
Derek Regensburger

There is an old saying that bad facts make bad law. After the Ninth Circuit issued its en banc ruling in United States v. Comprehensive Drug Testing, Inc., a new question must be asked—do bad facts which make bad law in an emerging and hotly debated area of law force the Supreme Court to step in and resolve the issue?

A couple of years ago, I wrote an article in this journal analyzing the decision in United States v. Comprehensive Drug Testing, Inc. ¹ (CDT I) issued by a panel of the Ninth Circuit.² The decision upheld the seizure of computer records containing drug testing results of ten major league baseball players involved in the Balco steroid distribution scandal as well as those of countless other players from baseball and other professional sports leagues. Under the initial decision, the government was allowed to keep the testing records of all the athletes and expand the scope of its investigation into steroid usage and distribution in Major League Baseball.³ While I applauded the decision for its analysis of computer search law generally, I criticized the opinion for failing to protect the testing records of the players who were not the subject of the original search warrants and for not ordering their return.⁴

By way of background, the government had executed search warrants in two different districts (one for the test results and one for the physical urine samples) and issued subpoenas for the same records in a third district.⁵ The government’s initial warrant application had requested only the records pertaining to the ten named players that were the focus of its Balco investigation.⁶ When the government executed the warrants, it seized a computer hard drive which contained the test results for the ten named players which were the focus of its investigation. The drive also contained the names and results of some 2900 other athletes who were not the targets of the investigation.⁷ All three district court judges found that the government had overstepped the bounds of its authorization. Two courts ordered the return of all information related to the testing of unnamed athletes who were not the focus of the investigation. A third court quashed the subpoenas for the same information. The courts ordered the government to return the testing results and samples for the non-Balco players it had seized under Rule 41(g) of the Rules of Criminal Procedure.⁸

---

¹ CDT I, 473 F.3d 915 (9th Cir. 2006).
³ CDT I, 473 F.3d at 923-24.
⁴ Bytes, supra at 1152-53.
⁵ CDT I, supra at 920-22.
⁶ United States v. Comprehensive Drug Testing, Inc. (CDT III), 579 F.3d 989, 993 (9th Cir. 2009).
⁷ CDT, supra at 947 (Thomas, J., concurring in part, dissenting in part).
⁸ CDT III, 579 F.3d at 993-94.
Just prior to publication of my article, the panel withdrew its initial opinion and reissued it (CDT II). This time around, the panel determined that the government had not timely appealed one of three district court orders which had formed the basis of its appeal. Judge Cooper’s order was issued in the Central District of California with regard to the seizure of the electronic testing records at the CDT facility. Judge Cooper held that the government had failed to comply with the conditions of the warrant pertaining to the segregation of computer data for which the government had probable cause to seize and which was intermingled with the test results for other athletes. She also held that the government had exhibited callous disregard for the rights of the nonBalco players. Since the government had not timely appealed this ruling, the panel determined that it did not need to address the issue of whether the government had exhibited callous disregard for the rights of the unnamed athletes. However, since the MLBPA had based its challenge to the search of the Quest lab in Nevada on the ground that the CDT files were illegally seized, the court still upheld the seizure of the testing results and reversed the lower courts’ orders to return the property. It also reversed the order of Judge Susan Illston quashing the subpoenas to CDT and Quest for the same information. The Major League Baseball Players Association (MLBPA) then requested a rehearing of the decision en banc.

The Ninth Circuit granted the motion and recently released its opinion (CDT III) authored by Judge Kozinski. The en banc panel reversed the three-judge panel’s decision and once again ordered the government to return testing results and drug test samples for the athletes not involved in the Balco investigation. The legal basis of its opinion primarily rested on the doctrine of issue preclusion. The panel held that since the government had not timely appealed Judge Cooper’s order, it was bound by those factual determinations. The en banc panel also held, however, that Judge Illston’s order, quashing the subpoenas issued in the Northern District of California, had preclusive effect on the core legal questions resolved in Judge Mahan’s Order issued in Nevada regarding the government’s failure to segregate intermingled data. Since the government had failed to timely appeal Judge Illston’s order as well, the court found that the Cooper and Illston rulings had effectively resolved all issues contained in the government’s appeal. Thus, the Ninth Circuit disposed of the government’s appeal in its entirety on the ground of issue preclusion.

