seized the spreadsheet for off-site review." The court also noted that the record contained no evidence that the agents specifically targeted and seized records unrelated to the subject of the warrant.

The real problem, as Judge Thomas pointed out in his dissent, was that the government took no steps to protect the confidentiality of the non-BALCO players’ records. CDT had offered to produce the requested files, subject to their review by a magistrate for segregation of the non-confidential material. This procedure was rejected by the government. Instead, the government seized the entire Tracey directory, examined it, and then sought additional search warrants for the material it had initially requested in the much broader February subpoenas. The government should have, at the very least, used a taint team to segregate the confidential material.

c. The Seizure of Intermingled Records Did Not Constitute Callous Disregard

Furthermore, the Ninth Circuit rejected the MLBPA’s contention that the government’s seizure of intermingled documents without providing procedures for judicial review evidenced callous disregard. The court reviewed two prior precedents involving intermingled documents and concluded that the agents in this instance had not violated the Fourth Amendment. In United States v. Beusch, the court upheld the seizure of ledgers which contained items both covered and not covered by the warrant. The court concluded that no Fourth Amendment violation occurs where “single files and single ledgers, i.e., single items which, though theoretically separable, in fact constitute one volume or file

\[260\] The government argued that the seizure of the records was justified by the plain view doctrine. The court did not reach this argument, holding instead that the seized material fell within the scope of the search warrants. Id. at 935 n.39. In essence, the court’s rationale was that since the government intended to use only those records which pertained to positive steroid tests of MLB players, they fell within the scope of the warrants. However, the government was entitled to use only information relating to the ten BALCO players under the warrants. Id. at 937.

\[261\] Id. at 932.

\[262\] As discussed previously, it was not until the agents had reviewed the contents of the Tracey directory that they expanded the scope of the warrant to include all 100-plus players who had tested positive. See supra Part III.A.

\[263\] Id. at 962 (Thomas, J., concurring in part and dissenting in part).

\[264\] Id. at 932-33. The court discussed United States v. Tamura, 694 F.2d 591 (9th Cir. 1982), and United States v. Beusch, 596 F.2d 871 (9th Cir. 1979). CDT, 473 F.3d at 932-33.

\[265\] 596 F.2d at 876-77.
Conversely, the *Tamura* court objected to the "wholesale seizure" of entire filing cabinets of records without making any efforts to limit the seizure of unrelated material.\(^{267}\)

The *CDT* court found the situation more similar to *Beusch*, noting that, unlike in *Tamura*, the agents did not remove "entire categories of documents to coerce employees into cooperation," but instead only removed files and data related to the BALCO investigation.\(^{268}\) "Their ultimate decision to remove a relevant number of files for off-site review stemmed not from disregard of privacy rights, but from sensitivity to the ongoing disruption caused by the search to CDT—an innocent third party in the underlying investigation."\(^{269}\) The court noted the agents took "only a limited set of clearly relevant disks and a copy of the Tracey directory" and provided copies of all material taken just eight days later. The court concluded that the "agents demonstrated the careful regard absent in *Tamura*.\(^{270}\)

Again, the majority's analysis misses the point. The fact that the agents seized a copy of the Tracey directory rather than the entire computer is really not relevant in this instance. While the seizure of a copy is certainly less disruptive to the operation of CDT's business, the more pertinent concern is whether the government's actions interfered with privacy rights of the non-BALCO related players whose records were contained on the directory. Judge Thomas correctly stated that "when the countervailing interest is privacy and not merely the disruption of business, that interest suffers whether it is copies or originals that are seized.\(^{271}\)

The court also refused to require that a second warrant be obtained before government agents could review the intermingled records. In so holding, it declined to apply the *Tamura* court's suggestion that the seized intermingled documents should be sealed and held pending approval by a magistrate of a further search, labeling such a requirement as "advisory

\(^{266}\) *Id.* at 877.

\(^{267}\) 694 F.2d at 595.

\(^{268}\) *CDT*, 473 F.3d at 934. Apparently the court considered all of the sports drug testing information in CDT's possession as being related to the BALCO investigation. The Tracey directory contained information on thirteen different sports organizations, not just MLB.

\(^{269}\) *Id.* To assign such noble motives to the agents in the *CDT* case ignores one small detail. The government here did exactly what the agents did in *Tamura*—they threatened to take all sixteen of CDT's computers unless the employees cooperated in helping locate the relevant records. *Id.* at 922. Faced with a complete shutdown of their business, the CDT directors begrudgingly complied with some of the agents' requests. *Id.* It seems disingenuous to reward the officers' conduct in this case simply because their threats were more successful in eliciting cooperation than those made in *Tamura*.

\(^{270}\) *Id.* at 934-35.

\(^{271}\) *Id.* at 963 n.9 (Thomas, J., concurring in part and dissenting in part).
dicta. Instead, the court focused on the *Tamura* court’s allowance for substitute procedures pursuant to which “all items in a set of files” may be inspected during a search if such procedures are spelled out in the initial warrant. The court approved the seizure of the Tracey drive and other intermingled records because the agents had followed the protocol laid out in the search warrant for seizing intermingled records and data.

However, the court failed to address whether the warrant or affidavit had established a threshold showing for the need to remove the computer hardware and intermingled files in the first place. Recall that another Ninth Circuit panel had recently held, just prior to the *CDT* decision, that more than a “conclusory allegation” is necessary to permit the wholesale removal of computer hardware and storage media from a search site. This conclusion stems from the fact that the *Tamura* court found the wholesale seizure of documents to be unreasonable in light of feasible alternatives which existed to sort the documents on site. Thus, the court’s suggestion of how to handle future cases where such on-site sorting was not feasible was dicta.

Upon searching the premises, law enforcement personnel trained in searching and seizing computer data (the “computer personnel”) . . . make an initial review of any computer equipment and storage devices to determine whether these items can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve the data. . . . If the computer personnel determine that it is not practical to perform an on-site search or make an on-site copy of the data within a reasonable amount of time, then the computer equipment and storage devices will be seized and transported to an appropriate law enforcement laboratory for review.

*Id.*

It is difficult to tell whether the *CDT* court concluded that the procedures laid out in the warrant for seizure of computer files and equipment satisfied the *Hill* requirement, or whether it simply chose to ignore it altogether. The omission is probably academic, however. Although the affidavit remains under seal, the portions of it reprinted in the opinion indicate that the government did justify removal in the affidavit on the ground that:

The volume of data sorted on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. . . . Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impractical to bring to the search site all of the necessary technical manuals and specialized equipment to conduct a thorough search. In addition, it may be necessary to consult with computer personnel who have specific expertise in the type of computer software application or operating system that is being searched.

