Bloomberg Law Reports® Privacy & Information

An Analysis of Protocols for Searches of Electronic Records Announced by the Ninth Circuit in *United States v. Comprehensive Drug Testing*

Contributed by Kenneth Breen, Douglas Koff, Keith Miller & Sean Haran, Paul, Hastings, Janofsky & Walker LLP

Introduction

Text and instant messaging, e-mail, and other forms of written electronic communication are part of everyday life. As a result, electronic data is maintained and stored without much expense and there has been a dramatic increase in the number of records and documents stored in computer files, disks and other electronic formats. As electronic advances continue, courts are struggling to balance the constitutional right to be free from unreasonable searches and seizures, with law enforcement's need in conducting searches, based on probable cause, to find and retrieve evidence of a crime where such evidence may be intermingled within thousands or millions of electronic records that would otherwise be private and inaccessible to state and local police and federal agents.[1]

In *United States v. Comprehensive Drug Testing*,[2] an *en banc* panel of the Ninth Circuit Court of Appeals announced a set of ground-breaking protocols to be followed by law enforcement when executing search warrants for electronic data. These protocols, which are described more fully below, place stringent limits on the ability of law enforcement officers to sift through electronic records. The government has complained loudly and forcefully in response to the ruling, characterizing the court's protocols as doing little more than "simply protect[ing] wrongdoers" and arguing that the protocols have caused "immediate and detrimental effects on law enforcement efforts," resulting in a virtual halt in federal search warrants for computer records in the Ninth Circuit.[3]

This article provides a primer on the Fourth Amendment principles governing search warrants, addresses the issues raised when law enforcement officers search for evidence of crimes among computer files and electronic records, and discusses the protocols set out in the *Comprehensive Drug Testing* ("*CDT*") opinion. The government is currently seeking reconsideration of the *CDT* case, and given the stakes involved and the breadth of the opinion, has taken the unprecedented step of seeking an *en banc* rehearing by the full court, comprised of all twenty-six active judges. Whether or not the government is successful in obtaining reconsideration by a panel of the entire court, the issues presented in the case arise whenever law

---

enforcement officers search computer files and will remain significant questions throughout the country, as many other federal appellate courts have not yet fully addressed them.

Search Warrants and the Fourth Amendment

The Fourth Amendment to the Constitution protects Americans from unreasonable searches and, absent certain limited exceptions, requires all searches by law enforcement officers to be conducted pursuant to a warrant based on probable cause. It provides:

> The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[4]

The requirement that a warrant particularize both the "place to be searched" and the "things to be seized," protects against a "general, exploratory rummaging in a person's belongings" by law enforcement.[5]

The "Plain View" Doctrine

During the execution of a search warrant, federal agents occasionally come across evidence of other crimes. Under the "plain view" doctrine, if the police "are lawfully in a position from which they view an object [whose] incriminating character is immediately apparent, and if the officers have a lawful right of access to the object, they may seize it without a warrant."[6] Thus, for example, if agents or the police are lawfully present in a home executing a search for narcotics, they may seize firearms or explosives that are readily apparent during the search and in plain view, as the incriminating nature of such objects is obvious, but they may not lawfully "rummag[e] through . . . files and papers for receipts pertaining to the purchase or manufacture of such items."[7]

Searches of Documents, Computers and Electronic Records

Searches for electronic records and other types of data pose unique Fourth Amendment problems because, when records are intermingled among large files or databases, the government must typically review and analyze each file to determine whether it is incriminating or otherwise relevant to an investigation. Indeed, while law enforcement officers may have probable cause to believe that documentary evidence of a particular crime, such as a fraud, is located within a particular physical location, they will often have little way of knowing the precise quantity, appearance or content of the documents or records.

More than thirty years ago, in a controversy surrounding a search of papers, the United States Supreme Court recognized that unique issues arise when law enforcement officers search for documents, as opposed to physical objects or other instruments of a crime:

> [T]here are grave dangers inherent in executing a warrant authorizing a search and seizure of a person's papers that are not necessarily present in executing a warrant to search for physical objects whose relevance is more readily ascertainable. In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized. . . .[O]fficials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy.[8]

These "inherent dangers" recognized by the Supreme Court years ago are heightened in the case of a search for electronic records.