Had the court stopped there, this ruling would have been unremarkable. But the court did not do so. After dispensing with the outcome of the case on procedural grounds, the

---

9 CDT II, 513 F.3d 1085 (9th Cir. 2008).
10 Id. at 1098-99.
11 CDT I, supra at 953-54.
12 Id.
13 CDT II, supra at 1098-99.
14 Id. at 1113.
15 Id. at 1114.
16 CDT III, 579 F.3d 989 (9th Cir. 2009) (en banc).
17 Id. at 997.
18 Id.
19 Id.
court then launched into a ten-page discussion of the issues central to the appeal, laying out wide-ranging new rules for the issuance of computer search warrants, particularly with respect to the handling of intermingled files and data. The dicta that followed on these issues sparked a plethora of comments in articles and blog posts.20

The opinion set strict new guidelines for the issuance of search warrants for electronic information and established protocols for segregating intermingled data. In doing so, the court went far beyond what the Ninth Circuit (and most other circuits) had previously required for the issuance of computer search warrants. This is notable since Judge Kozinski himself had issued a ruling much more favorable to the government five years earlier in *United States v. Hill.*21 Perhaps more surprising, however, was the complete lack of legal analysis offered for these sweeping new rules. The Court simply announced them without stating whether they were intended as an exercise of its supervisory authority over the district court or as constitutional mandates under the Fourth Amendment. This led Orin Kerr, a George Washington University law professor and former U.S. Attorney who helped draft the DOJ guidelines on computer searches, to label this decision as “bizarre” and “one of the strangest opinions that I have ever read.”22 Thus, the debate has ensued whether this decision will revolutionize computer forensics or will be a mere historical footnote en route to getting much-needed guidance on these issues from the Supreme Court.

I. The Five New Restrictions Pertaining to Searches of Electronically Stored Information Announced by the Ninth Circuit

In reversing the three judge panel’s ruling, the Ninth Circuit established five guidelines for future searches of electronic information:

1) Magistrates should insist the government waive reliance upon the plain view doctrine in digital evidence cases.

2) Segregation and redaction must either be done by specialized personnel or an independent third party. If the segregation is to be done by government computer personnel, it must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant.

3) Warrants and subpoenas must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other judicial fora.

---


21 F. Supp. 2d 1081 (C.D. Cal. 2004), rev’d in part, 459 F.3d 966 (9th Cir. 2006).

4) The government’s search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents.

5) The government must destroy or, if the recipient may lawfully possess it, return nonresponsive data, keeping the issuing magistrate informed about when it has done so and what it has kept.

In this article I will review each of these five restrictions.

a. Waiver of reliance on the plain view doctrine in a warrant application

First, the Ninth Circuit required that the government eliminate the plain view doctrine from consideration in future discussions of whether it will be able to retain evidence that is not within the scope of a warrant. The court agreed with the government that it should be able to carefully examine the contents of every file stored in a computer to determine whether the data that sought under the warrant is concealed, compressed, erased, or booby-trapped. However, the court objected to the government’s argument that it should be able to subsequently use any evidence of criminal activity that it comes across on the ground that it was in plain view. The court feared that this would create “powerful incentive” to seize more evidence rather than less. It cautioned that “[o]ne phrase in the warrant cannot be read as eviscerating the other parts, which would be the result if the ‘otherwise legally seized’ language [of the warrant] were read to permit the government to keep anything one of its agents happened to see while performing forensic analysis of a hard drive.”

To prevent this from occurring, the court mandated that the government should avoid relying on the plain view doctrine in future warrant applications, and if it doesn’t, the magistrate judge should order that intermingled data be separated by an independent third-party under supervision of the court.

Eliminating the plain view doctrine in the context of computer searches is a good thing, in my opinion. As I stated in my earlier article, the justifications for the plain view doctrine in the physical world--that evidence could disappear if investigators had to delay to get a second warrant--are not present in the digital realm. Unlike a search of a home where evidence could be lost or destroyed if it is not seized immediately, no such concern exists in the context of computer searches where the evidence remains in the possession of the forensic analysts at all times. Because of this, the act of obtaining a second warrant to seize any additional information discovered during the search of electronic data would not be a significant burden.

