BNA, INC.

CRIMINAL LAW REPORTER

BNA Employee-Owned Since 1947

Search and Seizure

Attorneys, Academics Sort Through Landmark Case on Computer Searches

Legal experts have identified a recent decision by a federal court of appeals as one of the most important rulings on government searches of electronically stored information. In *United States v. Comprehensive Drug Testing Inc.*, 85 CrL 647 (9th Cir. 2009) (en banc), the en banc U.S. Court of Appeals for the Ninth Circuit dramatically refashioned the legal landscape surrounding computer searches by setting out a list of strict requirements for search warrants for electronic data when it is commingled with private information for which authorities have no probable cause. There remain, however, important unresolved questions regarding the legal basis for the court's imposition of these new requirements, whether they apply to the state courts, and practical questions about the implementation of the rules.

New Restrictions on Warrants. ''It's hard to overstate the significance of this decision because it's the first time an appellate court has laid out explicit guidelines in this area, and they are pretty stringent,'' Stephen M. Byers, of Crowell & Moring LLP, Washington, D.C., told BNA. Byers is a member of the firm's E-Discovery and Information Management practice group, and its White Collar Defense practice group.

''It is a broad ruling, and it's an exciting one,'' said Jeremy Frey, of Pepper Hamilton, in Philadelphia and Princeton, N.J. For too long before this case, searching agents simply mirrored entire hard drives, taking all the electronic data present there back to the lab for examination, and the Ninth Circuit was right to protect against the ''erosion of Fourth Amendment rights'' resulting from such over-seizures, Frey said.

The Ninth Circuit announced its new rules in a case that arose out of a federal grand jury investigation into the distribution of steroids to Major League Baseball players. The government obtained a warrant authorizing the seizure and search of the computer records of a private company that had been hired by MLB to administer its drug-testing program.

The investigators, however, seized far more records than those related to the 10 players as to whom the warrant affidavit demonstrated probable cause. The agents also seized the records of hundreds of other players and individuals, claiming that those records were in ''plain view'' once the agents were in the database.

The court of appeals eventually upheld a district court's orders, pursuant to Fed. R. Crim. P. 41, that compelled the government to return all the testing records it had seized besides those related to the 10 targeted players. In the course of its analysis, the Ninth Circuit identified a number of problems that arise when traditional Fourth Amendment doctrines are applied in the context of searches of computer files. For example, investigators' inability to be certain that the labels on files accurately reflect their contents, as well as other problems endemic to searches of electronic media, have led courts to recognize that a seizure and examination of intermingled files will often be necessary, even if it means examining files outside the scope of the probable cause on which the warrant is based.

Plain View and Computer Searches. When the plain-view doctrine is introduced in these circumstances, it can overshadow the restrictions on general searches intended by the Fourth Amendment's probable cause and particularity requirements. What can be seen with eyes is often far less expansive than what can be discovered with search technologies, and the amount of information in a room, a house, or a file pales in comparison with the volume of data, and the millions of documents, that even a single hard drive can contain.

In an opinion by Chief Judge Alex Kozinski, the court in *Comprehensive Drug Testing* acknowledged that ''overseizing'' is a necessary and inherent feature of searches of electronically stored information. On the other hand, the court insisted 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.''

''Th[e] 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,'' the circuit court warned. To keep this from happening, the court announced the following requirements for the issuance and execution of search warrants for commingled electronically stored information:

■ Magistrates should insist that the government waive reliance upon the plain-view doctrine in digital evidence cases.

■ Segregation and redaction must be done by either specialized personnel or an independent third party. If the segregation is to be done by government computer personnel, the government 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 nonresponsive data, keeping the issuing magistrate informed about when it has done so and what it has kept.

Impact of Decision. Albert Gidari, of Perkins Coie, Seattle, said the court's efforts to reform electronic searches were well-conceived. ''Anyone who has had to defend an ongoing search understands the havoc caused by unconstrained computer searches and the breaches of privacy and privilege that follow when the government asserts everything is waived during the seizure because it is now in plain view,'' Gidari said.

''I expect any party who is the subject of a warrant within the Ninth Circuit to take immediate steps to determine that information being seized will be protected consistent with this order,'' Gidari said, and Frey agreed. Even outside the Ninth Circuit, the case ''adds 'new sizzle' to Fourth Amendment suppression claims in cases of over-seizures based on search warrants,'' Frey said.