*CDT*, 473 F.3d at 966 (Thomas, J., concurring in part and dissenting in part). However, it could certainly be argued that this language is mere boilerplate which is put in all warrant affidavits rather than a specific showing of probable cause.

---

272 *Id.* at 933 (majority opinion) (citing United States v. Hill, 322 F. Supp. 2d 1081, 1090 (C.D. Cal. 2004)). This conclusion stems from the fact that the *Tamura* court found the wholesale seizure of documents to be unreasonable in light of feasible alternatives which existed to sort the documents on site. Thus, the court’s suggestion of how to handle future cases where such on-site sorting was not feasible was dicta.

273 *Id.* (citing United States v. Tamura, 694 F.2d 591, 595 (9th Cir. 1982)).

274 *Id.* at 933-34. The search warrants provided:

Upon searching the premises, law enforcement personnel trained in searching and seizing computer data (the "computer personnel") . . . make an initial review of any computer equipment and storage devices to determine whether these items can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve the data. . . . If the computer personnel determine that it is not practical to perform an on-site search or make an on-site copy of the data within a reasonable amount of time, then the computer equipment and storage devices will be seized and transported to an appropriate law enforcement laboratory for review.

*Id.*

275 *Hill*, 459 F.3d at 975; see discussion supra Part II.C. It is difficult to tell whether the *CDT* court concluded that the procedures laid out in the warrant for seizure of computer files and equipment satisfied the *Hill* requirement, or whether it simply chose to ignore it altogether. The omission is probably academic, however. Although the affidavit remains under seal, the portions of it reprinted in the opinion indicate that the government did justify removal in the affidavit on the ground that:

The volume of data sorted on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. . . . Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impractical to bring to the search site all of the necessary technical manuals and specialized equipment to conduct a thorough search. In addition, it may be necessary to consult with computer personnel who have specific expertise in the type of computer software application or operating system that is being searched.

*CDT*, 473 F.3d at 966 (Thomas, J., concurring in part and dissenting in part). However, it could certainly be argued that this language is mere boilerplate which is put in all warrant affidavits rather than a specific showing of probable cause.
The Government Did Not Have to Limit Its Search of the CDT Computer Files to Keywords

Finally, the court rejected the argument that the government should have limited its search of the computer directory to keyword searches such as the names of the BALCO players. The court pointed out that the agents were not required to assume that all relevant documents were so conveniently named or that CDT had no incentive to avoid providing the requested documents. The dissent suggested that the use of a relational database program would have easily segregated the data since the test results were kept by player name or identifying number. Rather than relying on CDT officials to conduct the search, the dissent further noted that the preferred procedure is to have a magistrate supervise the segregation and management of the data.

The majority refused to limit computer searches in such a fashion. It pointed out that the test results at Quest were not saved by keyword at all, but instead were saved by number; the corresponding key was kept at a storage locker at a different facility. Thus, the court concluded the agents’ actions were not performed in bad faith:

The government’s decision to copy the entire directory represented a conscientious effort to seek out all the evidence covered by the search warrant. We do not discern bad faith or “callous disregard” simply because the agents determined, after an initial review, that certain intermingled files needed to be reviewed off site, as permitted under our applicable precedents and the warrant itself.

According to the court, the agents’ seizure of the intermingled files “displayed attentiveness both to the warrant’s precautionary procedures and to the importance of avoiding unnecessary disruption of CDT’s business operations.”

2. The Remaining Three Ramsden Factors Weighed in Favor of the MLBPA

As previously mentioned, while the court concluded that the first Ramsden factor weighed against invocation of the district court’s equitable power (and the district courts’ conclusions to the contrary were thus erroneous), it found that the other three factors weighed in favor of the

276 CDT, 472 F.3d at 935.
277 Id. at 975-76 (Thomas, J., concurring in part and dissenting in part).
278 Id. at 976 n.19.
279 Id. at 935 (majority opinion).
280 Id.
281 Id. at 936.
MLBPA. Therefore, it held that the district courts did not abuse their discretion in entertaining, at the outset, the motions for return of property.

However, the Ninth Circuit went on to hold that the district courts’ orders, granting the motions and requiring return of the seized evidence unrelated to the ten BALCO players, were erroneous.

3. Return of Property Was Not Warranted Under Rule 41(g)

The court found that Rule 41(g) motions are properly denied if the government has a continuing need for the property as evidence, noting that return is proper only when the government “no longer needs the property.” The court reasoned return of the property was unwarranted because the intermingled files and data were seized legally under the search warrant and the government stated the remaining evidence was “essential” to its investigation and prosecution of illegal steroid distribution.

a. The Ninth Circuit Failed to Determine Whether the Non-BALCO Files Were Lawfully Seized Under the Warrant and Were Relevant to the Investigation

This analysis provides only half of the picture. Before the court can examine the government’s continuing need for the evidence, it must first determine whether the evidence was lawfully seized under the warrant and whether it is relevant to the investigation described in the warrant. With regard to intermingled data, the CDT court’s analysis failed to distinguish between the lawfulness of the seizure of the intermingled property in toto and the lawfulness of its continued retention and search of each individual computer file. The court simply bootstrapped its assumption that the test results for the non-BALCO players could be retained to its finding that the computer data as a whole had been properly seized under the intermingled records doctrine. Instead, the court should have first asked whether the government had proven that the seizure of the positive test results for the other hundred MLB players had been authorized under the April 2004 warrant.

282 Id.
283 Id.
284 Id. at 937 (emphasis in original).
285 Id.
286 See discussion of Rule 41 motions supra Part II.E.
287 For example, suppose the government seized a laptop and computer bag while searching for evidence of a drug manufacturing ring. While the seizure of the laptop bag may be justified under the intermingled property doctrine, the government could not keep unrelated evidence in the bag such as personal photos, credit cards, etc., simply on the ground the laptop bag was lawfully seized. That evidence is irrelevant to the investigation and clearly exceeds the scope of the original warrant. Thus, it must be returned.
warrants (or as an exception to the warrant requirement). It clearly was not. The warrants only provided for the seizure of the test results for the ten BALCO players.\(^\text{288}\) Moreover, the government conceded that before it reviewed the Tracey directory, it did not have probable cause to issue search warrants for the data from the non-BALCO players.\(^\text{289}\)

Even acknowledging that the Rule permits the government to retain unlawfully seized evidence in some circumstances, the government must still show that such evidence is relevant to the investigation at hand. The Ninth Circuit seemed to ignore other cases like \textit{K-Sports}, where the court forced the government to return unrelated property.\(^\text{290}\) The Rule is designed to permit the government to use illegally seized evidence only for closely related purposes (such as impeachment), not to permit it to expand its investigation into unrelated matters.

