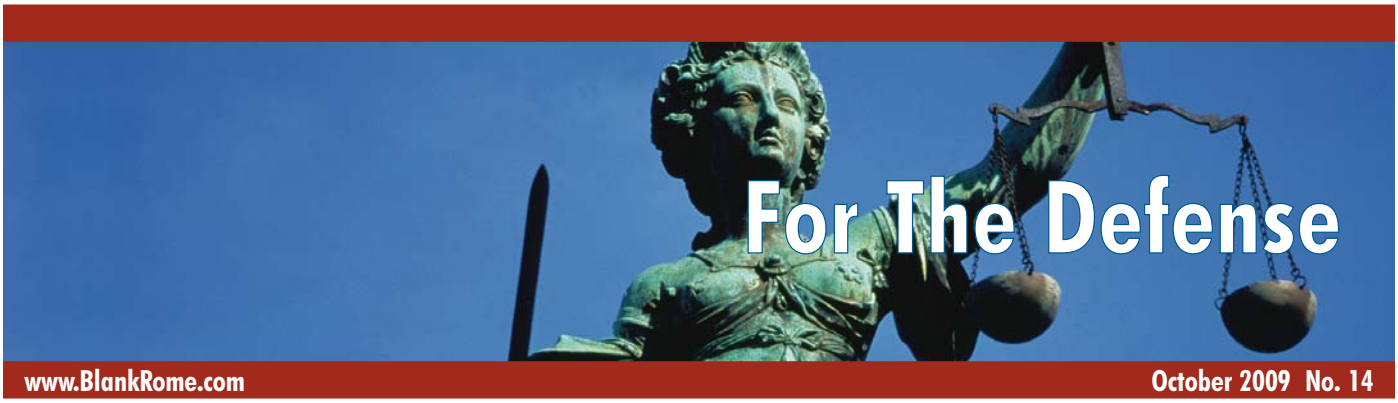
BLANK ROME LLP
COUNSELORS AT LAW



www.BlankRome.com October 2009 No. 14

Steroids In Baseball Impact More Than Just Home Runs:

Ninth Circuit Establishes New Limitations On The Seizure of Electronically Stored Information

By Matthew D. Lee & James T. Strawley

Nearly everyone is familiar with the ongoing federal investigation into steroid use by professional baseball players. What is less known, however, is the impact that such a high profile investigation could have on search-and-seizure jurisprudence. If a recent decision by the United States Court of Appeals for the Ninth Circuit is any indication, the implications could be major. In *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989 (9th Cir. 2009), and two companion cases, the Ninth Circuit, sitting *en banc*, has now established several new procedural limitations on the government's ability to seize and use electronically stored information in criminal cases. In adopting safeguards to prevent the government's "over-seizing" of electronic evidence during the execution of a search warrant, the Court held that the "process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect." *Id.* at 1006. Needless to say, this decision may well have significant implications for government investigative agencies, as well as the subjects of their criminal investigations.

Background

In 2002, a federal grand jury commenced an investigation into the Bay Area Lab Cooperative (Balco) pertaining to suspicions that the lab had provided steroids to a number of professional baseball players. In the wake of the media storm that followed, Major League Baseball (MLB) took steps to begin random drug testing for all of its players. Pursuant to an agreement between MLB and the Players' Association, urine samples were to be collected and tested for banned substances with the results remaining anonymous and confidential. In order to accomplish this random testing, MLB hired Comprehensive Drug Testing, Inc. (CDT), an independent company based in California, to administer the program and collect the specimens from the players. In turn, CDT contracted with Quest Diagnostics, Inc. ("Quest") to conduct the actual testing. After the specimens were tested by Quest, CDT maintained the list of players and their respective results while Quest kept the actual specimens on which the tests were conducted at its laboratory facility in Las Vegas, Nevada.

Federal authorities conducting the investigation of Balco were aware of the ongoing testing being done by MLB, and ultimately learned that ten players had tested positive in the CDT program. As a result, the government undertook a series of attempts to obtain these records.

First, the government obtained a grand jury subpoena in the Northern District of California seeking all "drug testing and specimens" pertaining to MLB in CDT's possession. After failed attempts to negotiate the scope of the grand jury subpoena, CDT and the players filed a motion to quash the subpoena.

