White-Collar Crime

Andrews Litigation Reporter

VOLUME 24 ★ ISSUE 2 ★ NOVEMBER 2009

Expert Analysis

The Blurring of Plain View

By Michael Horowitz, Esq., Jodi Avergun, Esq., and April Oliver, Esq.

For nearly four decades, the "plain view" doctrine, permitting a police officer to seize incriminating evidence without a warrant when discovered in plain view during a lawful entry, has been a fundamental precept of criminal procedure.[1] However, that doctrine has proved to be problematic when used to justify the seizure and subsequent use of vast amounts of data contained within hard drives, thumb drives and other electronic storage devices, much of it unrelated to the underlying conduct specified in a warrant.

In a provocative opinion from the *en banc* 9th U.S. Circuit Court of Appeals, Chief Judge Alex Kozinski has prescribed strict procedures regarding search warrant applications for the seizure of electronically stored information and sharply limited the government's ability to rely on the plain-view doctrine in the case of digital searches.[2] The divided panel of 11 judges upheld two district courts' rulings that federal prosecutors had wrongly seized an electronic spreadsheet from a drug testing business that was not itself under investigation.

The "plain view" doctrine has proved to be problematic when used to justify the seizure and subsequent use of vast amounts of data contained within electronic storage devices.

The implications of the decision are far-reaching. Unless and until the opinion is appealed to the U.S. Supreme Court, the 9th Circuit has put considerable restrictions on the future use of the plain-view doctrine in cases involving digital evidence.

The Facts

In 2002 the U.S. government began an investigation of the Bay Area Laboratory Cooperative, a company specializing in the development of performance-enhancing drugs. Well known major-league baseball players were among the professional athletes suspected of receiving these drugs from BALCO.[3] As controversy grew over

WEST®

steroid use by athletes, Major League Baseball initiated mandatory drug testing for all players. The league guaranteed the players' union that the tests would be conducted anonymously and confidentially.

The CDT Warrant

On April 7, 2004, a magistrate judge in the U.S. District Court for the Central District of California issued a warrant for the search of Comprehensive Drug Testing, which was involved in administering and collecting drug test specimens from MLB players, among others.[4] The CDT warrant specified the names of 10 baseball players implicated in the BALCO matter and authorized seizure of test records, as well as written and electronic materials regarding CDT's role in the testing.[5] Accordingly, the CDT warrant contained procedural restrictions to ensure that electronic data beyond the scope of the warrant would not be available to the federal prosecutors.

The underlying affidavit supporting the warrant recited a litany of potential problems with on-site examination of computer evidence, including the many ways in which evidence can be hidden and erased. This "made a strong case for off-site examination and segregation of the evidence seized," according to the 9th Circuit's opinion. Thus, the magistrate judge granted broad authority for seizure of electronic data, including "the right to remove pretty much any computer equipment found at CDT's Long Beach facility, along with any data storage devices, manuals, logs, or related materials," the opinion said.

However, the CDT warrant also provided that government computer specialists not working on the case would determine whether segregation of data could be performed on site and would also have a role in off-site segregation and review.

The government requested the search warrant from a judge in the Central District of California shortly after CDT had moved to quash a grand jury subpoena for substantially the same evidence issued in the Northern District of California at the government's request.[6] As part of its motion, CDT had agreed to keep its data intact until the Northern District judge decided the matter. None of this information was disclosed by the government in its warrant application to the judge in the Central District.

The Raid

A total of 12 federal agents, accompanied by a computer forensic expert, raided CDT's Long Beach office April 8, 2004.[7] The raid involved lengthy negotiations by telephone with CDT's counsel.[8] During one of the phone conversations, the government learned that CDT had two computers on which information relevant to the search warrant could be found.[9]

The agents soon isolated a hard-copy document "with names and identifying numbers for all MLB players, including some of the 10 named BALCO players."[10] A CDT director then offered the agents a hard-copy document that contained only the test results for the 10 players listed in the search warrant.[11] The agents rejected the offer and continued their search.

> *The sweeping nature of the 9th Circuit's opinion cannot be overstated, nor can its potential importance to courts and litigants involved in criminal investigations.*

Later in the day a CDT employee identified a relevant computer directory. This electronic directory, known as the Tracey directory, contained all the relevant files for CDT's drug tests on athletes.[12] The government's computer forensic expert determined on site that, rather than making a forensic copy of the entire CDT computer hard drive, the government would copy and take instead only the Tracey directory for later search and segregation. However, the Tracey directory itself included hundreds of files with drug test results beyond those sought by the warrant.[13]

Thus, the U.S. government carried away an electronic spreadsheet that included 104 MLB players' drug test results, as well as those of many other athletes. Soon after seizure, the government's case agent personally reviewed the Tracey directory before it had been analyzed and segregated by an independent team and "identified files authorized by magistrate judge[] for seizure, including the master file of positive drug test results."[14] Relying on the plain-view doctrine, the government used this information to obtain subsequent search warrants issued by the U.S. District Courts for the Northern and Central Districts of California and the District of Nevada.[15]

Following the search, the identities of a number of MLB players not identified in the warrant but who had reportedly tested positive as reflected in the spreadsheet were reported in the media. The 9th Circuit *en*

banc ruling embraced the lower court's view that the government displayed a "callous disregard for … those players as to whom the government did not already have probable cause and who could suffer dire personal and professional consequences from a disclosure."

