Ninth Circuit En Banc Panel Adopts Safeguards For Subjects Of Search Warrants Involving Electronically Stored Information

BRIAN C. ROCCA AND SETH WEISBURST

The authors examine a circuit court decision that limits the government's ability to seize electronic data from subjects of criminal investigations.

The Ninth Circuit Court of Appeals, sitting *en banc*, has adopted certain 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." This decision has potentially significant implications for both government regulators and the subjects of their criminal investigations.

BACKGROUND

In *United States v. Comprehensive Drug Testing, Inc.*,[1] commonly referred to as the "BALCO" case, the United States Attorney for the Northern District Court of California conducted an investigation of the Bay

Brian C. Rocca, counsel in the Antitrust and Trade Regulation Group in the San Francisco office of Bingham McCutchen LLP, can be reached at brian.rocca@bingham.com. Seth Weisburst, an associate in the firm's San Francisco office, can be reached at seth.weisburst@bingham.com.

Published in the November 2009 issue of Privacy & Data Security Law Journal.

Area Lab Cooperative ("BALCO"), which the government suspected of providing steroids to Major League Baseball players. The Major League Baseball Players Association agreed to anonymous and confidential drug testing during the 2003 season for the purpose of determining the extent of steroid use among players. Comprehensive Drug Testing, Inc. ("CDT") administered the confidential drug testing program and maintained a list of players and their test results.

The government obtained a warrant issued by the District Court for the Central District of California which authorized the search of CDT's Long Beach facilities. Even though the warrant was limited to the records of only 10 players, the government seized and reviewed commingled electronic data which included drug-testing records for hundreds of players (and many others). The government later obtained additional warrants for records at CDT and at Quest Diagnostics, Inc., the laboratory in Las Vegas which performed the tests.

When CDT and the players moved in the Central District of California for return of the seized property, the court ordered the property returned, finding that the government had failed to comply with the procedures specified in the warrant (the "California Order"). When the same parties made a similar motion in the District Court of Nevada, the court, on similar grounds, ordered the government to return all seized information that did not relate to the 10 identified players (the "Nevada Order").

THE NINTH CIRCUIT'S RULING

The government appealed the orders and a divided panel of the Ninth Circuit reversed the Nevada Order and found the appeal from the California Order to be untimely. The Ninth Circuit then took the case *en banc* and, on August 26, 2009, contrary to the earlier panel, affirmed the Nevada Order (and again dismissed the appeal of the California Order as untimely).

Comprehensive Drug Testing, Inc. relies on (and updates) *United States v. Tamura*,[2] which outlined procedural safeguards in the execution of search warrants, focusing on paper records. *Tamura* disapproved of the wholesale seizure of documents and the government's failure to return materials which were not the subject of the search. *Tamura* also suggested

that where documents are "so intermingled that they cannot feasibly be sorted on site…the Government [should] seal[ ] and hold[ ] the documents pending approval by a magistrate of a further search." If officers are aware of the need for large-scale removal of material, they should specifically apply for this authorization beforehand, and it should only be granted where on-site sorting is infeasible and there are no other practical alternatives.[3]

Comprehensive Drug Testing, Inc. acknowledges the tension between law enforcement officials' need to retrieve electronically stored information and the privacy rights of search warrant subjects and third parties. While there is a pressing need for broad authorization to examine electronic records (which are often intermingled with other data), the Ninth Circuit expressed concern "that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant."

The plain view exception to the warrant requirement further complicates matters. Under that exception, law enforcement officials may seize items which they observe and immediately recognize as evidence or contraband while they are engaged in a lawful search. In the electronic context, the government by necessity must often examine a larger directory of data to find the particular files it seeks. While reviewing this larger directory, the government in this case claimed that incriminating data was in plain view, and that the government could then retain and use this new incriminating data even if it was not specifically called for in the warrant. In *Comprehensive Drug Testing, Inc.,* the Ninth Circuit held that allowing this to continue would transform an authorization to search some computer files into an authorization to search all the computer files. *Comprehensive Drug Testing, Inc.* mandates that "[t]he 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."[4]

THE CIRCUIT COURT'S GUIDANCE

Specifically, the Ninth Circuit offers the following guidance for magistrates, government investigators, and the subjects of search warrants:[5]

- Magistrates should insist that the government, prior to execution of the warrant, waive reliance on the plain view doctrine when searching through digital evidence.[6]
- Segregation and redaction of data must be done by specialized personnel or an independent authority, and these personnel must not disclose to investigators working on the matter any information which is not the specified target of the warrant.[7]
- Warrants and subpoenas must disclose both the actual risks of destruction of electronically stored information and any prior efforts to seize the information in other judicial fora.[8]
- The government must design its search protocol to uncover only the information for which it has probable cause, and only that information may be examined by the case agents.[9]
- The government must return non-responsive data if the recipient may lawfully possess it. If not, the government must destroy the non-responsive data. The government must also keep the issuing magistrate informed about any data destroyed, returned, or kept.[10]

Companies subject to search warrants issued by the federal courts should insist that these procedures and safeguards are followed (at least in the districts which comprise the Ninth Circuit), in order to protect their own Fourth Amendment Rights, the confidentiality of electronic information, and the privacy rights of third parties whose information may be intermingled with the seized data.

As of the date of this article, the Ninth Circuit is reviewing briefs related to the government's request for rehearing *en banc*.

NOTES

[1] Case Nos. 05-10067, 05-15006, and 05-55354, 9th Cir. August 26, 2009, *en banc*.

[2] 694 F.2d 591 (9th Cir. 1982).

[3] *Id*. at 595-97.

[4] *See* p. 11891 of the Opinion.

[5] *See* pp. 11892-93 of the Opinion.
[6] *See* pp. 11876-77.
[7] *See* pp.11880-81.
[8] *See* pp. 11877-78, 11886-87.
[9] *See* pp. 11878, 11880-81.
[10] *See* pp. 11881-82.