In this instance, some of the seized material concerned obviously unrelated testing records. The Tracey directory contained over 2900 files, including test results from thirteen different sports. The government admitted, in a hearing before Judge Illston in the trial court, that it could theoretically launch independent investigations of other sports based on the information contained in the Tracey directory:

\begin{quote}
Court: What if hockey had a subdirectory that had positive results and he [Agent Novitsky] clicked on it to make sure it was what it said it was, by George, that’s what it was, what about that?

Counsel: If it did happen, I would think that theoretically Agent Novitsky would have the right to either request a search warrant . . . . So there might be a legal entitlement for Agent Novitsky to use that and do something with it. . . . [A]gain, you would have, I believe, probable cause to believe that evidence in there would lead to other persons potentially involved in disputable criminal drugs, which is the crime that’s under investigation.\(^\text{291}\)
\end{quote}

The government’s interpretation of the law as ratified by the Ninth Circuit would, in essence, authorize the issuance of general warrants.

b. The Ninth Circuit Improperly Relied on Precedent Concerning Blanket Suppression

The \textit{CDT} court compounded its error by comparing the facts of its case to those of other cases where blanket suppression was found to be unwarranted. It cited \textit{Ramsden} and \textit{Tamura} for the proposition that full

\begin{itemize}
\item \(^{288}\) \textit{CDT}, 473 F.3d at 921.
\item \(^{289}\) \textit{Id.} at 962 (Thomas, J., concurring in part and dissenting in part).
\item \(^{290}\) \textit{In re Search Warrant for K-Sports Imports, Inc.}, 163 F.R.D. 594, 597 (C.D. Cal. 1995).
\item \(^{291}\) \textit{CDT}, 473 F.3d at 964 n.10 (Thomas, J., concurring in part and dissenting in part).
\end{itemize}
suppression of evidence was not warranted, even where the officers had engaged in an improper, wholesale seizure of evidence.\textsuperscript{292} The court noted that the \textit{Tamura} court found return of the seized property "inappropriate," even though some of the evidence had been unlawfully taken.\textsuperscript{293}

\textit{Ramsden} and \textit{Tamura} are inapposite. While the court correctly stated that blanket suppression is warranted only upon a showing of a "particularly egregious violation," this statement is applicable only if the MLBPA was moving for blanket suppression.\textsuperscript{294} Unlike the defendants in \textit{Tamura} and \textit{Ramsden}, however, the MLBPA was not arguing that all intermingled evidence, even that which had been \textit{legally} seized during the search, should be suppressed. Rather, it sought return only of the test results and information which did not pertain to the ten BALCO players.\textsuperscript{295} It was undisputed that the government could keep and use the information pertaining to the named BALCO players.\textsuperscript{296} Instead, the MLBPA objected to the fact that the government intended to use the information obtained from the seized directory to expand the focus of its investigation to all MLB players who had tested positive.\textsuperscript{297}

Despite the government's broadening of the scope of its initial investigation, the \textit{CDT} court found that return of the property was unnecessary in this instance.\textsuperscript{298} "While we agree that some information still retained by the government, at least in duplicate, may fall outside the scope of the warrant, we do not believe a return of the lawfully seized intermingled evidence properly remedies that wrong."\textsuperscript{299}

While the government should be able to lawfully seize all intermingled files where they are not subject to ready separation, it should not be allowed to use those files or data which are unrelated to the scope of the original

\textsuperscript{292} \textit{Id.} at 937 (majority opinion).
\textsuperscript{293} \textit{Id.} This is a misreading of \textit{Tamura}. The court never addressed the issue of whether the unlawfully seized evidence had to be returned. It simply held that the "exclusionary rule does not require suppression of evidence within the scope of a warrant simply because other items outside the scope of the warrant were unlawfully taken as well." United States v. Tamura, 694 F.2d 591, 597 (9th Cir. 1982).
\textsuperscript{294} \textit{CDT}, 473 F.3d at 937.
\textsuperscript{295} \textit{Id.} at 924.
\textsuperscript{296} \textit{Id.}
\textsuperscript{297} Theoretically, the government could have even expanded its investigation to include hockey players, track athletes, and other sports figures whose test results were contained in the Tracey directory.
\textsuperscript{298} \textit{CDT}, 473 F.3d at 938.
\textsuperscript{299} \textit{Id.} There is certainly a legitimate argument that the test results of the hundred other baseball players were relevant to the government's investigation of BALCO. However, this would allow the government to retain evidence for which it admittedly had no probable cause to obtain a warrant. Also, given the privacy concerns surrounding the test results, retention of the results in this case is not proper.
warrant. To hold otherwise would allow the government to sort through the intermingled records and pick and choose which information could help further its investigation or even to begin another independent one. If this were indeed the case, what would be the purpose of limiting the scope of the warrant in the first place?

4. The Ninth Circuit Provided for Only Post-Seizure Judicial Review

Despite its overbroad interpretation of Rule 41(g), the CDT court attempted to lessen the impact of its ruling by refusing to grant the government total carte blanche to review and use the seized material. It recognized that the government should not have unfettered discretion to determine which intermingled records should be returned and which should not:

We cannot accept the government's argument that it may retain all evidence simply because it assured the Player's Association and CDT (without signs of bad faith) that it did not intend to use all the files. In the case of a lawful and reasonable seizure of intermingled computer records for off-site review, as at bar, our precedents and the general reasonableness mandate of the Fourth Amendment require the supervision of a magistrate. It is not reasonable to allow the government to seize an indeterminately bounded array of computer data only later to set its own standards for review and retention thereof.

