New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
Web address: http://www.nylj.com
VOLUME 236—NO. 89 TUESDAY, NOVEMBER 7, 2006 ALM

WHITE-COLLAR CRIME

BY ELKAN ABRAMOWITZ AND BARRY A. BOHRER

The Fourth Amendment in the Age of the Computers

After two centuries of Fourth Amendment jurisprudence, the rules applicable to government searches of offices, homes, and motor vehicles are by now reasonably clear. Much less certain, however, are the standards that govern searches and seizures of computers.

Computer searches are occurring with greater frequency in a wide range of cases. As stated by Justice John Paul Stevens, "[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[1] Although much has been written regarding these questions and how traditional rules of criminal procedure should be applied,[2] the Supreme Court has offered no guidance on the subject.

Two recent opinions from the U.S. Court of Appeals for the Ninth Circuit demonstrate the uncertain and developing nature of this area of law. Both cases address an individual's privacy right with respect to information maintained on computers and related storage media. The first case addresses this in the context of an employment situation, defining the nature of an employee's privacy interest in his office computer and raising a question as to whether there remains a distinction between private and public employees. The second case concerns the government's ability to seize and search—as opposed to search, and then seize—computerized information.

Elkan Abramowitz *Barry A. Bohrer*

These cases provide examples demonstrating that careful analysis of current Fourth Amendment law is required in technology cases to ensure its appropriate application and to avoid erosion of the protections against unreasonable search and seizure.

'United States v. Ziegler'

In *United States v. Ziegler*, the court examined the nature of an employee's Fourth Amendment rights to materials saved on the computer in his private office.[3] Mr. Ziegler was an employee of Frontline Processing (Frontline), a company that processed on-line electronic payments for Internet merchants. After discovering that Mr. Ziegler had accessed child pornography Web sites from his work computer, his employer contacted the FBI. Assisting the government in its investigation, two Frontline IT employees entered Mr. Ziegler's private office one evening and made two copies of his computer's hard drive, which were turned over to the government.[4]

Mr. Ziegler was indicted with receipt and possession of child pornography and receipt of obscene material. He filed a pretrial motion seeking suppression of evidence obtained from his computer's hard drive. The district court denied his motion, and Mr. Ziegler entered into a conditional plea agreement allowing him to appeal the district court's decision. On appeal, Mr. Ziegler contended that the search of his workplace computer violated the Fourth Amendment.

In opposition, the government argued that Mr. Ziegler did not have a reasonable expectation of privacy in his computer. To succeed on his Fourth Amendment claim, the court noted that Mr. Ziegler had to establish both that he had a subjective expectation of privacy and that he had an objectively reasonable expectation of privacy. Because Mr. Ziegler used a private password on his computer and a lock on his office door, there was no contention that he did not have subjective expectation of privacy. Rather, the court focused on whether his expectation of privacy also was objectively reasonable.

In answering this question, the court relied on a U.S. Court of Appeals for the Fourth Circuit decision, *United States v. Simons*. The *Simons* court held that "an employer's Internet-usage policy—which required that employees use the Internet only for official business and informed employees that the employer would 'conduct electronic audits to ensure compliance,' including the use of a firewall—defeated any expectation

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** *also 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.*

of privacy in 'the record or fruits of [one's] Internet use.'"[5] The government argued that the *Ziegler* situation was factually similar to that of *Simons* because Frontline had: (i) complete administrative access to its employees' computers; (ii) installed a firewall to regularly monitor Internet traffic; and (iii) informed its employees through training and employment manuals that the computers were not to be used for personal activities. Mr. Ziegler did not contradict any of these assertions.

Routine Monitoring

Setting forth a number of cases in which courts have examined the issue of searches of workplace computers, the Ninth Circuit stated that case law consistently established that "an employer's policy of routine monitoring is among the factors that may preclude an objectively reasonable expectation of privacy." Further finding that society had effectively diminished an employee's reasonable expectation of privacy with regard to the employee's use of his employer's computers, the court held that Mr. Ziegler had no objectively reasonable expectation of privacy in his workplace computer. Since he had no reasonable expectation of privacy, the Fourth Amendment was not implicated; accordingly, the district court's decision was affirmed.[6]

Last month, Mr. Ziegler petitioned the Ninth Circuit for an en banc rehearing on the matter, arguing that the circuit court's earlier decision conflicted with the Supreme Court's decision in *Mancusi v. DeForte*.[7] Specifically, the defendant contends that the court failed to recognize a well-established distinction between the types of Fourth Amendment protection accorded public employees versus those who work in the private sector, as he did.

