New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM

An ALM Publication
VOLUME 243—NO. 2
TUESDAY, JANUARY 5, 2010

WHITE-COLLAR CRIME

Expert Analysis

Further Developments On Privacy Rights in an Electronic Era

By **Elkan Abramowitz**

And **Barry A. Bohrer**

E-mail and other electronic evidence have become the hallmarks of modern day white-collar investigations. When a criminal investigation extends into the workplace, the interplay between electronic evidence and an employee's reasonable expectation of privacy with respect to that data takes center stage. In addition, corporate employers must contend with expansive requests from the government for electronically stored data. Two recent cases, one of which has been granted certiorari by the U.S. Supreme Court, signify a continuing effort by courts to more clearly define the parameters and constitutional limits around electronic evidence.

In the Workplace

The invocation of the Fourth Amendment in any context depends upon the legitimacy of an individual's expectation of privacy. Courts consistently have recognized a distinction in the Fourth Amendment rights of public versus private employees. As we have noted in previous articles, however, clearly articulated rules of law sometimes become muddled when the Fourth Amendment is applied to digital data.[1]

Courts are still feeling their way in applying traditional constitutional rights in scenarios involving computers, cell phones, BlackBerrys, and the like. The Supreme Court has granted certiorari in *City of Ontario v. Quon*,[2] a case involving text messages, to consider the nuances of these rights and their application in the workplace.

Jeff Quon was a member of the Ontario City SWAT Team in the state of California. As a city employee, Mr. Quon received a pager with texting capabilities. Although the City of Ontario had no official policy regarding use of the pagers, Mr. Quon and other employees were told that the city's Computer Usage, Internet and E-mail policy would apply. That policy provided that the use of all city-owned equipment was limited to City of Ontario-related business and that use for personal benefit was a violation of said policy. Further, Mr. Quon signed an Employee Acknowledgment upon receipt of the pager which stated that users should have no expectation of privacy or confidentiality when using the pagers.

> Clearly articulated rules of law sometimes become muddled when the Fourth Amendment is applied to digital data.

Despite these facts, Mr. Quon used the pager to send personal texts. Under the city's contract with the pagers' service provider, Arch Wireless Operating Company, each pager was allotted 25,000 characters per month, after which the city was required to pay overage charges. The use and cost of the pagers was monitored by a Commander with the police department, Lieutenant Steve Duke, who was responsible for procuring payment for overages. According to Lieutenant Duke's testimony at trial, his practice was to seek reimbursement for overage charges from the individual employee who used the pager. If the employee cooperated in paying the extra money, there was no audit of the pager's use to determine how many minutes were, in fact, work-related.

At some point, Lieutenant Duke was instructed to obtain the transcripts for Mr. Quon and another officer's pagers because they had continually exceeded their allotted minutes. An audit of Mr. Quon's pager transcripts revealed that he had exceeded his monthly character allotment by more than 15,000 characters and that many of the messages were personal in nature and often sexually explicit. The matter was referred to the city's Internal Affairs Department.

Mr. Quon, and those to whom he sent personal text messages—his wife, his girlfriend and a fellow member of the City's SWAT team—sued Arch Wireless and the city. They claimed that Arch Wireless had violated the Stored Communications Act[3] and that the city had violated their Fourth Amendment rights. The district court found that the plaintiffs had a reasonable expectation of privacy in their text messages as a matter of law as a result of Lieutenant Duke's informal policy not to audit a pager when overage charges were willingly paid by the employee.

The court then turned to the reasonableness of the search, which it opined was dependent on the intent with which the audit was conducted. The jury found that the audit was intended to establish the efficacy of the character count rather than uncover misconduct. Accordingly, the search was determined reasonable and the city was absolved of liability for the search.[4]

ELKAN ABRAMOWITZ *is a member of Morvillo, Abramowitz, Grand, Iason, Anello & Bohrer and 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.* GRETCHAN R. OHLIG, *an associate at the firm, assisted in the preparation of this article.*

The plaintiffs appealed to the U.S. Court of Appeals for the Ninth Circuit.

In *O'Connor v. Ortega*,[5] the Supreme Court reasoned that "[i]ndividuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer." However, the "operational realities" of the public workplace reduces a public employee's expectation of privacy. "Given the great variety of work environments in the public sector, the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis."[6]

Noting that the standard to be applied to e-mails and text messages was a "new frontier in Fourth Amendment jurisprudence that has been little explored," the Ninth Circuit in *Quon* articulated the threshold question as whether users of text messaging services had a reasonable expectation of privacy in their text messages that were stored in a service provider's network. Likening text messages to phone conversations or the contents of a sealed letter, the court found that they do. Further, the court distinguished the substance of text messages from pen registers that record phone numbers dialed from a phone and e-mail address books, to which no expectation of privacy is assigned.