The court went on to lay out the procedure for such review, requiring that, upon the filing of a proper post-seizure motion by the aggrieved party, the record should be sealed and reviewed in camera by a magistrate. The court instructed that in reviewing the motion, the magistrate should apply its ruling and prior precedents in a "balanced manner." The court noted that, in the context of a seizure of computer files, most seized material can be substantially "pared down" but that certain files, such as short spreadsheets, can be retained in whole. After the magistrate determines which sealed items fall within the scope of the search warrant, the government may retain and use such items but must return all others to the person or entity searched. Finally, the court made it clear that nothing

300 id. (emphasis in original).
301 id. at 939.
302 id. at 940.
303 id. In determining what evidence the government can "reasonably retain" after a lawful seizure of intermingled computer data, the court stated that the magistrate may consider among other factors: (1) whether evidence mentioned in the search warrant can be separated from unrelated evidence by copying or moving files, but without creating new documents; (2) whether the file, if printed, would fill more than a typical paper ledger (of the sort in Beusch); (3) whether excision of the unrelated portions of the document would distort the character of the original document. Id. at 940 n.45.
304 id. at 940.
in its ruling precluded the government from subsequently seeking to expand the scope of its investigation (through additional search warrants or district court review of the magistrate’s ruling) based upon a showing of “any item’s relevancy to suspected criminal behavior uncovered during review of the evidence initially seized.”

This procedure loses almost all value, however, if it is implemented after, not before, the government views the seized files. Judge Thomas criticized the majority’s new review procedure:

For a magistrate’s role to be effective, it must come before the privacy interests have been compromised. Under the majority’s holding, the government is newly empowered to search the data before the magistrate authorizes the search. This flips the traditional relationship of the magistrate to the searching officer on its head. In all other contexts, the magistrate stands between the government and the privacy of individuals; in the majority’s proposed world, the magistrate only appears after the privacy interests have been invaded.

He pointed out that the ruling would allow the government to seize the medical records of anyone who had the “misfortune” of visiting a hospital or receiving treatment from a health care provider that kept patient records in a master file which also coincidentally contained the data of a person whose information was the subject of a search warrant. The dissent concluded that the better practice would be to have the neutral magistrate review the intermingled data first to ensure that “private information that the government is not authorized to see remains private.”

More troubling, the majority’s review procedure would become effective only after an objection had been made to the seizure. If no objection was forthcoming, then no review would take place. As the dissent pointed out, “[H]ow precisely is an honest citizen to know if his or her confidential medical records have been seized by the government so that he or she may seek redress?” While the majority’s procedure may work fairly well in situations where the patient is aware of the seizure (such as where the patient and the target of the investigation are one and the same), it fails to account for those situations where an innocent third party has no notice of the government’s activities. Without notice, the third party

---

305 Id. This statement, along with other language in the opinion, seems to indicate the court’s assessment that the government should be entitled to retain the positive test results of the hundred or so non-BALCO players upon a showing that the results are relevant to their ongoing investigation of unlawful steroid distribution. In fact, the government applied for such subsequent search warrants to do just that, based on the information obtained from the Tracey directory. Id. at 923-24.

306 Id. at 974 (Thomas, J., concurring in part and dissenting in part).

307 Id. at 963-64.

308 Id. at 964-65.

309 Id. at 974.
DEREK REGENSBURGER

will have no opportunity to ask for review of the government’s seizure of his confidential records.

This concern is borne out by the facts of CDT. Of the thirteen major sports organizations whose test results were contained on the Tracey directory, MLB (whose players were the target of the subpoena) was the only one to file an objection to the government’s seizure of the records.\(^3\)

The dissent identified the irony that this ruling will bring about: those suspected of criminal activity will have notice and opportunity to object to seizures while the completely innocent citizen will not.\(^3\)

Thus, as the dissent pointed out, this lack of notice is one of the reasons the use of search warrants against innocent third-party repositories of records is “strongly discouraged.”\(^3\)

The protection of Fourth Amendment rights cannot be left to the winds of chance. Something more is needed to preserve the privacy rights of individuals when their records are seized pursuant to a police investigation. At the very least, the government should have used a taint team to inspect the data and sort it. More preferably, the record should have been sealed immediately after the seizure of the Tracey directory, pending an inspection by a magistrate. Instead, the proverbial cat is out of the bag. The privacy and confidentiality of these records has been lost forever. Government investigators know which players tested positive and for what. The majority’s provision for after-the-fact magistrate review does little more than apply salve to the wound. Even worse, it may add injury to the insult if the magistrate decides to let the government retain some of the material seized outside the scope of the warrant and those players’ identities are eventually revealed.

IV. THE APPLICABILITY OF THE PLAIN VIEW DOCTRINE TO COMPUTER SEARCHES

Although the Ninth Circuit did not rule on the question of whether the plain view doctrine justified the government’s seizure of the intermingled files (as noted above, the court found it did not have to address the question), the issue was extensively briefed and argued by the government and is thus an important one to resolve for future computer searches. The question of whether the plain view doctrine applies in the context of a computer search is one which is subject to great debate. Some have argued that the doctrine should apply equally in the context of both computer and

\(^3\) Id. at 976.
\(^3\) Id. at 974-75.
\(^3\) Id. at 974 n.18.
physical searches; others have urged that it must be severely curtailed or eliminated altogether from the computer search realm.\textsuperscript{313}

At first blush, the applicability of the plain view doctrine to a computer search seems dubious. Ordinarily, when one thinks of the plain view doctrine, one thinks of an officer who stumbles across contraband in open, obvious view while conducting a search for evidence of some other crime.\textsuperscript{314} If the officer does not have probable cause to believe that an object in plain view is contraband without "conducting some further search of the object," then the plain view doctrine does not apply.\textsuperscript{315} How, then, can something initially hidden from the human eye be said to be in plain view if it requires a computer analyst to first search the computer storage media for the file and then employ a program to interpret it, making its contents visible?