The Ninth Circuit quite correctly pointed out that the application of the plain view doctrine in the digital realm creates the very real possibility that every warrant for

---

23 CDT III, supra at 1006.
24 Id. at 998.
25 Id.
26 Bytes, supra at 1201.
electronic information will in effect become a general warrant.\footnote{Id. at 1004.} Because there is no other way to tell what a digital file contains without opening or examining it, the government could claim that its contents are always in plain view once it has done so. This is of particular concern for independent third parties whose information is stored on the same server or hard drive as the information law enforcement is seeking under the warrant. That party may have no inkling that his information is being seized and subject to scrutiny by the government.

What is odd about the court’s pronouncement, however, is that it requires the government to waive reliance on the plain view doctrine in future warrant applications. The court instructed that the “government should, in future warrant applications, forswear reliance on the plain view doctrine or any similar doctrine that would allow it to retain data to which it has gained access only because it was required to segregate seizable from non-seizable data.”\footnote{Id. at 998.} In essence, this is telling the magistrate judge to deny a warrant application not based on whether it is supported by probable cause or is sufficiently particular, but because he has concerns over how it will be executed. It would be akin to telling a detective that he can have a warrant for stolen cars if he promises not to look in the suspect’s underwear drawer along the way. This removes the power to oversee the lawful execution of the warrant from where it properly resides—the district court judge. Ordinarily, the court steps in to correct an overzealous act of investigators only after the suspect has had his rights violated, not before.

Another issue with regard to this waiver requirement is its apparent lack of enforceability. Will the district court be forced to suppress evidence because the government relies on the plain view doctrine to justify its seizure even though it promised it wouldn’t do so in the warrant application? Aside from the question of whether such a waiver would be enforceable, one has to ask why the court did not simply state that the plain view doctrine is no longer applicable to computer searches period. Regardless of whether the government tries to rely on the doctrine to justify future seizures of electronic evidence outside the scope of the initial warrant, it would be a pointless exercise if courts refused to recognize its applicability. Orin Kerr hypothesizes that the court may have been hesitant to do so since the government did not actually use the seized testing results to institute new prosecutions and thus no suppression question was at issue.\footnote{Orin Kerr, Do Magistrate Judges Have a Power to Refuse to Sign Warrants Based on Expectations of How a Warrant Would be Executed?, Volokh Conspiracy, (August 26, 2009), http://volokh.com/posts/1251311240.shtml.}

b. Use of forensic computer personnel or independent experts must be used to segregate information relevant to the investigation.

The second restriction that the Ninth Circuit imposed limits the initial review and segregations of intermingled data to computer personnel or neutral third parties appointed by the court. In other words, case agents handling the investigation cannot conduct such
a review. The court was particularly critical of the government in this regard since the agents had made no attempt to segregate the drug test results of the ten named players from the other results contained on the seized hard drive, but instead used the positive drug test results from other baseball players to issue additional warrants.\textsuperscript{30}

The court cautioned that if case agents were allowed to view the computer data alongside the forensic computer personnel, it would defeat the purpose of limiting the review of intermingled data in the warrant in the first place. The court found future warrants should specify that forensic computer experts unassociated with the investigation have to be used to review the intermingled data, and that case agents could only examine data for which probable cause had been shown.\textsuperscript{31} The court also indicated that the magistrate judge should appoint an independent expert or special master to segregate files where the party subject to the warrant is not under investigation and the privacy interests of innocent third parties are implicated by the search.\textsuperscript{32} If this type of procedure was not followed, the court feared that the government would sweep up large quantities of data in the hope that it could “dredge up” information that it could not otherwise lawfully seize.\textsuperscript{33} The court concluded that this case was an example of “deliberate overreaching” by the government to seize data for which it did not have probable cause.\textsuperscript{34}

Although the use of independent experts to review intermingled computer data sounds good in theory, this requirement is much broader than is necessary. First, it will likely prove to be burdensome to investigating agencies to comply with. It would require hiring two sets of computer experts—one to assist the investigation team and one to serve as the review team. While this is not an issue in larger cities, it may become a burden in more isolated areas where there are relatively few personnel.

