

The Legal Intelligencer

Select '**Print**' in your browser menu to print this document.

Copyright 2010. ALM Media Properties, LLC. All rights reserved. *The Legal Intelligencer*.

Page printed from: [The Legal Intelligencer](#)

[Back to Article](#)

To Avoid 'Plain View,' Investigators Need Blinders

Leonard Deutchman

05-18-2010

Editor's note: Second of two parts. The first part can be found [here](#).

In last week's column, [I wrote about cases from the 1st, 4th and 7th U.S. Circuit Courts of Appeal that applied the plain view doctrine to computer searches.](#)

This column discusses the 9th Circuit's opinion in *United States v. Comprehensive Drug Testing*, which rejected the doctrine, and looks at the pros and cons of both approaches. Comprehensive Drug Testing concerned the well-known "Balco," or Bay Area Lab Cooperative, investigation by the federal government of steroid use by Major League Baseball players, particularly those who were suspected of having received steroids from Balco.

Search, Suppression

Comprehensive Drug Treatment, an independent drug testing business, was engaged under an agreement by MLB and the Major League Baseball Players Association to test urine samples collected from players for substances banned by MLB, according to the opinion. The results were to be anonymous and confidential. The purpose of the testing was to determine whether more than 5 percent of the players tested positive, in which case more testing would be done. CDT engaged Quest Diagnostics to perform the tests. CDT maintained the list of tested players and results, while Quest maintained the samples.

During the Balco investigation, federal investigators learned of 10 players who had tested positive for steroids, according to the opinion. They secured a grand jury subpoena in the Northern District of California for CDT to produce all of its records regarding the testing — not just the records for the 10 who had tested positive. CDT and the players association moved to quash the subpoena. But on the same day, investigators obtained a search warrant in the Central District of California to search CDT's facilities for the records of the 10 specified players. Execution of that warrant yielded the "Tracey Directory," which contained information and test results involving, in addition to the specified players, hundreds of other baseball players and athletes engaged in other professional sports. Investigators also obtained a search warrant in the District of Nevada for the urine samples Quest kept in its Las Vegas facilities. They seized those samples and obtained additional warrants for records kept by CDT and Quest as well as new subpoenas in the Northern District of California, demanding production of the records they had seized, according to the opinion.

The CDT search warrant included a protocol which the personnel executing the warrant had to follow.

Under it, investigators first had to determine on scene whether the data pertaining to the 10 identified players could be segregated and seized, according to the opinion. Assuming not (as was the case), law enforcement personnel who were trained in computer forensics but who were not the case agents would have to determine, on scene, what computer media would have to be seized to ensure that the seizure of media was confined to only that on which the data sought would reside. Those same forensic experts would then, off-scene, segregate the sought-after data from the remaining data seized and return all media found not to contain sought-after data. Only then could the case agents inspect the sought-after data.

The suppression court found that federal agents ignored the protocol.

The case agents looked at all of the data seized, including information pertaining to players other than the 10 specified, and used the information acquired to obtain subsequent warrants in California and Nevada. The suppression court characterized the case agents as having acted with "a callous disregard for the rights of those persons whose records were

seized and searched outside the warrant."

Federal officials, relying upon *Horton v. California*, argued the plain view exception to the warrant requirement applied. The officials reasoned that: 1) the search warrant authorized the case agents to look through the data seized for the sought-after data, which included the Tracey Directory since that file contained the names of the 10 specified ballplayers; 2) while so doing, the agents saw in plain view data pertaining to the other players who tested positive for banned substances; so, 3) the agents did not need to ignore what they saw in the Tracey Directory not pertaining to the 10 specified players, but instead could lawfully seize that other data, the data in dispute.

The 9th Circuit, en banc, rejected the argument.