Specifically, because computers and other forms of electronic storage can contain vast amounts of data, finding and extracting documents or files that are the subject of a warrant may involve some level of sifting through thousands or millions of other records, which law enforcement officers have no probable cause to seize. And because incriminating computer files and folders can easily be disguised — indeed, one judge has aptly noted, "few people keep documents of their criminal transactions in a folder marked 'drug records'" — it is often necessary for law enforcement officers to open each drive, folder, file and document in order to conduct a thorough search to determine whether evidence has been concealed.[9]

As a result of these realities, prosecutors typically seek, and courts often grant, permission for law enforcement officers to take entire computers, servers or other large amounts of data or records off-site and back to government offices. As at least one court has put it, "a warrant authorizing seizure of records of criminal activity permits officers to examine all of the papers in a suspect's possession to determine whether they are within the described category."[10] But as agents are given broad ranging authority to "examine all of the papers in a suspect's possession," and are permitted to bring thousands or millions of computer files or records back to their offices for review and analysis, an argument can be made that the Fourth Amendment's protection against "exploratory rummaging" becomes largely illusory.

Comprehensive Drug Testing

In the *Comprehensive Drug Testing* case, the Ninth Circuit attempted to reconcile the conflicting interests of the Fourth Amendment's protections against "exploratory rummaging" and the need for law enforcement officers to sift through intermingled data to find and retrieve evidence of crimes. The case arises from the government's investigation into the Bay Area Laboratory Co-Operative ("BALCO"), the lab suspected of providing steroids to some of Major League Baseball's most prominent ballplayers. Comprehensive Drug Testing, Inc. ("CDT"), a third party lab, held urine samples from certain ballplayers who had been drug tested by Major League Baseball. When federal agents learned of ten players who tested positive for steroids, they obtained warrants authorizing a search of CDT's facilities for records relating to the ten players.[11] During the search, agents discovered a directory (the "Tracey Directory") containing the tests results for the ten players identified in the warrant, as well as records for hundreds of other professional athletes, including records of

other ballplayers who had tested positive, all of whom had been promised that the results of their drug tests would be kept confidential.[12]

During the execution of the search warrant, agents ignored CDT's requests, through counsel, that (a) CDT be permitted to voluntarily provide all of the information in its possession pertaining to the ten players identified in the warrant and (b) the government permit "all material not pertaining to the specific items listed in the warrant to be reviewed and redacted by a Magistrate or Special Master before it was seen by the government." Instead, agents seized the entire Tracey Directory and thereafter examined it and used evidence of positive tests by other ballplayers to conduct additional investigation.[13]

On appeal, the parties' dispute focused on whether the government properly followed the procedural safeguards that it had itself promised to follow when it sought the warrant. More specifically, the warrant had required that the government utilize trained computer personnel (as opposed to federal investigators) to segregate the targeted information from data that was not the subject of the warrant.[14] Based upon findings in the district courts that the agents had not followed their own promised procedures, the Ninth Circuit affirmed and held that the government had violated the Fourth Amendment by going outside the bounds of the warrant and sifting through numerous records for which it had no probable cause or authorization to search or to seize.[15]

In so holding, the court rejected the government's argument that, because the records for the ten ballplayers listed in the warrant were intermingled with other records in the Tracey Directory, the government was lawfully entitled to seize and review the entire Tracey Directory. As the court put it:

> 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: 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. Let's take everything back to the lab, have a good look around and see what we stumble upon.[16]

In response to the Court's perception that the government's conduct in seizing the entire Tracey Directory violated prior Ninth Circuit precedent, the Court set out five guidelines for searches of digital evidence going forward.

