New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 252—NO. 24
TUESDAY, AUGUST 5, 2014

WHITE-COLLAR CRIME

Expert Analysis

When the Government Searches Your Hard Drives

By **Robert J. Anello**

And **Richard F. Albert**

The Supreme Court's recent unanimous decision in *Riley v. California* barring warrantless searches of cellphones incident to arrest has rightly received a good deal of attention as an important example of the court's adapting Fourth Amendment principles to the realities of modern technology.[1] Chief Justice John Roberts' opinion for the court astutely recognizes how technological innovations have shifted the analytical paradigm, memorably expressed in the comment that government arguments analogizing cellphones to wallets and similar items carried on the person were "like saying a ride on horseback is materially indistinguishable from a flight to the moon."[2]

Just a week before the Supreme Court's decision, the U.S. Court of Appeals for the Second Circuit issued an opinion that, while less far-reaching than *Riley*, illustrates similar struggles of the legal system to apply Fourth Amendment concepts to electronic data different in kind and exponentially larger in volume than evidence typically seized by law enforcement officers in years past. In *United States v. Ganias*, the Second Circuit reversed a tax evasion conviction, finding that the government violated the defendant's Fourth Amendment rights by its unauthorized two-and-one-half year retention of the defendant's personal files located on an imaged hard drive seized in an earlier investigation.[3]

The Second Circuit's analysis in *Ganias*, like the Supreme Court's in *Riley*, provide reason for hope that, in the digital age, the courts may breathe a bit more life back into the Fourth Amendment after years of cutting back on its protections. For white collar criminal practitioners, *Ganias*, along with a 2012 Eastern District of New York decision suppressing seized electronic data because of the government's long delay in reviewing it and decisions addressing the problem of privilege review of seized electronic documents, illustrate potentially fertile areas for defendants to seek judicial examination of the government's actions in handling seized computer records.

Computer Searches

The Fourth Amendment provides that "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 also provides that "no Warrants shall issue, but upon probable cause…particularly describing the place to be searched, and the persons or things to be seized." As the Supreme Court explained in Riley, the Fourth Amendment "was the founding generation's response" to general warrants that permitted unrestrained rummaging through homes, and "[o]pposition to such warrants was in fact one of the driving forces behind the Revolution itself."[4] Because today computers will often be where individuals maintain the varied "privacies of life," they require protection similar to residences against improper government intrusion.[5] "If anything, even greater protection is warranted."[6]

Recognizing the practicalities of document searches, courts have long permitted officers to examine innocuous documents "at least cursorily" in the course of determining whether they fall within a described category authorized for seizure under a warrant.[7]

Because computer hard drives tend to store massive amounts of varied and commingled data that cannot possibly be sorted on site, court decisions generally have permitted officers executing search warrants to create mirror images of hard drives on-site to allow subsequent off-site review without burdening the use of the individual's premises or computer. Indeed, Fed. R. Crim. P. 41(e)(2)(B), adopted in 2009, expressly contemplates the off-site review of seized electronic files.[8] The Fourth Amendment's ultimate requirement of "rea-

ROBERT J. ANELLO *and* RICHARD F. ALBERT *are partners at Morvillo Abramowitz Grand Iason & Anello.* GRETCHAN R. OHLIG, *an attorney, assisted in the preparation of this article.*

sonableness," however, applies to all aspects of the execution of a warrant, including the off-site review of imaged computer files.[9] As the Supreme Court recognized in *Riley*, adherence to the Fourth Amendment imposes burdens on law enforcement; "[p]rivacy comes at a cost."[10]

'United States v. Ganias'

Whether the government's off-site review of computer hard drives met Fourth Amendment reasonableness requirements was at issue in *Ganias*. The defendant, Stavros Ganias, owned an accounting firm, and among his clients were James McCarthy and two businesses owned by McCarthy: Industrial Property Management (IPM) and American Boiler. IPM and American Boiler came under investigation for fraud and theft of government property in connection with a government contract.

While executing a warrant to search Ganias' offices for records relating to IPM and American Boiler in November 2003, government agents made forensic mirror images of the hard drives of Ganias' three computers. Eight months later, agents began to review the files to segregate documents related to IPM and American Boiler from non-responsive files, which included Ganias' personal financial records. The government's review was complete by December 2004, but it did not return the non-responsive files to Ganias.

