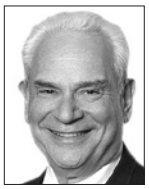
New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 245—NO. 39
TUESDAY, MARCH 1, 2011

WHITE-COLLAR CRIME

Expert Analysis

Search and Seizure of Digital Evidence: Evolving Standards



By **Elkan Abramowitz**

And **Barry A. Bohrer**

Since 2006, this column has discussed the uncertainty of standards governing the search and seizure of digital evidence.[1] Five years, and many court decisions later, the Fourth Amendment's application to computers and other accoutrements of the digital age remains murky. Uncertainty regarding the application of the Fourth Amendment to computers, e-mail, and other digitized information has a significant impact on those accused of white-collar crime because so much of the evidence in white-collar cases derives from those sources.[2] This article examines recent decisions on the Fourth Amendment's application to digital evidence, noting a number of open and controversial questions that seem ripe for adjudication by the U.S. Supreme Court. A recent decision from the Court indicates a reluctance to address such issues, however.

Plain View Doctrine

We previously have written about *United States v. Comprehensive Drug Testing Inc.* (*CDT*),[3] in which the U.S. Court of Appeals for the Ninth Circuit attempted to more clearly define the constitutional limits around electronic evidence, issuing a set of rules to be followed by judges reviewing warrant applications for electronic data. An en banc panel of the Ninth Circuit attempted to "strike a fair balance between the legitimate needs of law enforcement and the rights of individuals and enterprises to the privacy that is at the heart of the Fourth Amendment" by establishing five rules to be followed by judicial officers.

The first of the five rules set forth by the court effectively eliminated the application of the plain view doctrine in electronic discovery cases, prohibiting the government from using any "immediately apparent" evidence of illegality that is outside the scope of a search warrant.[4] A few months after the en banc panel's August 2009 opinion, the government requested a rehearing before the full Ninth Circuit, arguing that the decision and the protocol issued therein would cause "grave harm" to effective law enforcement.[5]

> The U.S. Supreme Court has signaled its reluctance to issue a definitive ruling on the application of the Fourth Amendment to digital evidence.

Although the government's request ultimately was denied, in September 2010, the Ninth Circuit amended and reissued its opinion, relegating the guidelines to a concurring opinion by Chief Judge Alex Kozinski, the author of the initial opinion. Although the per curiam majority opinion reaches the same conclusion regarding the validity of the searches and seizures in the case, the guidelines are no longer law in the Ninth Circuit, as Chief Judge Kozinski's concurrence was not joined by a majority of the en banc panel.[6]

The *CDT* guidelines, highly publicized in part because of the case's connection to steroid use in Major League Baseball, met with mixed reviews. While some courts declined to adopt the Ninth Circuit's "guidance,"[7] others applied the rules in evaluating the validity of the seizure of digital evidence.[8] The U.S. Court of Appeals for the Second Circuit has not "taken sides in the debate."[9] Most recently, in *United States v. Stabile*,[10] the U.S. Court of Appeals for the Third Circuit rejected the Ninth Circuit's "suggestion to 'forswear reliance on the plain view doctrine' whenever the government seeks a warrant to examine a computer hard drive."

Salvatore Stabile pled guilty to bank fraud and was convicted of receipt and possession of child pornography. Mr. Stabile appealed the district court's denial of his motion to suppress the evidence of child pornography found on six hard drives seized by the government, arguing that the evidence was beyond the scope of the search for financial records authorized by the consent of his housemate and a subsequent warrant. The court found that the search and seizure of the hard drives was reasonable and that the files containing child pornography properly were viewed pursuant to the plain view doctrine.

The court held that "the plain view doctrine applies to seizures of evidence during searches of computer files, but the exact confines of the doctrine will vary from case to case in a common-sense, fact-intensive manner," noting that what is permissible in one case may not be in another. In rejecting the Ninth Circuit's approach in *CDT*, the court cited *United States v. Mann* in which the Seventh Circuit expressed the view that "rather than jettisoning the plain view doctrine entirely in electronic searches, 'the more considered approach would be to allow the contours of the plain view doctrine to develop incrementally through the normal course of fact-based adjudication.'"[11]

Cell Phone Records

In a case of first impression, the Third Circuit tackled the issue of what legal standard the government must satisfy to obtain historical cell-site records—or cell site location information (CSLI)—from cell phone companies. The CSLI provides data that allows the government to determine, within several hundred feet, the location of the cell phone holder at the beginning