The court reasoned that, because the nature of electronically stored data is such that agents executing search warrants must seize media broadly and search it off-site, to let the federal officials' argument prevail would be to give law enforcement too much power to look outside the scope of a warrant in order to find the data that fell within the scope. The court saw the federal officials' argument as the first step on a slippery slope, reasoning that if "the government can't be sure whether data may be concealed, compressed, erased or booby-trapped without carefully examining the contents of every file — and we have no cavil with this general proposition — then everything the government chooses to seize will, under this theory, automatically come into plain view." This will "create a powerful incentive" for agents "to seize more rather than less."

To prevent this erosion of Fourth Amendment protections in computer searches, the court held 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. If the government doesn't consent to such a waiver, the magistrate judge should order that the seizable and non-seizable data be separated by an independent third party under the supervision of the court, or deny the warrant altogether." Second, all data must be segregated and redacted either by specialized personnel or an independent third party, who will not disclose to the investigators any information other than that which is the target of the warrant. An investigative search protocol must be designed to uncover only the information for which there was probable cause, and only that information may be examined by the case agents. Finally, officials must destroy or, if the recipient may lawfully possess it, return non-responsive data.

Circuits Split

The 1st, 4th and 7th Circuits rejected the 9th Circuit's argument that applying the plain view exception to computer searches eviscerates the particularity requirement of the Fourth Amendment.

Interestingly, two of the opinions address Comprehensive Drug Testing directly.

In *United States v. Farlow*, the 1st Circuit noted that the conduct of the agents in Comprehensive Drug Testing was "egregious" and that "no other circuit has gone as far as the Ninth to require such significant preconditions on the issuance of search warrants for computers" as the protocol requiring law enforcement to forswear the plain view exception and rely upon independent analysts to search the data. The 1st Circuit found that "the far preferable approach" was to "examine the circumstances of each case, to assess the validity of the computer search protocol, to determine whether the police strayed from the authorized parameters of the search warrant, and to hold the police to constitutional standards in the context of a motion to suppress." The suppression court can consider appropriate remedies if "the police conduct is as egregious as the Ninth Circuit found in" Comprehensive Drug Testing, the 1st Circuit ruled, but protocols should be avoided and remedies imposed only after "fact-intensive, considered analysis."

The 1st Circuit also found that Comprehensive Drug Testing "create[d] more problems than it solve[d]."

Without doubting the 9th Circuit's conclusion that the agents "deliberately overreached and seized evidence for which they had no probable cause," the 1st Circuit cautioned to use "the traditional sanction for police misconduct of this sort," which "remains exclusion of evidence." The problem with the 9th Circuit's protocol, the 1st Circuit ruled, was that it imposed "extraordinary precautions against police misconduct for all applications for a warrant to search a computer, assuming misconduct will be the rule, not the exception."

Such a prophylactic measure was not needed, the 1st Circuit continued, as there was "no evidence that police disobedience of search warrant limitations is so widespread to compel such onerous pre-issuance procedures, and at the very least the more traditional remedies should be tried first." Furthermore, the 9th Circuit's requirement that the issuing judicial officer insert a protocol for preventing agents "from examining or retaining any data other than that for which probable cause is shown" would test even "the most computer literate of judges," and it was "unrealistic" to believe that "a busy trial judge is going to be able to invent one out of whole cloth or to understand whether the proposed protocol meets ill-defined technical search standards," the 1st Circuit ruled.

Finally, the 1st Circuit noted that requiring investigators to forswear the plain view doctrine was "an extreme remedy better reserved for the unusual, not common case." While the baseball players' use of steroids in Comprehensive Drug Testing was "certainly a matter of notoriety," it was nevertheless "relatively benign in the scope of federal criminality." Not so in the instant matter, the 1st Circuit wrote, where the evidence in plain view was child pornography — "the possession of which is a serious federal felony."

What if, the 1st Circuit asked, the evidence in plain view was "profoundly serious" such as "photographs of a kidnapped child" or "plans to commit acts of terrorism[?]"

In such cases, the "judicial directive to forswear in advance the plain view doctrine ... is equivalent to demanding that a DEA investigative team engaged in the search of a residence for drugs promise to ignore screams from a closet or a victim tied to a chair," the court wrote. In sum, requiring the police "to forswear the plain view doctrine" before conducting computer searches "seems unwise."