The answer lies in cases which have applied the doctrine to document searches. Like computer searches, document searches require officers to at least briefly examine all files to determine if they are covered under the warrant. If, during that brief perusal, the document’s incriminating nature becomes obvious, officers are allowed to seize it under the plain view doctrine. In \textit{United States v. Rude}, the Ninth Circuit stated the analysis as follows:

\begin{quote}
[T]he incriminating character limitation necessarily permits a brief perusal of documents in plain view in order to determine whether probable cause exists for their seizure under the warrant. If in the course of that perusal, their otherwise incriminating character becomes obvious, they may be seized. Otherwise, the perusal must cease at the point at which the warrant’s inapplicability to each document is clear.\textsuperscript{316}
\end{quote}

Some types of documents which courts have held to be incriminatory on their face include papers relating to the sale or manufacture of drugs, gambling records, fake identification cards, and documents linking the defendant to known co-defendants.\textsuperscript{317} However, the court in \textit{Rude

\begin{footnotesize}
\textsuperscript{313} Ziff, supra note 68, at 865-66. \textit{But see} Kerr, supra note 66, at 582-83.
\textsuperscript{314} The plain view doctrine is commonly characterized as an exception to the warrant requirement, allowing officers to seize objects that are outside the scope of the warrant but that are patently contraband. \textit{Horton v. California}, 496 U.S. 128, 133 (1990). In order to justify a warrantless seizure under the doctrine, three conditions must be satisfied: (1) the officer must lawfully be in a position where the object can be plainly viewed, (2) the object must be in plain view, and (3) the incriminating nature of the evidence must be "immediately apparent." \textit{Id.} at 136.
\textsuperscript{315} Minnesota v. Dickerson, 508 U.S. 366, 375 (1993).
\textsuperscript{316} \textit{United States v. Rude}, 88 F.3d 1538, 1552 (9th Cir. 1996).
\textsuperscript{317} \textit{See} United States v. Barnes, 909 F.2d 1059, 1070 (7th Cir. 1990); United States v. Gargotto, 476 F.2d 1009, 1013 (6th Cir. 1973); United States v. Maude, 481 F.2d 1062, 1069 (C.A.D.C. 1973).
\end{footnotesize}
determined that the seizure of eighteen documents, which pre-dated the warrant cutoff, were not in plain view because the officers' "immediate observation" of the contested documents revealed that they were outside the scope of the warrant.\textsuperscript{318}

Only a handful of courts have addressed the question of whether the plain view doctrine applies in the context of a computer search. Two cases from the Tenth Circuit are instructive. In \textit{United States v. Carey}, the court held that the plain view doctrine could not be used to justify the officer's search of JPG files once it was determined that such files did not contain evidence related to the object of the warrant.\textsuperscript{319} The court reasoned that the detective had abandoned the initial purpose of his search by opening the subsequent picture files:

We infer from his testimony Detective Lewis knew he was expanding the scope of his search when he sought to open the JPG files. Moreover, at that point, he was in the same position as the officers had been when they first wanted to search the contents of the computers for drug related evidence. They were aware they had to obtain a search warrant and did so. These circumstances suggest Detective Lewis knew clearly he was acting without judicial authority when he abandoned his search for evidence of drug dealing.\textsuperscript{320}

The court concluded that the detective could not have "inadvertently discovered" the contents of each of the picture files he subsequently opened.\textsuperscript{321} The court's ruling hinged on its belief that the detective did not have authority under the warrant to view all files on the computer.\textsuperscript{322} The court stated:

\begin{itemize}
  \item \textsuperscript{318} \textit{Rude}, 88 F. 3d at 1522. \textit{But see In re Southeastern Equip. Co. Search Warrant}, 746 F. Supp. 1563, 1580 (S.D. Ga. 1990) (holding an address book seized from the office of a salesman, whose files were not within the scope of the warrant because the companies that were the target of the warrant were not his clients, fell under the plain view exception to the warrant requirement because the book contained information which was immediately apparent as being important to other ongoing investigations).
  \item \textsuperscript{319} 172 F.3d 1268, 1276 (10th Cir. 1999).
  \item \textsuperscript{320} \textit{Id.} at 1273. The court further found that it need not reach the question of what constituted plain view because the images were located in "closed files" and thus "not in plain view." \textit{Id.}
  \item \textsuperscript{321} \textit{Id.} The court's conclusion is contradicted by the detective's testimony. He testified that he believed he could search "these files [the image files] as well as any other files contained in the computer]." \textit{Id.} at 1271. He also stated that until he opened each file, he really did not know its contents, stating, "I wasn't conducting a search for child pornography, that happened to be what these turned out to be." \textit{Id.} Therefore, it appears the court was making a credibility determination—namely that the officer could not have reasonably been searching for evidence relating to the warrant when he searched the image files.
  \item \textsuperscript{322} Ziff frames the analysis a little differently:

The questions addressed by the court [in \textit{Carey}] should not have been "Were the files in plain view?" and "Were the files particularly listed in the warrant?" Indeed, the answer to these
In our judgment, the case turns upon the fact that each of the files containing pornographic material was labeled “JPG” and most featured a sexually suggestive title. Certainly after opening the first file and seeing an image of child pornography, the searching officer was aware—in advance of opening the remaining files—what the label meant. When he opened the subsequent files, he knew he was not going to find items related to drug activity as specified in the warrant, just like the officer in *Turner* knew he was not going to find evidence of an assault as authorized by the consent.

In *United States v. Walser*, the Tenth Circuit re-affirmed the inadvertence requirement of *Carey*. There, the agent testified that he opened an AVI file (a video file) which contained an image of child pornography during the course of his search of a computer hard drive for evidence of drug transactions. The court found that the opening of the AVI file, like the discovery of the first child pornography file in *Carey*, was proper since it was an inadvertent discovery.

These cases resurrected the inadvertent discovery requirement, which while at one time had been an element of the plain view doctrine, has since been eliminated. The Supreme Court in *Horton v. California* held that:

> [E]venhanded law enforcement is best achieved by the application of objective standards of conduct, rather than standards that depend upon the subjective state of mind of the officer. The fact that an officer is interested in an item of evidence and fully expects to find it in the course of a search should not invalidate its seizure if the search is confined in area and duration by the terms of a warrant or a valid exception to the warrant requirement.

The court suggested instead that “[s]crupulous adherence” to the particularity requirement serves to limit the area and duration of the search that the inadvertence requirement “inadequately protects.” Since an object seized in plain view does not involve an intrusion on privacy, the court concluded that if such an invasion of privacy had occurred, it must have occurred before the object came into plain view.

---

questions is “no.” Rather, the court should have asked, “Did the warrant authorize the opening of the file?” and “If so, did the plain view doctrine justify the officer’s seizure of that file?”


*Carey*, 172 F.3d at 1274.

275 F.3d 981 (10th Cir. 2001).

*Id.* at 984-85.

The court distinguished the facts from *Carey* because the agent, unlike the detective in *Carey*, immediately ceased his search and obtained a subsequent warrant for child pornography. *Id.* at 987.


*Id.* at 139-40.