Second, the bulk of computer search warrants are issued for personal computers which do not implicate the rights of innocent third parties. As I pointed out in my original article, taint teams or special masters are necessary only where the interests of innocent third parties are involved such as in the search of medical or legal offices.\textsuperscript{35} In my view, the need for a taint team or appointment of a special master is not present when the government conducts only a search of a private individual’s computer.

Third, the requirement that only forensic computer specialists, unrelated to the investigation, be allowed to initially examine the data is unnecessarily restrictive. A question should have been asked by the court whether forensic specialists would have the necessary training to recognize contraband and evidence of criminal activity in order to effectively accomplish this task without the aid of law enforcement expertise. For example, would a computer technician have the necessary knowledge to know what files

\begin{itemize}
\item \textsuperscript{30} Id. at 999.
\item \textsuperscript{31} Id. at 1000.
\item \textsuperscript{32} Id.
\item \textsuperscript{33} Id.
\item \textsuperscript{34} Id.
\item \textsuperscript{35} Bytes, supra at 1204.
\end{itemize}
contained on a medical office server would be related to a Medicare fraud investigation and which are not?

The better approach to this problem is to appoint a taint team composed of both case agents and forensic experts which is unconnected to the investigative team. Once the data is separated, the information relevant to the investigation would be handed over to investigators and a Chinese wall would be erected, barring communication between investigators and the taint team. Of course, if protection of privacy interests of third parties unrelatable to the investigation is of paramount concern, I suggested in my earlier article that the court should appoint a special master or independent expert for this purpose.36

c. Risk of concealment or destruction must be detailed in the warrant application

The court also required the government to state in future warrant applications the actual degree of risk that the electronic information it seeks will be concealed or destroyed if the government is not allowed to review each and every file on the hard drive. The court criticized the government for not revealing that CDT had agreed to keep the data intact until its motion to quash the subpoena had been ruled upon.37 As a result, it instructed lower courts, in determining a motion for return of property or suppression of evidence, to weigh heavily any lack of candor in this regard against the government.38

This requirement is akin to the court requiring the government to hire a psychic. While it is true that most electronic evidence examined by the government is not encrypted or concealed, it is very difficult for government agents to predict ahead of time whether such tactics will be encountered.39 Although it might seem logical to conclude that child pornographers and terrorists would be more likely to engage in such deceptive tactics (and thus the government could properly allege the likelihood of such tactics being used in warrant applications involving these types of cases), this requirement would make it difficult, if not impossible, to effectively search digital storage media in other contexts. Assume that the government applied for a search warrant in the case of a suspected burglar to examine his computer for evidence of the sale of stolen property. Unbeknownst to the agents, the burglar had disguised the files containing his fence contacts and sale of stolen merchandise as cooking recipes. If the agents had no reason to anticipate that the burglar had concealed evidence in this manner, they would not have seen the need to request the use of sophisticated search tools, and they will not discover the critical evidence as a result.

Given that the court had already eviscerated the plain view doctrine in the context of electronic searches, there was no need to include this additional prophylactic restriction. If the government cannot use information concerning unrelated criminal activity it

36 Id. at 1205-06.
37 CDT III, at 998.
38 Id.
39 Bytes, supra at 1161.
discovers or is forced to apply for second warrant to do so, then this additional restriction serves no purpose.

d. Search protocols

While recognizing the need for law enforcement officials to sift through large quantities of data to find concealed or disguised evidence, the majority clearly feared giving the government carte blanche to achieve this end. The court restricted the government’s ability to seize unrelated information further, holding that the search protocols used to discover the information sought under the warrant have to be limited to identifying that information only. In other words, the government may not use such search tools to ferret out unrelated contraband or evidence of criminal activity which may also be present on a hard drive. To that end, the court held that sophisticated search tools, which can be used to examine all files on a hard drive, may not be used without prior authorization in the warrant. It also held that the government must establish probable cause for the search of electronic media, i.e., that files evidencing criminal activity will be found on the media being searched.

These restrictions are essentially an adoption of the approach laid out by the Tenth Circuit in United States v. Carey. There, the Tenth Circuit refused to let agents retain evidence of child pornography found on a computer hard drive since they had failed to seek a second warrant for authorization to view the suspect image files. The court also required that agents limit the search of electronic media to key words designed to locate files relevant to information sought under the warrant. It is strange that the Ninth Circuit chose to rely on the Carey doctrine since most other circuits (including the Ninth) have since rejected it.