Almost immediately after the motion to quash was filed, the government obtained a search warrant in the Central District of California authorizing the search of CDT's facilities in Long Beach, California. Unlike the subpoena issued in the Northern District of California, the search warrant was limited to the records of the ten players as to whom the government had probable cause. However, when the search warrant was executed, the government seized and reviewed the drug testing results of hundreds of MLB players, as well as athletes engaged in other professional sports.

Finally, the government also obtained a search warrant from the District of Nevada for the urine samples on which the tests had been performed. As noted, these specimens were stored at Quest's facilities in Las Vegas. The government subsequently obtained additional warrants for the

© 2009, BLANK ROME LLP. Notice: The purpose of this newsletter is to review the latest developments which are of interest to clients of Blank Rome LLP. The information contained herein is abridged from legislation, court decisions, and administrative rulings and should not be construed as legal advice or opinion, and is not a substitute for the advice of counsel.

records at CDT's facilities in Long Beach and Quest's lab in Las Vegas. The government also served CDT and Quest with new subpoenas in the Northern District of California, demanding production of the same records that it had seized pursuant to the warrants.

CDT and the players subsequently challenged the warrants and various subpoenas. CDT and the players moved for the return of property pursuant to Federal Rule of Criminal Procedure 41(g) in both the Central District of California and the District of Nevada. The Central District of California ordered the property return on the basis that the government failed to comply with the procedures specified in the warrant. The District of Nevada also granted the Rule 41 motion and ordered the return of the seized property, with the exception of materials pertaining to the ten specifically identified players. Finally, the players and CDT also moved to quash the newly issued subpoenas before the Northern District of California. That motion also was granted and the subpoenas were quashed.

The government appealed all three orders and a divided panel of the Ninth Circuit reversed the orders issued by the District of Nevada and the Northern District of California. The matter was then accepted for further *en banc* review.

En Banc Ruling

The Ninth Circuit, sitting *en banc*, upheld all three district court orders.[1] In doing so, the Court also made a number of significant findings and holdings that could ultimately have a major impact on the procedures pertaining to searches for electronically stored information. As noted in the published opinion, the Ninth Circuit took "the opportunity to guide our district and magistrate judges in the proper administration of search warrants and grand jury subpoenas for electronically stored information, so as to strike a proper balance between the government's legitimate interest in law enforcement and the people's right to privacy and property in their papers and effects ...." *Id.* at 994. In particular, the Ninth Circuit discussed the scope of the plain view doctrine in electronic search cases, and has now placed a much greater burden on the government to describe the information it is seeking when applying for a search warrant by requiring that "the government waive reliance upon the plain view doctrine in digital evidence cases." *Id.* at 998, 1006.

In considering the original warrant pertaining to the search of the CDT facilities in Long Beach, the Ninth Circuit agreed with the district court's finding that the government, although granted broad authority for the seizure of electronic data, failed to limit the scope of its search to the ten players for whom the government had probable cause and failed to comply with the specific procedural safeguards set forth in the warrant. *Id.* at 995. These safeguards, which were largely based on the Ninth Circuit's decision in *United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982), included a requirement that the government examine the computer and storage equipment on site to determine if an on-site search was possible as well as significant restrictions on how the seized data was to be handled. *Id.* at 995-96. Specifically, an initial review and segregation was to be conducted by agents not assigned to the case and who were trained in computer searches. *Id.* at 996. Those agents were then to only turn over responsive data to the case agents, and any data that was beyond the scope of the warrant was to be returned to CDT with 60 days. *Id.*

In this instance, "once the items were seized, the requirement of the Warrant that any seized items not covered by the warrant be first screened and segregated by computer personnel was completely ignored." *Id.* at 996 (quoting district court's order). In fact, the government declined an offer by on-site CDT personnel to provide all information pertaining to the ten identified players. Instead, the government copied what is referred to by the parties as the "Tracey Directory" from CDT's computers. Going well beyond what was permitted by the warrant, the "Tracey Directory" contained "information and test results involving hundreds of other baseball players and athletes engaged in other professional sports." *Id.* (quoting district court's order). Despite requests from CDT's counsel that a taint review be conducted by a magistrate or special master, the primary case agent "himself reviewed the seized computer data and used what he learned to obtain the subsequent search warrants issued in Northern and Southern California, as well as Nevada." *Id.* at 997.