The CDT *Guidelines and Protocols for Searches of Computers and Electronic Records*

The Ninth Circuit's guidelines for the execution of search warrants for electronic records, announced in the *CDT* case, are set out here:

Waiver of Plain View Doctrine

First, magistrate judges should insist that the government waive reliance on the "plain view" doctrine when searching computers and computer files.[17] The court found that, in the context of computer searches, the plain view doctrine creates a "powerful incentive" for the government to seize vast amounts of data and thereafter open files, folders and documents that are otherwise closed, thereby rendering the protections of the Fourth Amendment a nullity.[18]

Mandatory Segregation and Review by Specialized Computer Personnel or Independent Third Parties

Second, the segregation and redaction of information that is intermingled among other files or electronic records that are not authorized for seizure must be performed by specialized computer personnel or an independent third party (and not federal investigators). If the segregation is done by government computer personnel, the government must represent in the warrant application that the personnel will not disclose to the investigators any information that is discovered that is not the target of the warrant.[19]

Disclosure in the Warrant Application of the Actual Risks of Losing Information and Prior Attempts to Seize Information

Third, in applications submitted for search warrants, the government must disclose the "actual risks of destruction of information as well as prior efforts to seize that information."[20] The Court noted that in situations like *CDT*, where the government had previously served subpoenas for the same information and had received assurances from the custodian of the evidence that it would not be destroyed, a failure to include such information may violate the government's duty of candor in seeking warrant applications.[21]

Implementation of a Narrowly Tailored Search Protocol

Fourth, the government must utilize a search protocol "designed to uncover only the information for which it has probable cause, and only that information may be examined by case agents."[22] The Court recognized that the government has sophisticated search tools which allow for the identification of well-known illegal files (such as child pornography), but cautioned that these tools may not be used absent probable cause and specific authorization in the warrant.[23]

Destroy or Return Information Not the Target of the Warrant

Lastly, the government must "destroy, or if the recipient may lawfully possess it, return non-responsive data, keeping the issuing magistrate informed about what it has done and what it has kept."[24]

Analysis of the CDT *Protocols*

The protocols set out in *CDT* go further than any other circuit court has gone in limiting the government's ability to search electronic data. In fact, the majority of

circuits do not require the government to specify any particular search protocol in advance of executing a search warrant for computer records.[25] Thus, the decision is not without controversy.

In separate dissenting opinions, Judge Callahan and Judge Bea individually expressed concern that the majority's decision to abandon the plain view doctrine is an overbroad approach, unsupported by Supreme Court case law and Ninth Circuit precedent.[26] Both judges agreed that the better approach would be "to allow the contours of the plain view doctrine to develop incrementally through the normal course of fact-based adjudication."[27] In addition, Judge Callahan cited "practical, cost-related concerns," especially for smaller law enforcement agencies, associated with imposing a requirement that computer personnel and/or third parties be used to search and segregate electronic data.[28]

More recently, courts in the First and Seventh Circuits have refused to follow *CDT's* requirement that the government waive reliance on the plain view doctrine. In *United States v. Mann*, the Seventh Circuit criticized *CDT*, choosing to allow the plain view doctrine to develop through common law.[29] And a district court in the First Circuit recently stated that requiring the government to forswear reliance on the plain view doctrine is an "extreme remedy better reserved for the unusual, not the common case"[30] and that the "far preferable approach is to examine the circumstances of each case."[31]

Practitioner's Tips

Despite the controversy, the *CDT* case provides defense lawyers with powerful ammunition with which to attack the procedures employed by the government in seeking and executing search warrants for electronic evidence, as well as a number of reinvigorated theories upon which to seek the suppression of electronic evidence obtained in searches.

First, defense counsel should closely examine the warrant, on its face, to determine whether it is proper. The warrant should, among other things, specify the particular evidence to be seized, the particular place to be searched and the particular crimes that the evidence must relate to in order to be authorized for seizure. If any of these items are not sufficiently particularized, the lawyer should move for suppression. Indeed, a district court in New York recently suppressed e-mails obtained through a search warrant because the warrant, on its face, neglected to identify the crime that was the basis for the warrant, even though the affidavit in support of the warrant had identified the crime.[32]

Second, counsel should gather as much information as possible and determine whether the warrant application contains any misleading information and/or material omissions. For example, if the subject of the search warrant had previously offered to provide the evidence sought by the warrant and/or otherwise maintain the data, or if the government had already served grand jury subpoenas seeking the same evidence, these facts and circumstances should be reflected in the warrant application.