Even the Tenth Circuit has recently backtracked from some of the dicta laid out in Carey. Although the court refused to abandon the concerns expressed in Carey, it applied a more pragmatic approach to requiring search protocols in United States v. Burgess. It noted that while the warrant did not “direct the search by describing filename extensions, filenames or directory structure,” it found that the scope of the search was “explicitly constrained by content – computer files containing evidence of drug use or trafficking.” The court rejected the argument that computer searches have to be constrained by search protocols in the warrant application:

40 CDT III, supra at 999.
41 Id.
42 Id.
43 172 F.3d 1268, 1276 (10th Cir. 1999). I would also note that it hard to tell what precedent the Ninth Circuit was relying on since it did not cite any authority in support of these new restrictions.
44 See, e.g., United States v. Gray, 78 F.Supp.2d 524 (E.D. Va. 1999) (Seizure of pornographic images of children was proper under a warrant which entitled agents to seize evidence relating to unauthorized access of a government computer because all files stored on a computer may be examined to determine whether they contain evidence that falls within the scope of a warrant); United States v. Adjani .
45 576 F.3d 1078, 1092-93 (10th Cir. 2009).
46 Burgess, 576 F.3d at 1093.
It is unrealistic to expect a warrant to restrict the scope of the search by directory, file name or extension or to attempt to structure search methods – that process must remain dynamic. While file or directory names may sometimes alert one to the contents (e.g., ‘Rssina Lolitas,’ ‘meth stuff,’ or ‘reagents’), illegal activity may not be advertised even in the privacy of one’s personal computer – it could well be coded or otherwise disguised. . . In summary, it is folly for a search warrant to attempt to structure the mechanics of the search and a warrant imposing such limits would unduly restrict legitimate search objectives.⁴⁷

Judge Kozinski himself had previously refused to require magistrate approval for the use of sophisticated search tools in Hill. He likened the situation to officers having to ignore white powdery substances during a search of a home if the bags were labeled “flour” or “talcum powder.”⁴⁸ The Ninth Circuit adopted his reasoning verbatim on this issue.⁴⁹ This raises an interesting question which the court did not address: if the use of search protocols was a bad idea three years ago, why did the Ninth Circuit think their use is now necessary?

e. The government must return all copies of information not authorized by warrant

Finally, the court required the government to return (or destroy) any electronic data it had seized which is not pertinent to its investigation and destroy all copies of that data still in its possession.⁵⁰ This restriction appears to conflict with the new version of Rule 41(f) which will take effect December 1, 2009. The new rule permits agents to retain copies of electronically stored information that is seized pursuant to a warrant.⁵¹

The court’s order also lacks clarity as to when, if ever, the government could use evidence it obtains which is outside the scope of the warrant. Under this decision, the court made clear that the government cannot just seize such information and make subsequent use of it. If the government wishes to retain data as to which no probable cause was shown in the original warrant, the court mandated that agents must now seek a second warrant for that information.⁵² Of course, this assumes that government investigators would learn of the existence of such incriminating information in order to obtain a second warrant. As discussed above, the court limited the access of government investigators to only the information covered by the terms of the warrant and required forensic specialists to perform the segregation of data.

---

⁴⁷ Id.
⁴⁸ Hill, supra at 1090.
⁴⁹ United States v. Hill, 459 F.3d 966, 968 (9th Cir. 2006).
⁵⁰ CDT III, supra at 1000-01.
⁵¹ The new rule 41(f)(1)(B) will provide in part: . . . In a case involving the seizure of electronic storage media or the seizure of copying of electronically stored information, the inventory may be limited to describing the physical storage media that were seized or copied. The officer may retain a copy of the electronically stored information that was seized or copied. Fed. R. Crim. P. 41(f)(1)(B) (emphasis added).
⁵² CDT III, supra at 1001.
This raises another question left unanswered by the Ninth Circuit: what do forensic experts do with contraband or evidence of criminal activity that they come across which is unrelated to the task at hand of separating information under the terms of the warrant? Can they hand it over to the investigation team for review so that a second warrant can be obtained or are they required to simply return or destroy that information? Also, does it make a difference whether the incriminating evidence is found in the files of the target of the investigation or in the files of unrelated third parties?