The Internal Revenue Service later expanded the scope of the investigation to include potential tax violations, and in April 2006 the government obtained a warrant to search the personal financial records of Ganias, which were located on the preserved images previously segregated and held by the agents. In October 2008, a grand jury indicted Ganias and McCarthy. The trial court denied Ganias' pre-trial motion to suppress the computer files, and Ganias was convicted of tax evasion.

On appeal, the U.S. Court of Appeals for the Second Circuit, focusing on the Fourth Amendment's reasonableness requirement, held that officials executing a warrant for the seizure of particular data on a computer are not permitted to seize and indefinitely retain every file on that computer for future use. The government had segregated out non-responsive files by December 2004, but then held them for another 16 months before it developed probable cause to search and seize them. The court concluded that the government's retention of Ganias' personal financial records deprived him of their exclusive control for an unreasonable period of time and effectively converted the original warrant into a general warrant, thus violating the Fourth Amendment.

> In the digital age, the courts may breathe a bit more life back into the Fourth Amendment after years of cutting back on its protections.

The court then turned to the question whether suppression was the appropriate remedy. Suppression is required when a widespread seizure of items not covered by a warrant has occurred; the agents have acted in bad faith; and the benefits of deterrence outweigh the cost of suppression.[11] Finding that the government effected a broad seizure beyond the scope of the warrant, the court held that the government did not meet its burden to prove that the officers acted in good faith in concluding that the original 2003 warrant allowed them to claim Ganias' personal records as "government property" and retain them for more than two years. The court found the costs of suppression to be "minimal" because a dangerous defendant would not be set free, and the benefits to be "great" because "[w]ith the government's use of forensic mirror images becoming increasingly common, deterring its unconstitutional handling of non-responsive data has grown in importance."[12]

Other Issues

Two other Fourth Amendment-related issues that pose particular practical challenges when the government seizes computer media—namely, the length of time it takes for the government to review seized materials and the protection of privileged information—merit attention from white-collar practitioners. While these issues arise when the government seizes and reviews hard copy documents, the logistical difficulties posed and the privacy interests implicated tend to expand exponentially when the government seizes electronic media.

Delay in Review—'United States v. Metter.' Whereas *Ganias* considered the implications of the government's retention of seized computer files outside the scope of a warrant after the government had reviewed and expressly segregated such files, in a 2012 decision, Eastern District of New York Judge Dora L. Irizarry addressed the related issue of how long the government can wait before undertaking such review. In the securities fraud prosecution *United States v. Metter*,[13] pursuant to a series of search warrants, the government seized four hard drives from Metter's home, 61 hard drives from the business premises of his company, Spongetech Delivery Systems, Inc., and email and text message data from Internet service providers. The court granted Metter's motion to suppress the data from Metter's four hard drives because of the government's 15-month failure to review any of the seized data to determine which data was within the scope of the applicable warrants. The government's failure to undertake such review was exacerbated by its insistence on disseminating copies of various defendants' data to other defendants' counsel in discovery prior to reviewing and segregating it, and

by its failure to complete a review of the data for attorney-client privilege.

The court recognized that the vast storage capacities of computer hard drives required courts to use a "flexible approach" in assessing the execution of warrants, and that numerous decisions had permitted a several-month delay between seizure of electronic records and the completion of off-site review. The court ruled, however, that the government was not authorized to "seize and image electronic data and then retain that data with no plans whatsoever to *begin* review of that data to determine whether any irrelevant, personal information was improperly seized. The government's blatant disregard for its responsibilities in this case is unacceptable and unreasonable."[14] Based on such finding and its consideration of the applicable standard referenced above, the court found that the government's conduct did not meet the good-faith exception and thus suppression was required.[15]

Privilege Review and 'Taint Teams.' Another issue referenced by the court in *Metter* but not addressed in detail is how to avoid violation of the privileges against disclosure maintained by the subject of a search warrant. The extent of the problem can vary significantly depending upon the nature of the computer media seized, but when the government seizes the hard drive of a senior executive or professional advisor in a business case, unless appropriate protective procedures are applied, members of the prosecution team will likely gain improper access to files subject to the attorney-client privilege, work-product doctrine or other applicable privilege.