Third, to the extent the warrant sets forth a search procedure (*e.g.*, requires the segregation of information to be performed by computer personnel), counsel should

confirm that such procedures were followed by law enforcement officers during the execution of the warrant. As noted above, the agents in *CDT* had promised in the application for the warrant to employ certain procedures in executing the warrant, but had neglected to do so.

Fourth, counsel should closely examine the evidence sought to be introduced by the government to determine whether it falls within the scope of a proper search. For example, if the magistrate issuing the warrant required the use of search terms, counsel should confirm that the electronic evidence sought to be introduced by the government contains one or more of those terms (or is otherwise justified by a permissible exception to the warrant requirement).

Conclusion

The interplay between law enforcement efforts to search electronic records and the continued development of sophisticated electronic communications systems and large scale storage of data will continue to raise dynamic Fourth Amendment issues. Care should be taken whenever evidence has been obtained by a search warrant to ensure that the government has not overreached or otherwise acted unreasonably in seeking, obtaining or executing the warrant. The *CDT* case should be required reading in all such circumstances.

Kenneth Breen, Douglas Koff and Keith Miller are partners, and Sean Haran is of counsel, in the litigation department of Paul, Hastings, Janofsky & Walker, LLP. As members of the firm's white collar criminal defense, internal investigations and regulatory enforcement practice, Mssrs. Breen, Koff, Miller and Haran regularly defend individuals and corporations in criminal, civil and regulatory enforcement proceedings. Anthony Antonelli, a litigation associate at the firm, assisted with the preparation of this article.

---

1 *See, e.g.*, *United States v. Cioffi*, 668 F. Supp. 2d 385, 391–92 (E.D.N.Y. 2009) [2009 BL 236643] ("Courts and commentators have wrestled with how best to balance privacy interests and legitimate law enforcement concerns in the context of computer searches.").

2 579 F.3d 989 (9th Cir. 2009) [2009 BL 183010].

3 *Brief for the United States in Support of Rehearing En Banc By the Full Court*, at 1. The Ninth Circuit includes the following states: Alaska, Arizona, California, Hawaii, Idaho, Montana, Nevada, Oregon and Washington State.

4 U.S. Const. Amend. IV.

5 *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971).

6 *Minnesota v. Dickerson*, 508 U.S. 366, 375 (1993).

7 *Groh v. Ramirez*, 540 U.S. 551, 560–61 (2004).

8 *Andresen v. Maryland*, 427 U.S. 463, 482 n. 11 (1976).

9 *United States v. Riley*, 906 F.2d 841, 845 (2d Cir. 1990).

10 *Id.*

11 *Comprehensive Drug Testing*, 579 F.3d at 993.

12 *Id.* at 996–97.

13 *Id.*

14 *Id.* at 995–96.

15 *Id.* at 997.

16 *Id.* at 998 (internal citation omitted).

17 *Id.* at 1006.

18 *Id.* at 998.

[19] *Id.* at 1006.
[20] *Id.*
[21] *Id. at* 998–99.
[22] *Id.* at 1006.
[23] *Id.* at 999.
[24] *Id.* at 1006.
[25] *Cioffi*, 668 F. Supp. 2d at 392.
[26] *Comprehensive Drug Testing*, 579 F.3d at 1013 (Callahan, J., dissenting), 1017 (Bea, J., dissenting).
[27] *Id.* at 1013 (Callahan, J., dissenting); *see also id.* at 1018 (Bea, J., dissenting).
[28] *Id.* at 1014 (Callahan, J., dissenting).
[29] *See United States v. Mann*, 592 F.3d 779, 785 (7th Cir. 2010).
[30] *United States v. Farlow*, CR-09-38-B-W, slip op. at 11 n.3 (D. Me., Dec. 3, 2009).
[31] *Id.* at 11.
[32] *Cioffi*, 668 F. Supp. 2d at 395–96.