

Ninth Circuit Announces New Protocols for the Government's Handling of Electronic Evidence

August 31, 2009

On August 26, the U.S. Court of Appeals for the Ninth Circuit issued its decision in *United States v. Comprehensive Drug Testing, Inc.* The result is an extremely positive development for employers concerned with protecting the confidentiality of business records that are the subject of a government search warrant.

The opinion concerns the government's seizure of thousands of electronic records relating to an anonymous drug testing program provided for in a collective bargaining agreement between Major League Baseball (MLB) owners and the MLB Players' Association. The Ninth Circuit ordered the records returned and called their seizure "a deliberate overreaching by the government in an effort to seize data as to which it lacked probable cause."

For employers that negotiate drug testing arrangements with union-represented employees into their collective bargaining agreements, this decision is a vital development because it supports the confidentiality and anonymity of these programs. The Ninth Circuit's specific guidelines for the collection and review of electronic records also safeguard employers from the prospect of overly broad searches and seizures of electronic data, unsupported by probable cause and unchecked by the involvement of a neutral judicial officer.

Factual and Procedural Background

In 2002, the federal government launched a criminal investigation into the Bay Area Lab Cooperative (Balco), a company that was suspected of providing steroids to professional athletes from a number of sports. That same year, the MLB Players' Association entered into a collective bargaining agreement with MLB that provided for the suspicionless drug testing of all players by Comprehensive Drug Testing, Inc. (CDT).

Federal investigators in the Balco case learned of 10 players who had tested positive through the testing program conducted by CDT. The government then secured a grand jury subpoena in the Northern District of California seeking all "drug testing records and specimens" pertaining to MLB players in CDT's possession. CDT eventually moved to quash this subpoena, but the government, through search warrants issued by the Central District of California and the District of Nevada, obtained electronic records stored at CDT's facilities in Long Beach and records maintained by Quest Diagnostics, Inc. (Quest), the laboratory that performed the actual tests on the players' urine samples. New subpoenas were then served

on CDT and Quest in the Northern District of California seeking the information that was seized via the search warrants.

CDT and the MLB Players' Association moved for the return of the seized property in the Central District of California and the District of Nevada pursuant to Federal Rule of Criminal Procedure 41(g). They also moved to quash the subpoenas issued to CDT and Quest in the Northern District of California, which were based on information obtained by the search warrants pursuant to Federal Rule of Criminal Procedure 17(c). CDT's and the MLB Players' Association's motions were granted by all three District Courts; the Ninth Circuit noted that "[m]ore than one of the judges" from these cases "commented that they felt misled or manipulated by the government's apparent strategy of moving from district to district and judicial officer to judicial officer in pursuit of the same information, and without fully disclosing its efforts elsewhere."

On appeal by the government, a Ninth Circuit panel reversed the rulings of the District of Nevada and the Northern District of California but dismissed as untimely the government's appeal of the ruling of the Central District of California. The Ninth Circuit then voted to rehear the appeal en banc. The en banc opinion concurred with the finding that the Central District of California judgment was untimely but reversed the earlier panel's decision and affirmed the judgments of the District of Nevada and the Northern District of California.

The Ninth Circuit's Decision

The Ninth Circuit's en banc opinion chastised the government for its tactics in procuring the electronic records at issue. For example, the affidavit submitted by the government in support of obtaining a federal search warrant for CDT's records identified "generic hazards" of retrieving electronic data, including the ease with which computer data could be disguised, erased, or hidden. The government's affidavit of probable cause made no mention, however, of CDT's offer to preserve the records sought. The Ninth Circuit held that omitting such "highly relevant information" showed a lack of candor that "shall bear heavily against the government in the calculus of any subsequent motion to return or suppress the seized data."

The Ninth Circuit also found that the government "utterly failed" to follow the specific procedural safeguards in the warrants it was issued. The requirement that any seized items were to be first screened and segregated by computer personnel was "completely ignored." Brushing aside an offer by onsite CDT personnel to provide all information pertaining to the 10 identified baseball players, the government copied from CDT's computer the "Tracey Directory," which contains, in the District Court of Nevada's words, "information and test results involving hundreds of other baseball players and athletes engaged in other professional sports."

The Ninth Circuit noted that CDT repeatedly requested that "all material not pertaining to the specific items listed in the warrant be reviewed and redacted by a Magistrate or Special Master before it was seen by the Government." The case agent, however, "himself reviewed the seized computer data and used what he learned to obtain the subsequent search warrants issued in Northern California, Southern California, and Nevada."

The government made the argument that the Tracey Directory was in "plain view" once government agents examined CDT's computers in an effort to find information on the 10 named baseball players. The Ninth Circuit dismissed this argument because the government was unable to show any effort by the

government to separate the data for which probable cause was identified in the search warrant from all of other data on CDT's computer. The Ninth Circuit noted that accepting such an argument would be equivalent to allowing government investigators to "take everything back to the lab, have a good look around and see what [they] might stumble upon." To guard against such "unlawful conduct," the court held that a search warrant should include "a protocol for preventing agents involved in the investigation from examining or retaining any data other than that for which probable cause is shown."