Courts have considered various methods to facilitate examination of the seized electronic data to segregate out privileged material before the prosecution team gets access. These methods include in camera review by the court; appointment of a special master; and utilizing a "taint team" of prosecutors and agents who are not otherwise participating in the investigation.

The use of a "taint team"—by far the preferred method of prosecutors—is highly problematic.[16] By its very nature, it does not fully protect privileges, because it allows government investigators to access privileged material. Further, experience teaches that distinguishing between what is and what is not privileged can be difficult, and it can become nearly impossible without the ability to freely discuss potentially privileged documents with the privilege holder. The government bears the burden of proving that the "wall" around the taint team was effective in preventing communication of privileged information to the investigation team.[17]

Two Fourth Amendment-related issues that pose particular practical challenges when the government seizes computer media—namely, the length of time it takes for the government to review seized materials and the protection of privileged information—merit attention from white-collar practitioners.

On several occasions, courts have questioned the ability of prosecutors to protect applicable privileges through the use of a taint team, suggesting that this method should be avoided when possible.[18] All of these concerns are amplified in the context of computer searches, given their technical complexities and the variety and sheer number of files subject to review.

Conclusion

Government searches of ever more sophisticated technology and ever vaster quantities of electronic data implicate ever increasing stakes for individual privacy. Decisions like *Riley*, *Ganias* and *Metter* demonstrate that courts are recognizing these stakes, and suggest that counsel should remain vigilant rather than routinely accept law enforcement methods of seizing and searching electronic media.

1. 134 S.Ct. 2473 (2014).
2. Id. at 2488.
3. ___ F.3d ___, 2014 WL 2722618 (2d Cir. June 17, 2014).
4. *Riley*, 134 S.Ct. at 2494.
5. Id. at 2494-95 (citing *Boyd v. United States*, 116 U.S. 616, 630 (1886)); *Ganias*, 2014 WL 2722618 at *7, (citing *United States v. Galpin*, 720 F.3d 436, 446 (2d Cir. 2013)).
6. 2014 WL 2722618 at *14 (citing *Galpin*, 720 at 446).
7. *Andresen v. Maryland*, 427 U.S. 463, 482 n. 11 (1976); see also *United States v. Riley*, 906 F.2d 841, 845 (2d Cir. 1990).
8. Rule 41(e)(2)(B) provides in relevant part that a warrant "may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information," that ordinarily a warrant allows "a later review of the media or information" and that the time for execution specified in the warrant does not limit "any off-site copying or review."
9. *Ganias*, 2014 WL at 2722618 at *8 (citing *United States v. Ramirez*, 523 U.S. 65, 71 (1998)).
10. *Riley*, 134 S.Ct. at 2493.
11. *Ganias*, 2014 WL 2722618 at *12 (citing *Herring v. United States*, 555 U.S. 135, 41 (2009); *United States v. Shi Yan Liu*, 239 F.3d 138, 141 (2d Cir. 2000)). Judge Peter Hall dissented in part from the majority opinion, writing that he did not believe suppression was the appropriate remedy in this case because the government did not act in bad faith.
12. Id. at *13.
13. 860 F.Supp.2d 205 (E.D.N.Y. 2012).
14. Id. at 215 (emphasis in original).
15. The government appealed the district court's ruling, but the case was resolved by Metter's guilty plea before any substantive appellate decision.
16. See Robert J. Anello and Robert G. Morvillo, "In Internal Investigations, All Lawyers Are Not Created Equal," NYLJ (Dec. 7, 2010).
17. *United States v. Neill*, 952 F.Supp. 834 (D.D.C. 1997).
18. See, e.g., *In re Seizure of All Funds on Deposit in Accounts in Names of Nat'l Electronics, Inc. at JP Morgan Chase Bank 8765013327-65*, 2005 WL 2174052 at *3 (S.D.N.Y. Sept. 6, 2005); *United States v. Stewart*, 2002 WL 1300059 at *6 (S.D.N.Y. June 11, 2002).