The distinction can be articulated as follows: private employees have Fourth Amendment protection in the contents of their offices, regardless of their employer's office procedures, whereas public employees' protections hinge on the degree to which the employee's workspace is publicly available. One commentator notes that this distinction suggests that the government cannot enter an employee's workspace in a private office without the employer's consent, while the same rules do not apply in the public sector because the government is the employer.[8]

In its initial decision, the Ninth Circuit panel specifically relied on *Simons* and another Supreme Court case, *O'Connor v. Ortega*, both of which involved searches of the workspace of government employees. In *Ortega*, the Supreme Court found that a public employee's expectation of privacy in his workspace could be reduced "by virtue of actual office practices and procedures, or by legitimate regulation…," such as those workplace monitoring policies in effect in both the *Simons* and *Ziegler* cases.[9] This position differed from that articulated by the Supreme Court in *Mancusi*, which held that a private employee had a reasonable expectation of privacy in his office space and the contents therein, despite the fact that he shared the office with other employees.[10] Indeed, Justice Antonin Scalia's concurring opinion in *Ortega* specifically notes the private/public distinction by recognizing that a private sector employee's workspace is "constitutionally protected" despite his employer's internal regulations.[11]

The government disputes the notion that there is a public/private distinction, stating that "[t]he key factors—the policies and practices of the employer, and the reasonable expectations of the employees—are the same for both private and government employees."

In its response to Mr. Ziegler's petition for rehearing, the government disputes the notion that there is a public/private distinction, stating that "[t]he key factors—the policies and practices of the employer, and the reasonable expectations of the employees—are the same for both private and government employees." Further, the government contends that the panel correctly applied the "reasonable expectation of privacy" test in determining whether the Fourth Amendment was implicated by Frontline's copying of Mr. Ziegler's hard drive. Arguing that no legitimate expectation existed, the government asserts that no "search" occurred under the Fourth Amendment.[12]

Perhaps the government has failed to recognize that the Supreme Court has issued different localized rules for Fourth Amendment rights in the public versus private employment context, however.[13] Resolution of the issue within the context of the *Ziegler* case depends on whether the Ninth Circuit agrees to reconsider the case. It is almost certain, though, that the issue will arise again. Fourth Amendment scholars have sided with Mr. Ziegler in this dispute, arguing that the correct way to analyze the case is to determine that Mr. Ziegler had a reasonable expectation of privacy in the contents of his private-sector office and turn to the issue of whether the search violated the Fourth Amendment. The "unfortunate result" of the decision as it currently stands is the "incorrect conclusion that private-sector employees do not have a reasonable expectation of privacy in the workplace computers in their office when the employer has access rights to the machine."[14]

'United States v. Hill'

In *United States v. Hill*, the court examined the question of the extent to which the government is permitted to seize and search personal computers and computer storage media. The court determined that where the government needs to remove the equipment offsite to complete the search, the affidavit supporting the warrant for such equipment must detail the reasons for such removal.[15]

In *Hill*, the defendant was indicted for possession of child pornography after a computer technician repairing the defendant's computer discovered pornographic photographs on his hard drive and reported him to the police. There were two warrants involved in the seizure of Mr. Hill's computer data. First, the local police obtained a warrant to search the computer repair store and seize the defendant's computer and all storage media belonging to him. However, when the police arrived to execute the warrant, Mr. Hill had already picked up his computer. Accordingly, they obtained a second warrant to search the defendant's home, authorizing seizure of the same items.

In executing the second warrant, the police were unable to find Mr. Hill's computer, but seized floppy disks, CD-ROMS and zip disks

from his home. The pornographic pictures in issue were obtained from the zip disks when they were reviewed by the police in their laboratory. The defendant sought to suppress this evidence in the district court arguing, among other things, that the warrant was overbroad in allowing seizure of all discovered computer storage media with no regard to whether such media contained child pornography and in placing no limitation on the police officers' search of the seized media. The district court denied the suppression motion, and Mr. Hill entered a conditional guilty plea, reserving the right to appeal the evidentiary ruling.

Considering Mr. Hill's appeal, the Ninth Circuit found that there was sufficient probable cause to support the search warrant and turned to the question of whether the warrant was overbroad. Mr. Hill asserted that the warrant was overbroad because it authorized the officers to seize and remove equipment without first determining whether they actually contained child pornography. The court noted that the defendant had raised an important question regarding the execution of warrants seeking computerized evidence—one that typically does not arise with respect to other personal effects that constitute contraband or evidence of criminal activity.