Addressing the claims of Mr. Quon's wife, girlfriend and co-worker, the court noted that they had no reasonable expectation that Mr. Quon would maintain the private nature of their text messages, or vice versa. However, because the city "surreptitiously reviewed messages that all parties reasonably believed were free from third-party review," these plaintiffs had a reasonable expectation that their messages would not be reviewed by the city without consent from either themselves or Mr. Quon. The searches, therefore, violated these individuals' Fourth Amendment rights.[7]

The court then turned to Mr. Quon's reasonable expectation of privacy with respect to the same messages. Despite its formal written policy regarding Internet and e-mail usage, the court found that the police department followed Lieutenant Duke's informal policy that no audit would occur if overages were paid with respect to text messages, and therefore held that Mr. Quon also had a reasonable expectation of privacy in the text messages archived by Arch Wireless.

Thus, the question with respect to each plaintiff's claim was whether the search conducted by the city was reasonable. Accepting the jury's determination that the search was conducted for the purpose of determining the efficacy of the character limit on text messaging, the Ninth Circuit found that the scope of the search was unreasonable because there were simpler, less intrusive ways to assess the validity of the monthly character limit. Accordingly, the search of Mr. Quon's text messages violated the Fourth Amendment's prohibition against unreasonable searches and seizures.[8]

The Supreme Court granted certiorari to determine: "(1) whether a SWAT member has a reasonable expectation of privacy in text messages transmitted on his SWAT pager, where the police department has an official no-privacy personal use of the pagers; and (2) whether individuals who send text messages to a SWAT team member's SWAT pager have a reasonable expectation that their messages will be free from review by the recipient's government employer."[9]

The guidelines advocated by the Ninth Circuit in 'Comprehensive Drug Testing' serve as a strong basis for attorneys representing clients in government investigations to object to wide-ranging, unlimited government requests for electronic data without the proper procedural safeguards.

Observers question the Court's motives in granting certiorari in *Quon*. The Ninth Circuit was the first federal appeals court to address the issue of Fourth Amendment protection of text messages. Further, issues revolving around a public employee's privacy rights are highly fact-specific. Accordingly, some are wondering why the court is interested in the case.[10] Perhaps the vigorous dissent of seven judges in the Ninth Circuit's decision to deny rehearing en banc prompted the Court's involvement. Regardless, the outcome is likely to be significant in terms of further defining privacy rights in the workplace and the Fourth Amendment's application to text messages, which also could be applied to e-mails—another open issue in this electronic age.[11]

Seizure and Handling

In an effort to avoid a "serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant," the Ninth Circuit issued an en banc opinion in *United States v. Comprehensive Drug Testing Inc.*,[12] setting forth "clear rules" to be followed by the government in order to protect the confidentiality of data sought by warrant. These rules are intended to "strike a fair balance between the legitimate needs of law enforcement and the right of individuals and enterprises to the privacy that is at the heart of the Fourth Amendment."[13]

In 2002, the government initiated an investigation into the Bay Area Lab Cooperative (Balco), which it suspected of providing steroids to professional baseball players. During the same time, the Major League Baseball Players Association entered into a collective bargaining agreement with Major League Baseball agreeing to drug testing of all players. Comprehensive Drug Testing Inc. (CDT) administered the drug testing program as an independent third party and maintained all data related to the players and the results of their tests in electronic form.

During the Balco investigation, federal authorities learned that 10 players had tested positive for steroids in the CDT program. In response, the government obtained a grand jury subpoena in the Northern District of California seeking "all 'drug testing records and specimens' pertaining to Major League Baseball in CDT's possession." After unsuccessfully trying to negotiate a compliance agreement with the government, CDT and the Players Association moved to quash the subpoena.

The same day, the government obtained a warrant in the Central District of California to search CDT's facilities for the records of the 10 players identified as failing the tests. However, when the warrant was executed, the government instead seized and reviewed the drug testing records for hundreds of Major League Baseball players. Another warrant was obtained in the District of Nevada for the urine samples on which the drug tests had been performed. Further warrants for records at CDT facilities were obtained, in some instances seeking records already seized.

CDT sought and obtained an order pursuant to Federal Rule of Criminal Procedure 41(g) for the return of the property seized in the Central District of California. In addition, the government was ordered to return all property seized in the District of Nevada with the exception of those materials pertaining to the 10 identified players. Finally, CDT moved to quash all subpoenas issued in the Northern District of California. This motion

also was granted. According to the Ninth Circuit, "[a]ll three judges below expressed grave dissatisfaction with the government's handling of the investigation, some going so far as to accuse the government of manipulation and misrepresentation."[14] The government appealed all three orders, and all were upheld by the Ninth Circuit.

The government's affidavit in support of its first search warrant detailed the difficulty in retrieving electronic information and the "generic hazards" associated with searching such electronic data, including the ways in which data can be disguised or may be destroyed or hidden. The Ninth Circuit observed that this information "made a strong case for off-site examination and segregation of the evidence seized" and provided authority for the government to "seize considerably more data than that for which it had probable cause."

Indeed, the Magistrate Judge's Order authorized a broad seizure of CDT records by the government, but subject to certain procedural safeguards based on the Ninth Circuit's 1982 decision in *United States v. Tamura*.[15] In *Tamura*, the government was authorized to seize evidence of certain payments received by a criminal defendant from his employer's records. The process of identifying such payments was voluminous and impossible to complete on-site. Accordingly, the government seized several boxes and dozens of file drawers to be sorted out in their offices at leisure.