Implicit in the court’s holding is the notion that the government cannot comb electronic information for evidence of unrelated criminal activity and then make subsequent use of that information against third parties which are unconnected to the investigation. Even had the government taken great care to separate the drug testing records of the Balco players from the other athletes on the directory (such as utilizing forensic specialists alone to inspect the drug testing results), I doubt that the court would have allowed the government to seek a second warrant for the positive drug test results of the players unassociated with the Balco investigation. Thus, it would appear that where the segregation team uncovers evidence of criminal activity relating to independent third parties, the government cannot use that information to acquire additional warrants.

The corollary to the above question is what can forensic experts do with incriminating information that is unrelated to the subject of the warrant but is connected to the target of the investigation. For example, assume that government forensic experts stumble across child pornography files while searching for evidence of terrorist conspiracies on the personal laptop of a suspect. Do they have to destroy those files without taking any further action or can they apply for second warrant to seize the child pornography? Although the answer is unclear under the court’s ruling, it would appear that agents could use this information if they applied for a second warrant to seize it.

Given the existence of these unanswered questions, the more logical approach would have been to restrict investigator’s access only to those records and files of third parties unrelated to the investigation. Once the records and files relevant to the target of the investigation have been separated from those of individuals unrelated to the investigation, the government should be able to inspect and review the electronic files of the target of its investigation for information within the scope of its warrant. If, during investigators’ inspection of the relevant data they stumble across unrelated evidence of criminal activity, then the agents should be able to apply for a second warrant to utilize that evidence.

II. Rule 41(g) is the Correct Remedy to Order Return of Property

In addition to its computer search protocols, the court also held that return of property under Rule 41(g) was the proper remedy for the government’s overreaching. The court distinguished between the retention of lawfully seized property on the one hand and the retention of illegally seized property on the other. The court found that Rule 41(g) is

53 Id.
broader than a motion to suppress, noting that Rule 41(g) applied to both lawfully and unlawfully seized property.\textsuperscript{54}

Ordinarily, the government is allowed to retain evidence that is has seized as long as it can demonstrate a continuing need for the property in an ongoing investigation. However, the court noted that Rule 41(g) contemplates the return of all copies and originals where equitable considerations justify it.\textsuperscript{55} The court instructed that where there is an intentional disregard for the rights of third parties, there is no need to balance the government’s need for the evidence:

> When, as here, the government comes into possession of evidence by circumventing or willfully disregarding limitations in a search warrant, it must not be allowed to benefit from its own wrongdoing by retaining the wrongfully obtained evidence or any fruits thereof. When the district court determines that the government has obtained the evidence through intentional wrongdoing-rather than through a technical or good-faith mistake-it should order return of the property without the need for balancing that is applicable in the more ordinary case.\textsuperscript{56}

Thus, the court found that Judge Mahan did not abuse his discretion in ordering return of the testing samples unrelated to the Balco investigation.\textsuperscript{57}

This aspect of the court’s opinion is quite correct. The government’s argument that it should be allowed to retain the testing results of the other athletes because the information is relevant to its investigation of steroid distribution in baseball is circular logic. It would allow the government to circumvent the Fourth Amendment simply by alleging that it is entitled to keep information it never had probable cause to seize in the first place because it is now relevant to its investigation. This is like arguing it’s okay to keep dolphins and other sea creatures you’re not allowed to fish for simply because they got caught in your tuna nets.

III. What does the Future Hold for Electronic Searches?

The most troubling aspect of Judge Kozinski’s opinion is the complete lack of legal analysis to support any of these new restrictions the court announced. While I believe some of the regulations imposed by the court are necessary, particularly those protecting the rights of innocent third parties, the decision provides precious little guidance to future courts on how to apply them. The court gave almost no explanation as to why it imposed various restrictions, what situations those restrictions applied to, and provided no case citations in support of them. This aspect of the case reminds me of line from Blazing Saddles: “Precedent? We don’t need no stinking precedent.”\textsuperscript{58}