The 7th Circuit in *United States v. Mann* also explicitly rejected Comprehensive Drug Testing, finding, with the dissent in Comprehensive Drug Testing, that the forswearing of plain view and following the protocol was an "efficient but overbroad approach." The court, again quoting the dissenters from Comprehensive Drug Testing, found "the more considered approach to be to 'allow the contours of the plain view doctrine to develop incrementally through the normal course of fact-based case adjudication.'"

As with the 1st Circuit, the 7th Circuit found the requirement that all computer search warrants contain the 9th Circuit's protocol unnecessarily burdensome, finding the better course to "counsel officers and others involved in searches of digital media to exercise caution to ensure that warrants describe with particularity the things to be seized and that searches are narrowly tailored to uncover only those things described."

Pros and Cons

The 9th Circuit's approach to computer searches has not been warmly received by other circuits.

All of the arguments in favor of applying the plain view exception to computer searches as well as the specific criticisms of the 9th Circuit's protocol are sound. There is no "find the evidence" button on computer forensics tools. Searching computers requires searching across all files and opening those files which appear to contain the evidence sought; invariably, such search strategies will yield evidence of other crimes. The 9th Circuit's solution to the problem of over-searching is an unwarranted response to what is not a widespread problem: sanctions specific to the facts in Comprehensive Drug Testing could have been imposed without imposing the 9th Circuit's protocol for all computer search cases.

In addition to the unrealistic notion that law enforcement officers take an oath before conducting a search to ignore evidence of other crimes during the conduct of the search, the 9th Circuit's protocols are unrealistic because they are prohibitively expensive.

It is hard to find field agents who can conduct computer-related investigations, expensive to send them to the training they need — and with the changes in both digital media and the forensic tools available, they always need training — and harder still to keep them when private vendors entice them to "greener pastures." The prospect of needing two sets of highly trained investigators, one to do the investigation, the second the computer analysis, is daunting at best.

Moreover, the idea that a second set of "independent" analysts can perform an analysis without discussing their results with the case agents is absurd. The only way to do that is for the analysts to know as much about the investigation as do the case agents, a goal that will not be met in 90 percent of cases and, in the remaining 10 percent, will be met at the cost of those analysts having to spend dozens, if not hundreds, of hours becoming conversant in the case just to meet that goal.

While the analysts are getting up to speed on the case agents' case, independent of the agents, analyses in other cases are put on hold. The only way to resolve this problem is to hire more computer-trained agents and forensic analysts, and neither the money nor the personnel is likely available.

Regardless of the many flaws of the 9th Circuit's protocols, however, George Washington University Professor Orin S. Kerr is nevertheless onto something when he observes that the architecture of a computer is so different from that of a house or container that traditional Fourth Amendment doctrine will have to be re-examined in the digital age.

The other circuits that have taken issue with the 9th Circuit have done so because they have not seen law enforcement using the plain view exception to subvert the Fourth Amendment.

If the courts do see a rise in police misconduct, the police will see a rise in the granting of suppression motions. The 7th Circuit's admonition that law enforcement "exercise caution to ensure that warrants describe with particularity the things to be seized and that searches are narrowly tailored to uncover only those things described" is sound advice. The court in Mann was "troubled" that the analyst did not stop and get a second search warrant once the four files showed "Alerts" that their hash values matched those of known child pornography.

The prudent course for law enforcement to follow when officers come upon evidence of a different crime than the one under investigation is to cease searching and obtain a warrant for that new evidence. Law enforcement officers examining computers should follow that course unless exigencies prohibit it. If they do not, courts will fashion remedies and law enforcement will find those remedies unpalatable, whether they are the protocols of the 9th Circuit or old fashioned suppression of evidence. •

Leonard Deutchman, *esquire is general counsel and administrative partner of LDiscovery, LLC, a firm based in New York City, Fort Washington, Pa., McLean, Va. and Chicago that specializes in electronic digital discovery and digital forensics.*