Search warrants for information from internet service providers are not likely to be affected, Gidari said. Such warrants are generally served by fax and fulfilled by the company's own personnel, he explained. ''If it appears overbroad for any reason, or raises First Amendment issues, the ISP might negotiate narrowing it, but I don't see the decision resulting in ISPs demanding proof that the seized files will be handled in accord with the opinion,'' Gidari said.

''My advice to defense counsel presently faced with a situation in which the government is holding seized commingled ESI is to put the prosecutor on notice that her entire case may be tainted if the guidelines in *United States v. Comprehensive Drug Testing* are not followed, and be prepared to file a Rule 41 motion for return [of the data],'' Byers said.

Scope of Ruling. The Ninth Circuit's opinion does not make clear whether its imposition of the new restrictions is based on the Fourth Amendment or, instead, on the circuit court's supervisory authority over the district courts' issuance of warrants. The source of the court's authority not only has impact in matters of civil liability and retroactivity, it also will greatly affect the applicability of the new protocols outside the Ninth Circuit.

State courts are not bound by a Fourth Amendment ruling of a lower federal court, and their own Fourth Amendment decisions are insulated from federal habeas corpus review by *Stone v. Powell,* 428 U.S. 465 (1976). Nevertheless, a federal circuit court's interpretations of the Fourth Amendment do represent persuasive authority that is harder for other courts to ignore than exercises of supervisory authority.

Professor Orin Kerr, of the George Washington University Law School, Washington, D.C., is one of the authors of the leading casebooks on criminal law, criminal procedure, and computer crime law. He has also written a series of influential articles on the Fourth Amendment computer issues, such as the plain-view problem. His careful review of the Ninth Circuit's opinion has left him without firm conviction as to what ground the court was standing on. He found this omission in the court's opinion to be ''bizarre'' and possibly an intentional ploy by the Ninth Circuit to goad the U.S. Supreme Court to provide guidance on these issues. ''It's one of the strangest opinions that I have ever read,'' Kerr said.

When pressed, Kerr said the court was ''probably'' exercising its supervisory power. ''When a court announces a laundry list of rules without saying what its authority is, it seems more likely that it's not intended to be a constitutional ruling,'' Kerr reasoned. The court said it was announcing the rules in order to protect Fourth Amendment privacy rights, but it did *not* say, ''It violates the Fourth Amendment to do X,'' Kerr stressed.

Addressing more practical concerns, he observed that the resource-intensive nature of the requirements imposed in *CDT* make it ''very difficult'' if not ''impossible'' for the government to comply with them. In addition to the delays and expense resulting from the participation of third-party forensic screeners, bureaucratic issues abound even when law enforcement officers are the ones segregating seized information, Kerr observed. He added that there also appear to be conflicts between the Ninth Circuit's decision and amendments to Rule 41 that were recently approved by the U.S. Supreme Court and that go into effect in December.

For a number of years before becoming a professor, Kerr served as a trial attorney in the Computer Crime and Intellectual Property Section of the Justice Department's Criminal Division. He reported that, even within the government, there are disagreements across agencies regarding the standards for computer forensic examinations.

Moreover, ''the scale of the computer forensics project is massive,'' Kerr continued. The Ninth Circuit's ruling requires government officials at both the state and the federal level to ''go back and rethink their computer forensic practices''; it is going to force the government to ask, ''Do we treat this as the binding rule nationally, or do we only follow it in the Ninth Circuit?'' Kerr said.

  CRL ISSN 0011-1341

U.S. Supreme Court Review. ''If the decision stays on the books, it will revolutionize computer forensics,'' Kerr said, ''but you can't really know the impact of a case until you know whether it is the law a year from now.''

Representatives from the U.S. Attorney's office declined to comment on the decision in *Comprehensive Drug Testing*, but they did obtain a stay of the Ninth Circuit's judgment while the solicitor general's office contemplates seeking review in the U.S. Supreme Court. The government has until Nov. 24 to file for petition for a writ of certiorari.

''If the government appeals in *CDT*, there is a good chance this case will get reviewed by the Supreme Court,'' Frey said.

Kerr was not so sure. He clerked for Justice Anthony M. Kennedy during the October 2003 term, and he thought the justices might prefer to wait for future Ninth Circuit opinions to clarify the authority the court was relying upon in *CDT* and some of the other murkier aspects of the ruling in that case. He also suggested that the unusual facts and ''weird'' procedural posture of the case—that is, an appeal of rulings on nonsuspects' Rule 41 motions for return of property that were brought before the information was searched—might prompt the solicitor general and/or the justices to wait for a more typical case, such as one involving an appeal of a suppression ruling in a criminal prosecution for child pornography.

BY HUGH KAPLAN & CHRISTINE MUMFORD