\textsuperscript{54} Id.
\textsuperscript{55} Id. at 1002.
\textsuperscript{56} Id. at 1003.
\textsuperscript{57} Id.
\textsuperscript{58} My apology to Mel Brooks.
The court also failed to state whether it was basing its decision on its supervisory powers or on Fourth Amendment principles. This is an important distinction. Supervisory rulings only impact federal courts—they do not apply to state decisions unlike rulings grounded in constitutional theory. A supervisory ruling is far easier to alter or revoke than a constitutional ruling since it may be freely revised by the courts or by legislation. There are three bases for the court’s exercise of its supervisory power: to implement a remedy for the violation a recognized statutory or constitutional right; to preserve judicial integrity by ensuring that conviction rests on appropriate considerations before a jury; and to deter future illegal conduct. Consequently, courts possess power to correct injustices which do not amount to statutory or constitutional violations. They have frequently used this power to discourage future government or prosecutorial misconduct.

The district court’s ability to exercise its supervisory powers is not unlimited, however. In the context of suppression hearings, for example, the Supreme Court has limited the scope of supervisory powers where the government’s actions did not detrimentally impact the defendant’s Fourth Amendment rights. Consequently, it held that a court couldn’t substitute its supervisory power for “established Fourth Amendment doctrine” by invoking its supervisory powers to suppress evidence which was unlawfully seized from a third party not before the court.

Judge Kozinski has also previously espoused the notion of judicial restraint for courts exercising their supervisory powers. In United States v. Simpson, the Ninth Circuit ruled on the propriety of a district court’s dismissal of an indictment. In reversing the district court’s order, Judge Kozinski noted that “sleazy investigatory tactics alone – unless so offensive that they amount to a violation of due process – do not provide the ‘clear basis in law’ required for the exercise of the supervisory power.” He cautioned that in exercising their supervisory power, “judges must be careful to supervise their own affairs and not those of the other branches.”

This notion is particularly important in the context of a ruling on Rule 41 motion for return of property since the court’s jurisdiction rests on its supervisory powers. Courts have cautioned that this power should be exercised with “great restraint and caution.” If the Ninth Circuit was indeed invoking its supervisory power to create a new set of regulations governing electronic searches, it was exercising anything but judicial restraint.

60 Id.
62 Leslie, 783 F.2d at 569 (Williams, J., dissenting).
65 Id. At 736.
66 927 F.2d 1088 (9th Cir. 1991).
67 De Almeida v. United States, 459 F.3d 377, 382 (2d Cir. 2006).
in this case. Certainly, there is no dispute that the district courts in this case could have (and did) use their supervisory powers to sanction the government for overreaching conduct by ordering the return of the unrelated testing results. However, the Ninth Circuit greatly expanded this power by applying a sweeping new set of regulations to all future searches of electronic data, not just the searches of the Comprehensive Drug Testing and Quest labs at issue in the case.

The other alternative is that the court based these new restrictions on Fourth Amendment principles. As noted above, constitutional rulings are much harder for courts to later overturn. Other circuits and even state courts could give the decision strong deference in determining what rules to institute in their own jurisdictions. As a result, the impact of this decision could extend far beyond ordering the government to return the samples and data surrounding the positive test results of a hundred or so baseball players.

A more nefarious interpretation of this ruling is that the Ninth Circuit was intentionally vague in this regard, trying to goad the Supreme Court into providing more guidance in the area of electronic searches. What better way to attract the attention of the high court than by issuing a new set of draconian restrictions without any authority or need? If this was the case, the Ninth Circuit was taking a big risk. Because of the factual and procedural irregularities of the CDT case, the Supreme Court may not accept certiorari. The government may also choose to wait to appeal until a case with more favorable facts comes along. Of course, if the government does wait, it will have to deal with these new restrictions in all investigations in the Ninth Circuit involving electronic data searches until then.

We may never get the answer to these intriguing questions, however. Amazingly, the Ninth Circuit may hear this case a fourth time. The Ninth Circuit has requested the parties in this case to file briefs addressing whether the case should be reheard en banc by the full court. Under Ninth Circuit rules, en banc hearings are ordinarily comprised of only 11 of the 28 judges on the court. The rules also provide for the opportunity for the case to be reheard before all 28 judges. Such motions are rare, however. Only three have ever been filed and none has ever been granted.

---