Although disapproving of the wholesale seizure and the government's failure to return those materials identified as non-relevant, the Ninth Circuit "saw no reason to suppress the properly seized materials just because the government had taken more than authorized by the warrant." Accordingly, the *Tamura* court suggested that certain guidelines be followed by the government in such situations, including the sealing and holding of documents pending approval of a further search by a magistrate and a request for specific authorization for the large-scale removal of material where such a need is known ahead of time.[16]

Because the guidelines set forth in *Tamura* pre-date the "dawn of the information age," the en banc Ninth Circuit took the opportunity in *Comprehensive Drug Testing* to expand and update their application to present day realities. The court stated that "[w]hen the government wishes to obtain a warrant to examine a computer hard drive or electronic storage medium in searching for certain incriminating files, or when a search for evidence could result in the seizure of a computer, magistrate judges must be vigilant in observing the guidance we have set out throughout our opinion." In sum, five steps were outlined by the court.[17]

First, magistrate judges should insist that the government waive reliance upon the plain view doctrine in digital evidence cases. Because the government ultimately decides how much evidence to seize, the ability to argue the application of the plain view doctrine to evidence not originally covered in the warrant would "make a mockery of *Tamura* and render the carefully crafted safeguards…a nullity."[18] Second, segregation and redaction of evidence must be done by specialized personnel or an independent party so that the investigating agents do not have access to information other than that which is the target of the warrant.

Third, warrants and subpoenas must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other districts. For instance, although the government's warrant application to seize evidence from CDT included many cautionary notes on the "theoretical risk" that digital evidence is easily destroyed or hidden, it failed to note that CDT had agreed to preserve the data in its original state until the resolution of its motion to quash. According to the court, "[a] lack of candor in this or any other aspect of the warrant application should bear heavily against the government in the calculus of any subsequent motion to return or suppress the seized evidence."[19]

Fourth, the government's search protocol must be designed to uncover only information for which it has probable cause. And finally, the government must destroy or, if the recipient may lawfully possess it, return non-responsive data, keeping the issuing magistrate aware about when it has done so and what it has kept.

These guidelines safeguard parties from overly broad searches and seizures of electronic data while simultaneously acknowledging the government's legitimate law enforcement interests. Referencing the Ninth Circuit's opinion in *Comprehensive Drug Testing*, a recent opinion from the Eastern District of New York considering the level of specificity required in a warrant application notes that, "[t]o date, the Second Circuit has not taken sides in the debate on the particularity required for computer searches,"[20] although it has condemned warrants authorizing a search for evidence of "any crime." Regardless, the guidelines advocated by the Ninth Circuit serve as a strong basis for attorneys representing clients in government investigations to object to wide-ranging, unlimited government requests for electronic data without the proper procedural safeguards.

1. Elkan Abramowitz and Barry A. Bohrer, "Expansion of Border Searches to Laptops, Electronic Items," NYLJ (May 6, 2008); Elkan Abramowitz and Barry A. Bohrer, "The Fourth Amendment in the Age of the Computers," NYLJ (Nov. 7, 2006).
2. 529 F.3d 892 (9th Cir. 2008); rehearing denied, 554 F.3d 769 (9th Cir. 2009) (en banc).
3. The issue of whether Arch Wireless violated the Stored Communications Act hinges on whether they are considered a "remote computing service" or "electronic communication service" under the statute. That issue is not addressed in this article.
4. 445 F. Supp.2d 1116 (C.D.Cal. 2006).
5. 480 U.S. 709 (1987).
6. Id. at 718.
7. 529 F.3d at 906.
8. Id. at 909-10.
9. __S.Ct.__, 2009 WL 1146443 (Dec. 14, 2009).
10. Orin Kerr, "Supreme Court Grants Cert on Fourth Amendment Protection in Text Messages," The Volokh Conspiracy Blog (Dec. 14, 2009).
11. The Ohio Supreme Court recently held that the Fourth Amendment's exception for searches incident to arrest does not allow police officers to look through an arrestee's cell phone call log. *State v. Smith*, __N.E.2d__, 2009 WL 4826991 (Ohio Dec. 15, 2009). In so holding, the court distinguished the Fifth Circuit's opinion in *United States v. Finley*, in which the Fifth Circuit upheld the district court's denial of defendant's motion to suppress call records and text messages obtained from his cell phone after his arrest. In that case, the defendant conceded that the cell phone was akin to a "closed container" found on an arrestee's person which lawfully may be searched. 477 F.3d 250, 259-60 (5th Cir. 2007).
12. 579 F.3d 989 (9th Cir. 2009) (en banc).
13. Id. at 1006.
14. Id.
15. 694 F.2d 591 (9th Cir. 1982).
16. Id. at 595-96.
17. 579 F.3d at 1006
18. Id. at 998
19. Id. at 998-99
20. *United States v. Cioffi*, __F. Supp.2d__, 2009 WL 3738314, *5 (EDNY Nov. 2, 2009)