Although the court concurred with the district court's reasoning that the warrant was not fatally defective in failing to require an onsite search and isolation of child pornography before removing the equipment, it stated that the government should not be given an "automatic blank check when seeking or executing warrants in computer-related searches." Rather, the government is required to demonstrate to the magistrate factually why such a search is necessary— "there must be some threshold showing before the government may 'seize the haystack to look for the needle.'"[16] Accordingly, warrants authorizing blanket removal of computer equipment for later examination must be supported by an affidavit from the government giving a reasonable explanation as to why a wholesale seizure is necessary.

In setting forth its rationale, the court cited a Department of Justice manual on "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations":

> [I]f agents expect that they may need to seize a personal computer and search it off-site to recover the relevant evidence, the affidavit [accompanying the warrant application] should explain this expectation and its basis to the magistrate judge. The affidavit should inform the court of the practical limitations of conducting an on-site search, and should articulate the plan to remove the entire computer from the site if it becomes necessary.[17]

Effectively transforming these recommendations into a constitutional requirement, the court found that the warrant executed in the defendant's home lacked the requisite explanation and therefore was overbroad.

Despite finding that the warrant was overbroad, the court did not believe that suppression was the appropriate remedy in this case. Rather, because the zip disks had been "seized and retained lawfully because described in and therefore taken pursuant to a valid search warrant" and because the officers were properly motivated "by considerations of practicality rather than by a desire to engage in indiscriminate 'fishing,'" the court determined that suppression of the fruits of the overbroad search was not necessary.[18]

In deciding not to suppress evidence found on the zip disks, it appears that the court was applying a "flagrant disregard standard," under which "the court will only suppress evidence within the scope of a facially proper warrant if the warrant was executed in flagrant disregard of its terms."[19] But the application of this standard may create a "right without a remedy." As stated, the rule is that warrants seeking to seize, remove and then search computers and computer storage devices must be accompanied by an explanation. However, the typical Fourth Amendment remedy of suppression will not be available where a warrant lacks the required explanation unless there has been a flagrant disregard for the terms of the warrant.[20] Given that it is difficult to prove such a level of disregard, it is unlikely that insufficient affidavits will result in the suppression of evidence. Such an outcome will do little in providing an incentive to searching agents in complying with the government's own standards.

Conclusion

These cases demonstrate that the application of traditional Fourth Amendment rules to the seizure and use of digitized evidence can potentially result in less than satisfactory conclusions of law. Practitioners should be aware of the nuances of what was previously viewed as hornbook law and press for legal considerations that recognize the unique circumstances created by new and evolving technologies.

1. *Kyllo v. United States*, 533 US 27, 33-34 (2001) (Stevens, J., dissenting).

2. See, e.g., Orin S. Kerr, "Searches and Seizures in a Digital World," Harvard Law Review, Vol. 119 (2005) at fn. 1 (listing various law review articles); Orin S. Kerr, "Digital Evidence and the New Criminal Procedure," Columbia Law Review, Vol. 105 (January 2005).

3. 456 F3d 1138 (9th Cir. 2006).

4. There is some factual dispute as to whether Frontline took these actions at the FBI agent's request or on their own accord. The resolution of this issue had no bearing on the 9th Circuit's holding. Id. at 1140-41.

5. Id. at 1143-44 (citing *Simons*, 206 F3d 392, 395, 398 (4th Cir. 2000)).

6. Id. at 1145.

7. Defendant-Appellant's Petition for Rehearing and Suggestion for Rehearing En Banc, No. 05-30177 (Sept. 1, 2006).

8. Orin Kerr, "Ninth Circuit Mostly Eliminates Private-Sector Workplace Privacy Rights in Computers," The Volokh Conspiracy Blog (Aug. 9, 2006) (available at http://volokh.com/posts/chain_1157474085.shtml).

9. 480 US 709 (1987).

10. 392 US 364 (1968).

11. Id. at 730 (Scalia, concurring).

12. Appellee's Response to Petition for Rehearing and Rehearing En Banc, No. 05-30177 (Oct. 5, 2006).

13. Orin Kerr, "Government Responds in 'United States v. Ziegler,'" The Volokh Conspiracy Blog (Oct. 9, 2006).

14. Orin Kerr, "Ninth Circuit Mostly Eliminates Private-Sector Workplace Privacy Rights in Computers," The Volokh Conspiracy Blog (Aug. 9, 2006) (available at http://volokh.com/posts/chain_1157474085.shtml).

15. 459 F3d 966 (9th Cir. 2006).

16. Id. at 975.

17. United States Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations 43, 69 (July 2002) (available at http://www.cybercrime.gov/s&smanual2002.htm).

18. 459 F3d at 977 (citing *United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982)).

19. Orin Kerr, "'United States v. Hill,'" OrinKerr.Com Blog (Aug. 11, 2006) (available at http://www.orinkerr.com/2006/08/11/united-states-v-hill/).

20. Id.