Similarly, the district judge in Nevada also found that the government had exceeded its authority with regard to those players beyond the ten specifically identified players. In challenging this order, the government contended that it had complied with the *Tamura* segregation and screening requirements, but noted that it was not required to return the additional data pertaining to other players beyond the ten players specifically identified in the warrant affidavit. In support of this claim, the government argued that the data demonstrating steroid usage by other players was "otherwise legally seized" as authorized by the warrant pursuant to the plain view doctrine. More specifically, the government argued that once the government agents examined the seized computer directory to determine what was contained in the files and what was responsive to the warrant, the additional incriminating information was in the agents' plain view and therefore also was subject to seizure. *Id.* at 997.

The Ninth Circuit rejected this argument as "a mockery of *Tamura*" that would essentially undermine the protections established by the Fourth Amendment because anything the government chooses to seize would automatically come into plain view. In so holding, the Court reiterated the government's own argument to the magistrate judges that broad

1. The Ninth Circuit noted at the outset that the findings of the district courts in the Central and North Districts of California are binding on the government due to their untimely appeal. As such, the Court also concluded that the government's appeal of the third order from the District of Nevada also should be upheld based upon the preclusive effect of the other two orders. *Id.* at 997. Nevertheless, the Court reviewed all three orders to avoid any question about the proper scope of preclusion, and to address the important issues raised.

seizure authority was necessary in terms of electronic data because it is often not immediately possible to determine whether additional data is concealed, compressed, or hidden. *Id.* at 998. Although acknowledging that this broad authority is inherently necessary in many situations, the Ninth Circuit nevertheless noted that "[t]his pressing need of law enforcement for broad authorization to examine electronic records … creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." *Id.* at 1004. Furthermore, "since government agents ultimately decide how much to actually take, this will create a powerful incentive for them to seize more rather than less …." *Id.*

In an effort to "avoid this illogical result," the Ninth Circuit held that a clear limitation should be placed on the ability of the government to rely on the plain view doctrine in electronic search cases:

> 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.

Id.

The Ninth Circuit also established a number of additional procedural safeguards that the government must follow in order to obtain a search warrant pertaining to electronically stored evidence. Recognizing the "reality that over-seizing is an inherent part of the electronic search process," the court of appeals also called for "greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures." *Id.* at 1006. In order to assist magistrate judges in maintaining this balance, the Ninth Circuit made clear that the following precepts must be followed in connection with warrants for electronically stored evidence:

- Magistrate judges should insist that the government waive reliance upon the plain view doctrine in digital evidence cases.
- Segregation and redaction must be either 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.
- 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.
- 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.
- The government must destroy or, if the recipient may lawfully possess it, return non-responsive data, keeping the issuing magistrate informed about when it has done so and what it has kept.

Id.

While it remains to be seen how the *CDT* decision will be received in other judicial circuits, the Ninth Circuit's opinion serves to reiterate the fine balance that courts must strike between the government's law enforcement interests and the protections afforded by the Fourth Amendment in considering whether to authorize a search warrant. This is particularly true given the ever-increasing reliance on electronic data storage. Judges, prosecutors, agents, and defense attorneys must continue to be aware of the changes that the electronic age has and will have on Fourth Amendment jurisprudence, and must be prepared to articulate ways that courts can "update" its prior precedents in order to meet the changing legal landscape. In this regard, any practitioner faced with a case involving the seizure of electronically stored evidence would clearly benefit from a careful review of the holding and rationale set forth in this case. ■

White Collar, Internal & Government Investigations Practice Group

Philadelphia Office	Telephone	Washington, DC Office	Telephone
Ian M. Comisky	215.569.5646	Jane F. Barrett	202.772.5907
Norman E. Greenspan	215.569.5635	Jeanne M. Grasso	202.772.5927
Matthew D. Lee	215.569.5352	Gregory F. Linsin	202.772.5813
Joseph G. Poluka*	215.569.5624	Jennifer Peru Gary	202.772.5863
James T. Strawley	215.569.5664	Hardy Vieux	202.772.5997
New York Office	**Telephone**	Charles E. Wagner	202.772.5963
Jerry D. Bernstein	212.885.5511	Shawn M. Wright	202.772.5968
Laura A. Brill	212.885.5533	**Princeton, NJ Office**	**Telephone**
Michelle Gitlitz Courtney	212.885.5068	Nicholas C. Harbist	609.750.2991
James V. Masella III	212.885.5562	Stephen M. Orlofsky	609.750.2646
Inbal Paz	212.885.5010	John J. Pribish	609.750.2647
Marc Rothenberg	212.885.5121	*Editor	
Leonard D. Steinman	212.885.5524		