If the government seeks information on particular people, a search protocol must be designed to discover only the data regarding those named individuals for whom probable cause exists. In order to protect against government investigators unlawfully obtaining possession of computer data that was not called for in the search warrant and for which no probable cause exists, the Ninth Circuit instructed that segregation of data should be performed by "specially trained computer personnel who are not involved in the litigation" and who will not communicate any information learned during the segregation process absent further court approval. Importantly, for third parties not suspected of criminal wrongdoing, "the presumption should be that the segregation of the data will be conducted by, or under close supervision of, an independent third party selected by the court."

Specific Guidance

The Ninth Circuit's opinion sets forth the following steps that courts should take when the government seeks to obtain a subpoena or search warrant to examine a computer hard drive or other electronic storage medium in order to find incriminating files:

1. "Magistrates should insist that the government waive reliance upon the plain view doctrine in digital evidence cases." (citations omitted)
2. "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." (citations omitted)
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." (citations omitted)
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." (citations omitted)
5. "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." (citations omitted)

Key Lessons

- If your company's records are the subject of a federal search warrant, it is vital for the company to follow carefully established protocols and to make and document a complete record of the company's efforts to comply with the preservation and production of the electronic data that is the subject of the search warrant. The Ninth Circuit specifically noted the offer by CDT's counsel to

provide all information pertaining to the 10 identified baseball players and the company's request that all electronic data not pertaining to the specific items listed in the warrant be reviewed and redacted by a magistrate or special master before it was seen by the government.

- Company counsel should ensure that reliable searches can be performed on their electronic data systems so that government investigators are not able to use the unreliability of a data search as an excuse for an overinclusive request for electronic records.
- Company counsel should ensure that any search warrant for its electronic records includes a search and review protocol outlined by the court. If the search warrant does not include such protocols, company counsel should go directly to the magistrate who issued the warrant and request sequestration of the seized material until a specialized forensic examiner segregates it.
- Subject companies and their counsel should proactively identify for the court how it proposes to segregate the subject electronic data—for example, key word searches, custodian, dates, and location.
- Company counsel should not hesitate to go to the magistrate if a government search warrant involves the search for electronically stored data that could affect the privacy interests of clients, employees, vendors, etc. The Ninth Circuit's decision sanctioned the use of Federal Rule of Civil Procedure 41(g) to seek the return of improperly seized property in these circumstances. "The government argues that Rule 41(g) is inapplicable because it is not designed to be used as a suppression motion. But CDT and the Players' Association are not seeking to have evidence suppressed, as they are not criminal defendants. Rather, by forcing the government to return property that it had not properly seized, CDT is preserving the integrity of its business and the Players Association is protecting the privacy and economic well-being of its clients, which could easily be impaired if the government were to release the test results swept up in the dragnet."
- Subject companies should request that the segregation of any data be conducted by, or under the close supervision of, an independent third party selected by the court.

The Ninth Circuit's opinion is a recognition of and an effort to combat the "serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." As a result, this decision provides "clear rules to follow that strike a fair balance between the legitimate needs of law enforcement and the right of individuals and enterprises to the privacy that is at the heart of the Fourth Amendment." These rules should be utilized by employers to protect the confidentiality of data requested via a government search warrant.

If you have any questions about the information contained in this LawFlash, please contact any one of the following Morgan Lewis attorneys:

Philadelphia

Nathan J. Andrisani

215.963.5362

nandrisani@morganlewis.com

San Francisco

John H. Hemann

415.442.1355

jhemann@morganlewis.com

Lisa Tenorio-Kutzkey

415.442.1309

ltensorio-kutzkey@morganlewis.com

Washington, D.C.

Peter Buscemi	202.739.5190	pbuscemi@morganlewis.com
Jonathan C. Fritts	202.739.5867	jfritts@morganlewis.com
Barbara “Biz” Van Gelder	202.739.5256	bvangelder@morganlewis.com

Morgan Lewis associate Jonathan W. Light contributed to this LawFlash.

About Morgan Lewis’s Corporate Investigations and White Collar Practice

Attorneys in Morgan Lewis’s national Corporate Investigations and White Collar Practice represent and counsel companies and individuals through all phases of criminal investigations and prosecutions. Our practice focuses on three broad areas of client service: corporate investigations and related crisis management, corporate and individual defense, and corporate compliance. We provide representation at every step of a corporate crisis, from the earliest stages of government investigations through trial. We routinely assist clients during the crisis management exercise of responding to—and preparing for—the execution of a search warrant.

About Morgan, Lewis & Bockius LLP

Morgan Lewis is an international law firm with more than 1,400 lawyers in 22 offices located in Beijing, Boston, Brussels, Chicago, Dallas, Frankfurt, Harrisburg, Houston, Irvine, London, Los Angeles, Miami, Minneapolis, New York, Palo Alto, Paris, Philadelphia, Pittsburgh, Princeton, San Francisco, Tokyo, and Washington, D.C. For more information about Morgan Lewis or its practices, please visit us online at www.morganlewis.com.

This LawFlash is provided as a general informational service to clients and friends of Morgan, Lewis & Bockius LLP. It should not be construed as, and does not constitute, legal advice on any specific matter, nor does this message create an attorney-client relationship. These materials may be considered **Attorney Advertising** in some states. Please note that the prior results discussed in the material do not guarantee similar outcomes.

© 2009 Morgan, Lewis & Bockius LLP. All Rights Reserved.