*Id.* at 140.
The unworkable nature of the inadvertence requirement espoused in *Carey* and *Walser* is highlighted by the facts of *United States v. Gray*.331 There, the agent opened picture files contained in two suspicious directories labeled “Teen” and “Tiny Teen.”332 The court distinguished its case from *Carey* on the ground that the agent testified that he continued the focus of his original search, even after the initial discovery of the first pornographic photograph.333 However, unlike the Tenth Circuit, the *Gray* court permitted the officer to open all files pursuant to the warrant to search the computer, not just those limited by key word or file type.334 Thus, even though the testimony of the officers was virtually identical with respect to how the computer search was carried out, the courts came to opposite conclusions as to the officers’ subjective intent.

Because of these problems, Kerr argues for a severe curtailment or even complete elimination of the plain view doctrine from computer searches.335 Kerr rejects the *Carey* inadvertence approach because its “critical weakness” is trying to determine the subjective intent of an officer in the computer context.336 Because agencies often develop guidelines which mandate very thorough searches, he concludes, “When every step taken by an analyst is a matter of routine policy, it becomes difficult to exclude evidence on the ground that the analyst was attempting to circumvent the warrant.”337 Kerr suggests the plain view doctrine could be applied to serious crimes only or may have to be eliminated altogether for digital searches:

> Although forensic practices may be invasive by technological necessity, a total suppression rule for evidence beyond the scope of a warrant would both remove any incentive for broad searches and neutralize the effect of broad searches that occur. It would regulate invasive practices by imposing use restrictions ex post rather than attempting to control searches ex ante, offering a long-term second-best approach to regulating the computer forensics process. In short, it would allow the police to

332 Id. at 527.
333 Id. at 528-29. The difference between *Carey* and *Gray* is not that clear cut. In *Gray*, the agent first opened JPG files in the “Teen” directory which appeared to contain images of adult pornography. He next opened the “Tiny Teen” subdirectory. While the agent admitted that the name did cause him to wonder if it contained images of child pornography, he testified that he opened the files in the subdirectory because it was the next subdirectory listed, and he was opening all of the subdirectories as part of his search for material listed under the warrant. Only after he viewed several of the images in the “Tiny Teen” directory did the agent cease his search and apply for a second warrant to search for additional images of child pornography. *Id.* at 527.
334 *Id.* at 529; see also discussion of *Gray* supra Part II.
335 Kerr, supra note 66, at 577.
336 *Id.* at 578.
337 *Id.* at 579.
conducted whatever search they needed to conduct (to ensure recovery) and then limit use of the evidence found (to deter abuses). 338

Perhaps the better argument for eliminating the plain view doctrine from the realm of digital searches is that the concerns justifying its use in the physical search context are often lacking in computer searches. The practical justification for allowing the police to make a warrantless seizure of evidence in plain view is to spare the police "the inconvenience and the risk—to themselves or to preservation of the evidence—of going to obtain a warrant."339 That concern is not often present in the computer context. In executing a computer search, government agents often will either seize the original computer hardware and/or storage media or make a full bitstream copy of the data, removing it from the control of the suspect.340 Thus, any delay in obtaining a subsequent warrant would not risk the disappearance of any evidence or the safety of the officers because the computer files would remain in the constant control of government investigators.341

V. A PROTOCOL FOR COMPUTER SEARCHES IN THE FUTURE

The lesson that this article has hopefully provided is that a more systematic and consistent approach to computer searches is needed. Investigators' efforts should not be unduly hampered in one jurisdiction while going virtually unchecked in another. Such inconsistent application of the law makes it difficult for computer owners to develop and implement policies designed to protect privacy, particularly for business owners whose servers are located in multiple jurisdictions.

Resolving this conflict involves weighing two competing interests: (1) the privacy rights of an individual or business in the computer data, and (2) the government's need for flexibility in conducting searches of such data. Balancing these interests is particularly tricky, however, given the inherent difficulties in predicting the technological sophistication of a particular

---

338 Id. at 584.
340 Agent Reese confirmed that it is not inconvenient for forensic investigators to obtain a new warrant for material that is discovered pursuant to the original warrant but which is outside the scope of the investigation. The process usually takes only a few hours. Interview with Collin Reese, supra note 20.
341 Judge Thomas made this point in his dissent in United States v. Comprehensive Drug Testing, Inc.

Electronic data is simply not the kind of evidence that forms a natural extension of an officer's discovery of obvious contraband in a public place. The fact that further careful electronic assistance is required outside the searched premises to interpret the data belies the "practical" justification that there is insufficient time to obtain a warrant.

473 F.3d 915, 967 (9th Cir. 2006) (Thomas, J., concurring in part and dissenting in part).
suspect. Some investigations may require relatively simple inspections of
the directories and files of a given computer system to uncover the desired
information; others may require lengthy and complicated search
methodologies to defeat encryption or other techniques used to mask the
true identity of the contents of a file. The problem confronting investigators
in the context of digital searches is that criminals rarely advertise the fact
that such encryption techniques have been used. Unlike most physical
searches, the investigator cannot simply look at a computer and tell whether
the files have been encrypted. Therefore, he cannot predict ahead of time
which type of search to expect.

Another difficulty in deciding what rules to apply to computer
searches is that the methodologies and tools needed for conducting such
searches are dramatically different from those needed to search a house or a
car. The tools used to search in the physical world are relatively basic: light
sources, a good pair of eyes, and a keen intuition for ferreting out evidence.
The investigator might also make use of simple technology such as
fingerprint powder or Luminol to illuminate evidence unseen to the naked
eye. The investigator often needs something more than the digital
equivalent of these tools in searching a computer because nothing is visible
to the naked eye. Even for the most basic computer search, the analyst
must use software to translate the digital data into some recognizable form.

Thus, trying to analogize digital computer searches to traditional
physical searches is problematic. This analogy would be akin to the courts
having compared the search of automobiles to horse-drawn carriages or
houses when they first appeared on the scene. Instead, courts should just
treat computers for what they are and analyze the Fourth Amendment issues
accordingly. Yet simply because the technology has changed does not
mean that traditional analyses of Fourth Amendment issues should be
discarded. While adjustments may be necessary to conform search and
seizure law to digital principles, a wholesale makeover or “special
approach” to accommodate them is unnecessary.

In order to develop a consistent set of guidelines to help frame search
and seizure law in this area, the first issue that must be decided is what
information the warrant should contain to authorize the seizure of
computers and digital storage devices. To comply with the Fourth
Amendment probable cause requirement, an officer must first demonstrate
that the computer or storage media in question will contain evidence of the
alleged crime. Officers should not be allowed to seize computers and other
digital devices based on vague assertions that computers generally may
contain relevant evidence of criminal activity. Because I argue that officers
should be entitled to inspect the contents of a computer freely once they
have shown proper justification for its seizure, this step is particularly important to protecting personal privacy interests.