Now, five years after the Tracey directory was originally seized, the propriety of the government's conduct in acquiring the information is finally being settled. The sweeping nature of the 9th Circuit's opinion cannot be overstated, nor can its potential importance to courts and litigants involved in criminal investigations. Indeed, the opinion gives parties aggrieved by a seizure of electronically stored information critical new bases to challenge those searches, and it also gives judicial officials new, though perhaps unjustifiable, criteria by which to evaluate search warrants. However, the opinion raises almost as many questions as it answers.

Legal Analysis

The 9th Circuit's approach, embodied in Chief Judge Kozinski's lengthy opinion, was purposefully sweeping in its reach. In affirming the two district courts' orders invalidating the search warrants and ordering return of the seized information, the court handed down procedural guidelines that specify, in concrete detail, the steps law enforcement and judicial officers now should take when collecting and reviewing electronic evidence in a criminal matter. The ruling squarely focused on "the procedures and safeguards that federal courts must observe in issuing and administering search warrants and subpoenas for electronically stored information."

The Government's Plain-View Argument

In defending its warrants in the district courts, the government relied heavily on the plain-view doctrine, asserting that its seizure and review of the entire Tracey directory were appropriate because the federal agents complied with procedures outlined in a prior 9th Circuit opinion, *United States v. Tamura*.[16] That case, decided in 1982, focused on the broad seizure of paper documents and concluded that, "In the comparatively rare instances 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."[17] The government argued that its actions were consistent with *Tamura* because the intermingled information in the Tracey directory was in plain view of the case agent when it was being reviewed and thus was lawfully seized.

The court stamped the government's reliance on the plain-view doctrine as "too clever by half." Chief Judge Kozinski said the government's interpretation of *Tamura* and reliance on plain view were untenable and would result in the classic slippery slope, eventually leading to, in his view, an evisceration of the Fourth Amendment.

"Since the government agents ultimately decide how much to actually take, this will create a powerful incentive for them to seize more rather than less," he colorfully wrote. "Why stop at the list of all baseball players when you can seize the entire Tracey directory? Why just that directory and not the entire hard drive? Why just this computer and not the one in the next room and the next room after that? Can't find the computer? Seize the Zip disks under the bed in the room where the computer once might have been."

The court concluded that the government should, in future warrant applications based on a review of electronic evidence, forswear reliance on the plain-view doctrine. The court added that, if the government refused to waive the plain-view doctrine, a reviewing magistrate should either deny the warrant or have an independent third party under supervision of the court perform the segregation of data. Thus, at least in the 9th Circuit, the plain-view doctrine has been substantially curtailed in the context of the seizure of digital evidence.

The 9th Circuit's Prescriptive Protocol

The appeals court justified its broad prescriptions on the analytic foundation that *Tamura* was outdated in the digital age. Specifically, the court noted that "electronic storage facilities intermingle data, making them difficult to retrieve without a thorough understanding of the filing and classification systems used — something that can often only be determined by closely analyzing the data in a controlled environment."

The majority decision conceded that, because of the duplicities of the criminal mind, law enforcement does have "a legitimate need to scoop up large quantities of data and sift through it carefully for concealed or disguised pieces of evidence." However, the court went on to express concern that such broad authorization in an electronic context might turn a "limited search for particular information into a general search of office file systems and computer databases," violating the Fourth Amendment.

Given the conundrum, the court said: "We accept the reality that such over-seizing is an inherent part of the electronic search process and proceed on the assumption that, when it comes to the seizure of electronic records, this will be far more common than in the days of paper records. This calls 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." Specifically, the opinion emphasizes that the process by which "over-seized" digital evidence is winnowed down to that which was sought by the warrant should not give the government access to materials for which it did not have probable cause to obtain.

The court's concerns result in the following prescriptive procedural guidance:

- "Magistrates 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; and
- "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."

Notably, in her partial dissent, Judge Maria Callahan underscored that the proposed guidelines "are overbroad and restrict how law enforcement personnel can carry out their work without citing to legal authority that would support these new rules." Further, she complained that "the majority essentially jettisons the plain-view doctrine in digital cases" but "without explaining why our case law or the Supreme Court's case law dictate or suggest that the plain-view doctrine should be entirely abandoned."

Further Observations

Given the 9th Circuit's sweeping tone, the opinion's policy ramifications and the lack of case law cited to justify the new methodology, the government may seek Supreme Court review, despite the appeals court's condemnations of the government's prior conduct. Indeed, the government has sought a stay while it decides whether to appeal the court's decision.