ELKAN ABRAMOWITZ *is a member of Morvillo, Abramowitz, Grand, Iason, Anello & Bohrer. He is a former chief of the criminal division in the U.S. Attorney's Office for the Southern District of New York.* BARRY A. BOHRER *is a member of Morvillo Abramowitz and was formerly chief appellate attorney and chief of the major crimes unit in the U.S. Attorney's Office for the Southern District of New York.* GRETCHAN R. OHLIG*, an attorney, assisted in the preparation of this article.*

and end of a call. *In Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to Government*,[12] the Third Circuit rejected a Magistrate Judge's finding that the government was required to show probable cause in order to obtain such information.

Pursuant to section 2703(c)(1) of the Stored Communications Act (SCA), the government can seek a warrant or court order for disclosure of a "record or other information pertaining to a subscriber to or customer of" a cell phone service provider. Under the statute, the government need only offer "specific and articulable facts" showing "reasonable grounds" to believe that such information is "relevant and material to an ongoing criminal investigation."[13] The Magistrate Judge found that because CSLI sought by the government was akin to a tracking device, however, the government also was required to make a showing of probable cause.[14] The Magistrate Judge's opinion was summarily affirmed by the district court.

The Third Circuit disagreed with the Magistrate Judge's conclusion that CSLI is akin to information received from a tracking device, however, and found a reasonable expectation of privacy could only be impinged upon if the CSLI would reveal information about activity or location within the confines of a person's home and that cell phones did not "extend[] to that realm." Accordingly, the court rejected the Magistrate Judge's grafting of a probable cause requirement onto the lesser standard articulated in the SCA. The Third Circuit nonetheless opined that magistrate judges are not required to issue orders for CSLI even if the lesser standard set forth in the SCA is satisfied.[15] Because the Magistrate Judge did not evaluate the facts of this case under that standard, the case was remanded.

Commentators believe the Third Circuit's opinion is "fuzzy" and "leave[s] key privacy issues unsettled."[16] Further, they project that advocacy of a case-by-case decision-making process may lead to inconsistent results in applications for this type of electronic information.

Supreme Court

It is unlikely that the Supreme Court will be the source of any clarity on the myriad issues presented in these cases, having signaled its reluctance to issue a definitive ruling on the application of the Fourth Amendment to digital evidence. In *City of Ontario v. Quon*,[17] the Court granted certiorari to determine whether an employee had a reasonable expectation of privacy in text messages transmitted on his employer-provided pager. In reviewing the case, the Supreme Court acknowledged that although the case "touche[d] on issues of farreaching significance," it could be resolved "by settled principles" of reasonableness. Accordingly, the Court declined the opportunity to more clearly define the expectation of privacy in the workplace in the digital age.

First, the Court passed on the opportunity to reconcile the plurality and concurring opinions in *O'Connor v. Ortega*, 480 U.S. 70 (1987), to offer a single approach to be taken by courts analyzing the privacy rights of public employees. Rather, the Court found that the search at issue in *Quon* would be reasonable under either approach offered in *O'Connor*, so long as *Quon* was found to have had a reasonable expectation of privacy. The parties disagreed about this latter point.

Nevertheless, the Court declined to directly address the dispute about the reasonableness of Jeff Quon's expectation of privacy in his text messages as well, hesitating to "elaborat[e] too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."

Most recently, in 'United States v. Stabile,' the U.S. Court of Appeals for the Third Circuit rejected the Ninth Circuit's "suggestion to 'forswear reliance on the plain view doctrine' whenever the government seeks a warrant to examine a computer hard drive."

The Court noted that rapid changes were occurring not only with technology itself, but also in society's expectations of proper behavior regarding the technology. "At present, it is uncertain how workplace norms, and the law's treatment of them, will evolve."[18] Accordingly, the Court refrained from a broad holding concerning employees' privacy expectations vis-à-vis employer-provided equipment, finding only for purposes of the case that Mr. Quon had a reasonable expectation of privacy in the text messages on the pager provided by his employer.

Conclusion

Technology has drastically altered the nature of government investigations and the types of evidence at issue in a criminal case. To date, however, the Supreme Court has failed to adapt Fourth Amendment jurisprudence to reflect these changes and appears unwilling to do so now, deferring for the moment to the lower courts.