Under current law, once investigators have demonstrated probable cause to enter a home or office, they are allowed to search any place the object of their search is likely to be found.\footnote{United States v. Ross, 456 U.S. 798, 820-21 (1982) (holding a warrant that authorizes an officer to search a home for illegal weapons also provides authority to open closets, chests, drawers, and containers in which the weapon might be found).} Depending on the type of object sought, a computer could be viewed as merely another container to be searched. Since the computer is, in effect, the digital equivalent of a house due to its immense storage capacity and the variety of information capable of being stored on it, courts should view computers as the front door of a house or office, rather than just another object or container found within the house. This standard would require a showing of particularized suspicion before any computer or storage device found within the home or office could be searched. It would prevent computers from being treated like traditional containers, which can at most hold a few pairs of clothes or other objects.

In most cases, this requirement would have little practical effect. Where it is suspected that the computer is intimately involved in the commission of the crime—as in computer fraud or child pornography—the government will have little trouble making this showing of particularized suspicion.\footnote{Agent Reese stated that it would “not be a big issue” to add a paragraph to a warrant if officers discovered a computer during a search and had reason to believe it contained evidence relating to the investigation. Interview with Collin Reese, supra note 20.} For example, if the allegation is that a doctor has committed Medicare fraud, it is perfectly logical to assume that the medical records evidencing the fraud are kept on the medical office’s computer system.

However, where only generalized suspicion exists as to a computer’s relevance to the suspected criminal activity or as a possible repository for evidence, then the government should not be allowed to search a computer for evidence of a crime. Assume agents have a warrant to search the house for evidence of alleged sale and manufacture of drugs. While the agents would be permitted to search areas of the home and containers where such evidence could be found, they would not be permitted to search a computer found in the home based on general allegations alone. They would have to demonstrate probable cause exists, separate and apart from the first warrant to search the home, that the computer contains evidence of drug sales or manufacture such as statements from an informant that the suspect kept such information on his computer.

Once it has been demonstrated that officers have a lawful right to seize a computer, the next question that must be addressed is under what
circumstances should officers be allowed to remove computer equipment to an off-site location for inspection and potential copying. Judge Koziński argued quite eloquently in *Hill* that the difficulties inherent in conducting computer searches are so well known today that officers need not detail these concerns in their affidavits. The Ninth Circuit rejected this approach, instead requiring that the affidavit spell out the reasons for believing such removal will be necessary. This requirement seems to put form over substance. Given its obvious complexities, common sense suggests that the off-site search of a computer is more convenient for both examiner and computer owner. As long as the owner is not deprived of use of the computer for an unreasonable period of time, off-site inspection and/or copying of relevant files or directories is the preferable search method in this context.

The more troubling question is how to separate relevant computer data and files from intermingled, irrelevant data. Winick advocated the adoption of the *Tamura* procedure for all computer searches, requiring the impoundment of the computer data until a magistrate has had an opportunity to review it and separate the relevant from the irrelevant. While this method sounds good in theory, I hazard to guess it would prove unworkable in practice. If law enforcement officials had to stop their investigation and seek judicial oversight every time they seized a computer, law enforcement would grind to a halt in the United States. This scenario would be akin to requiring law enforcement officials to impound the contents of a desk or a car before being allowed to search it. The Fourth Amendment does not require the use of such judicial handcuffs. As long as an officer demonstrates he has probable cause to search the computer, then he should be allowed to search all of its contents without having to sort the data first. If an individual is foolish enough to store evidence of criminal activity on the same computer that he stores personal information, then he should suffer the invasion of privacy that comes with the territory, just as if he had placed the intermingled information in a desk drawer.

However, the search of a business computer requires a more concerted effort to separate the wheat from the chaff. Wholesale seizures of the records of a business are unwarranted, absent extraordinary circumstances. As a result, when applying for a warrant to search business computers, law enforcement officers should have to demonstrate

---

345 United States v. Hill, 459 F.3d 966, 975 (9th Cir. 2006).
346 Winick, supra note 51, at 107.
probable cause for the seizure of particular servers, desktop computers, directories, and storage media that may contain the sought-after material. If that requirement is not possible beforehand, the officers must provide for procedures to accomplish this task on site. To that end, agents applying for a search warrant of a business should describe procedures for accomplishing this on-site sorting to assure the magistrate that they are taking no more than what is necessary and will avoid the wholesale removal of business computers.

In addition, where it is anticipated beforehand or discovered during the search that records of innocent third parties, unconnected to the allegations of criminal activity, are intermingled with the records evidencing a crime, then the procedures for magistrate review outlined in *Tamura* should be implemented. This is the only way to ensure that the privacy rights of innocent third parties are not violated and the confidentiality of the records will be maintained. In such instances, the investigator must seek judicial assistance to separate out the irrelevant, third-party files before searching further. The magistrate could either conduct the review himself with the assistance of a forensic investigator or appoint a special master to do the same. In order to protect the privacy of such third parties, this review must occur before, not after, the investigator has had an opportunity to search the files (as was the case in *CDT*).

While the use of taint teams has been approved by some courts as an available alternative to judicial oversight, their use should be strongly discouraged and limited to specific situations where judicial oversight would be impractical. The use of taint teams still reveals the files' content to investigators; it just attempts to minimize the damage resulting from that disclosure by erecting a Chinese Wall. It can hardly be comforting to innocent third parties that the sanctity of their records depends solely on the integrity of the members of the taint team. Members

---

348 This rule would be easy to implement in the context of the search of a business office where it is expected that such records will be intermingled. However, it is not so easy to implement where a laptop, used for both business and personal reasons, is seized. One can imagine a situation where the officers seize a laptop which at first blush appeared to contain only personal files, but upon further examination was discovered to also contain business records. In such an instance, the officer should stop the search of the computer and apply for a magistrate's assistance in sorting out the relevant material from the irrelevant, and potentially confidential, business information.

349 Kerr advocates the use of search protocols in this instance: “Search protocols may be useful in specific circumstances. For example, searches of computers believed to contain privileged documents present special concerns. In such cases, investigators may specify a search protocol to explain how the analysts will handle privileged documents.” Kerr, *supra* note 66, at 576 n.199.