The court concluded that the government should, in future warrant applications based on a review of electronic evidence, forswear reliance on the plain-view doctrine.

Much of the existing case law related to search and seizure is grounded in outdated concepts that compare computers to closed containers, filing cabinets or drawers, which hold far less information than a digital device. Thus, judicial review by the Supreme Court may be timely, even though there is no circuit conflict as of yet. In the meantime, the 9th Circuit's opinion is likely to be studied by other courts nationwide as it is the first of its kind to delineate guidelines broadly for searching and seizing electronically stored information. Moreover, it will provide ammunition to legal commentators who have suggested that the plain-view doctrine may not have a place in the digital world.[18]

In the civil context, e-discovery rules have been debated for years, resulting in numerous recent amendments to the Federal Rules of Civil Procedure and a large body of case law fundamentally changing the process of electronic discovery for litigators and litigants alike. Rules and procedures related to electronic evidence in the criminal context are less developed and in need of sharp focus, and perhaps that was the 9th Circuit's intent. But in writing such a sweeping decision that attempts to adapt decades-old Fourth Amendment law to new technology, the court has swung for the fences and decided it would round the bases without touching all the bags.

What are the ramifications of this decision? First, it is likely to be welcomed by third parties, defendants and their counsel. The decision certainly leaves open the possibility that, at least in the 9th Circuit, all electronically stored information that was not seized pursuant to the procedures outlined by the court must be returned under Rule 41(g) if the owner can lawfully possess it or, in the context of a criminal case, it might be suppressed.

Secondly, while the opinion does not discuss retroactive application of the new procedural guidelines, enterprising counsel will surely seek to derive the full benefit of the opinion. Third, the opinion's strictures raise questions about a reviewing court's ability to deny a search warrant that otherwise complies with the Fourth Amendment's requirements of probable cause and particularity. For now, it appears that there is uncertainty in the 9th Circuit about the enforceability of this opinion in a practical context.

It is doubtful that the court's suggestion that if the government does not consent to the demanded waiver of the plain-view exception, the magistrate judge should deny the warrant altogether is practical or even lawful. Judge Callahan's partial dissent underscores the potential issues with applying the majority's ruling in a child pornography case under the 9th Circuit's own precedent. But the problems don't end there. For example, under the ruling, what happens if the government has probable cause to believe someone has lodged a terrorist threat against a specific landmark? Under this ruling, would the government then be prohibited from immediately reviewing the entire contents of a computer hard drive to see if other terrorist schemes were being plotted?

The 9th Circuit chastised the U.S. government for what the panel perceived as an egregious overreach. In so doing, the court has boldly put forth a comprehensive vision of digital criminal procedure. While the decision is certainly an attempt to provide additional privacy protection for digital data and is a new tool in the arsenal of criminal defense counsel, allowing process-based attacks for either return of property or, in the appropriate case, suppression of evidence, it remains to be seen, over the coming months, whether the 9th Circuit's prescription is an overreach itself, caused more by anger over aggressive prosecutorial tactics than a pragmatic application of Fourth Amendment jurisprudence in the modern age.

Notes

1 *Arizona v. Hicks,* 480 U.S. 321 (1987).
2 *United States v. Comprehensive Drug Testing,* 579 F.3d 989 (9th Cir. Aug. 26, 2009).
3 All quotes and facts hereafter are drawn from the 9th Circuit's recent opinion, unless otherwise referenced.
4 *United States v. Comprehensive Drug Testing*, 513 F.3d 1085, 1091 (9th Cir. 2008).
5 *Id.*
6 *Id.*
7 *Id.* at 1092.
8 *Id.*
9 *Id.*
10 *Id.*
11 *Id.*
12 *Id.*
13 *Id.*
14 *Id.* at 1093.
15 *Id.* at 1093-94.
16 694 F.2d 591 (9th Cir. 1982).
17 *Id.* at 595-96.
18 *See, e.g.,* Orin S. Kerr, *Searches and Seizures in a Digital World,* 119 Harvard L. Rev. 531 (2005); RayMing Chang, *Why the Plain View Doctrine Should not Apply to Digital Evidence,* 12 Suffolk J. Trial & App. Adv. 31 (2007).

Michael E. Horowitz is a litigation partner in the business fraud and complex litigation group at **Cadwalader, Wickersham & Taft** in Washington. A former senior official within the U.S. Department of Justice and a former assistant U.S. attorney in the Southern District of New York, Mr. Horowitz recently stepped down as a U.S. sentencing commissioner.

Jodi Avergun is special counsel in the firm's business fraud and complex litigation group. She previously served as a senior official with both the Justice Department and Drug Enforcement Administration, and she served as an assistant U.S. attorney in the Eastern District of New York for 12 years. **April Oliver** is a senior associate at Cadwalader and is co-chair of the American Bar Association's White Collar Crime Subcommittee of the Young Lawyers' Division.