1. Elkan Abramowitz and Barry A. Bohrer, "The Fourth Amendment in the Age of Computers," NYLJ (Nov. 7, 2006); Abramowitz and Bohrer, "Expansion of Border Searches to Laptops, Electronic Items," NYLJ (May 6, 2008); Abramowitz and Bohrer, "Further Developments on Privacy Rights in an Electronic Era," NYLJ (Jan. 5, 2010); Abramowitz and Bohrer, "Square Peg, Round Hole: Fourth Amendment and Digital Searches," NYLJ (March 2, 2010).

2. See, e.g., Peter Lattman and Azam Ahmed, "F.B.I. Agents Raid 3 Hedge Fund Offices," New York Times (Nov. 22, 2010) (government's seizure of computers and electronic data in insider trading cases).

3. 579 F.3d 989 (9th Cir. 2009) (en banc).

4. Recent Cases, "Fourth Amendment—Plain View Doctrine—En Banc Ninth Circuit Holds that the Government Should Waive Reliance on Plain View Doctrine in Digital Contexts—*United States v. Comprehensive Drug Testing Inc.*, 579 F.3d 989," 123 Harv. L. Rev. 1003, 1008 (2010). The remaining steps include the segregation and redaction of electronic evidence by independent parties or specialized personnel, full disclosure of actual risks of information destruction and prior attempts to seize information in warrants and subpoenas, narrowed search protocol by the government, and destruction and return of non-responsive data. *CDT*, 579 F.3d at 1006.

5. Brief for the United States in Support of Rehearing En Banc by the Full Court, *United States v. Comprehensive Drug Testing Inc.*, Nos. 05-10067, 05-15006, 05-55354 (9th Cir. Nov. 23, 2009).

6. __F.3d__, 2010 WL 3529247 (9th Cir. Sept. 13, 2010).

7. See, e.g., *United States v. Blake*, 2010 WL 702958, at *4 (E.D. Cal. Feb. 25, 2010) (distinguishing *CDT* on the basis of federal and state law); *United States v. Farlow*, 2009 WL 4728690, at *6-7 (D. Me. Dec. 3, 2009) ("far preferable approach is to examine the circumstances of each case, to assess the validity of the computer search protocol, to determine whether the police strayed from the authorized parameters of the search warrant, and to hold the police to constitutional standards in the context of a motion to suppress").

8. See, e.g., *United States v. Kim*, 677 F.Supp.2d 930, 947 (S.D. Tex. 2009) (granting defendant's motion for suppression of evidence seized from computer because the search conducted by government was not "in accordance with the narrow guidelines promulgated" in *CDT*); *United States v. Cerna*, 2009 WL 5125920 (N.D. Cal. Dec. 21, 2009) (finding that government's search protocol was sufficiently tailored to meet the criteria established in *CDT*).

9. See *United States v. Cioffi*, 668 F.Supp.2d 385, 392 (E.D.N.Y. 2009).

10. __F.3d__, 2011 WL 294036 (3d Cir. Feb. 1, 2011).

11. 2011 WL 294036, at *16 n. 16, (citing *United States v. Mann*, 592 F.3d 779, 785 (7th Cir. 2010) (citing *CDT*, 579 F.3d at 1013 (Callahan, J., concurring in part and dissenting in part))).

12. 620 F.3d 304 (3d Cir. 2010).

13. 18 U.S.C. §2703(d).

14. The Third Circuit noted that the Magistrate Judge's opinion was joined by the other magistrate judges in the Western District of Pennsylvania which demonstrated a "unique" and "impressive level of support." 620 F.3d at 308.

15. Id. at 319.

16. Orin Kerr, "Third Circuit Rules That Magistrate Judges Have Discretion to Reject Non-Warrant Court Order Applications and Require Search Warrants to Obtain Historical Cell-Site Records," The Volokh Conspiracy Blog (Sept. 8, 2010) (available at: http://volokh.com/2010/09/08/third-circuit-rules-that-magistrate-judges-have-discretion-to-reject-court-order-application-and-require-search-warrants-to-obtain-historical-cell-site-records/); "Recent Third Circuit Court of Appeals Opinion: *In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Services to Disclose Records to the Government*," The Secure Times: An online forum of the ABA Section of Antitrust Law's Privacy and Information Security Committee (Sept. 13, 2010) (available at: http://www.thesecuretimes.com/2010/09/recent_third_circuit_court_of.php).

17. 130 S. Ct. 2619 (2010).

18. Id. at 2629-30.