350 For example, if the material is particularly complex or voluminous, the use of a magistrate or special master may unreasonably delay an investigation or prosecution.
of a taint team may not always be as diligent as they should be in performing their duties or may not have purely noble motives.351 Who is to say that a prosecutor, who discovers evidence of criminal activity unrelated to the main focus of the investigation, will not have an incentive to disclose the confidential information and pursue that lead? As a result, the use of taint teams should be strictly limited.

Regardless of what review method is chosen, these special procedures should be reserved for cases implicating heightened confidentiality and privacy concerns such as searches of medical or law offices. Searches of personal computer or regular business records do not implicate such concerns, and thus they should not be subjected to this extra layer of judicial oversight.

The CDT decision also poses a related question: Should the government be allowed to execute search warrants against independent third parties who are not targets of the investigation, or should subpoenas be the exclusive investigatory tool permitted to be used in such instances? The preferred method for obtaining this material is obviously by subpoena. The issuance of the subpoena provides notice to the third party such that it has an opportunity to litigate issues of privacy, confidentiality, and overbreadth prior to the seizure of the records. The justifications for using search warrants—to preserve the element of surprise and prevent destruction of records—are often lacking in these situations. However, where the use of a warrant is necessary (such as where the object of the investigation works in the medical or law office where the records are kept), investigators must identify these reasons in their warrant application.

The next issue that must be resolved is whether courts should adopt the second part of the Carey/Winick approach, which requires that officers use specific search protocols in conducting searches of hard drives and other storage media. The Winick approach would permit officers to use more invasive search techniques only where they can articulate their suspicions that the suspect has encrypted or altered the files.352 This requirement is unworkable. As detailed by Orin Kerr, forensic computer examiners cannot easily predict the course their searches may take.353 Examiners may

351 The recent admission of a Colorado Springs attorney to leaking transcripts of the BALCO grand jury testimony to San Francisco Chronicle reporters is a case in point. Although bound by legal and ethical obligations not to reveal secret grand jury testimony, the attorney violated the sanctity of the grand jury. The attorney’s agreement to plead guilty will keep the reporters from serving jail time as a result of their refusal to give provide his name as the source of the leak. Troy E. Renck, Reporters to Avoid Jail with Lawyer’s Plea, DENV. POST, Apr. 15, 2007, available at http://www.denverpost.com/search/ci_5229261.

352 Agent Reese notes that he has encountered very few cases where suspects have encrypted files. Interview with Collin Reese, supra note 20.

353 Kerr, supra note 66, at 575.
encounter suspects who have deleted files in an effort to hide their tracks, and as such, will have to search every file to look for and retrieve deleted files. In addition, examiners should not be required to take the suspect's word for it that the files are labeled properly. This would be akin to forcing investigators who had come upon paper files written in a foreign language to rely on the accuracy of the suspect's translation.

Given that officers should be permitted to inspect all files on a hard drive, then the question of whether the plain view doctrine should apply must be answered next. As outlined in Part IV, the justifications underlying the plain view doctrine are typically not present in the computer search realm. Since the evidence remains under the control of investigators while it is being searched, the additional step of applying for a second warrant to seize new evidence creates a minimal burden. Assuming arguendo that the plain view doctrine should apply to computer searches, it should only be applied in a limited set of circumstances where the incriminating character of the evidence is obvious on its face. If it takes more than a casual glance to determine the file's incriminatory character, then the government cannot justify its seizure under the plain view doctrine. On the other hand, if its incriminatory character is obvious (such as a photo of child pornography or some other crime) then its seizure should be permitted.

VI. CONCLUSION

The CDT decision is notable because it touches on several issues on the frontier of digital search and seizure law. It is laudable for the freedom it gives officers to conduct digital searches due to their inherent complexity. However, it sets a dangerous precedent with respect to both the limited amount of protection it provides to third parties whose medical records have

---

354 Interview with Collin Reese, supra note 20.
355 See supra Part IV and note 341.
356 Ziff looks at the plain view doctrine from a slightly different angle. Under this doctrine, in order for the contents of a file to be seized, he hypothesizes that the determination of its incriminatory nature must occur within the time it takes to determine if the document is within the scope of the warrant:

During the time in which the warrant allows a searching officer to view the contents of a file, the second condition of the plain view doctrine must be met—the incriminating character of the file must be immediately apparent. After a determination can be made that the contents of a given file are outside the scope of the warrant, the officer's authority to examine that file under the warrant expires. Therefore, if the incriminating character of a file only becomes apparent after the officer has determined that the file is outside the scope of files to be seized under the warrant, the plain view doctrine cannot apply because the authority of the warrant has expired and the officer is no longer in a lawful position from which to view the file.

Ziff, supra note 68, at 866.
been seized pursuant to a search warrant and the standard that it sets for determining motions for return of property. In the Ninth Circuit’s view, as long as government agents can assert some legitimate need or interest in seized property, such as relevance to an ongoing or even a potential future criminal investigation, the government can review confidential medical records of innocent third parties and retain copies of the seized information.\(^{357}\)

In their zeal to ferret out illegal steroid distribution, government investigators trampled on the rights of over a hundred baseball players and countless other professional athletes. Confidential medical records containing the most private of information (drug screen results) were exposed to prying eyes.\(^{358}\) All of this was done in flagrant disregard of Department of Justice regulations which expressly prohibited the conduct engaged in by the government in this instance. The Ninth Circuit was all too happy to oblige by sanctioning their tactics. What's next? Will Lance Armstrong’s chemotherapy records be subject to review if the government decides to investigate allegations of blood doping during the Tour de France? Then, if his records are intermingled with other patient records, will those unrelated records be subject to review as well? The Framers of the Fourth Amendment could not have intended such perverse results.

Courts that consider these issues in the future should be wary of granting the government too much power. If the government is granted this much leeway in investigating the crime of illegal drug distribution, what check, if any, will be left if the alleged crime is terrorism? The \textit{CDT} decision highlights the need for the Supreme Court to lay out a set of consistent guidelines which will protect both the privacy interests of the individual and at the same time accommodate law enforcement’s legitimate need for flexibility in conducting computer searches.

\(^{357}\) \textit{CDT}, 473 F.3d 915, 937 (9th Cir. 2006).

\(^{358}\) As discussed previously in Part III.A, the government agents seized the Tracey directory which contained almost 3000 drug test results for various sports. \textit{See supra} note 227. The agents used the information to obtain new search warrants to seize all specimens and records relating to the over one hundred non-BALCO players. \textit{Id.} at 924.