New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 252—NO. 49
WEDNESDAY, SEPTEMBER 10, 2014

Outside Counsel

Expert Analysis

Judicial Battles Over Criminal Subpoenas for Online Data



By **Ben Barnett**
And **Rebecca Kahan Waldman**
And **Nathaniel Hopkins**

The amount of electronically stored information (ESI) in the digital universe is staggering and increasing exponentially. Much of this data is personal. According to IBM, every day, people globally send 294 billion emails, publish 230 million Tweets, and upload 100 terabytes of data to Facebook. These statistics account for a small fraction of online ESI, which can include purchase invoices, travel itineraries, contact lists, private correspondence, photographs, calendar appointments, tax documents, medical information, and so on. A collection of such digital information provides an archive of an individual's personal life—more detailed, reliable, and intimate than the most meticulously maintained diary or scrapbook. This phenomenon is equally true in the business world. The average American office worker creates 1.8 million megabytes of ESI each year, and more companies are considering moving their enterprise data into cloud storage to manage this growth.

Never before has so much personal data been available anywhere but also completely outside the immediate control of the person who created it. After all, ESI saved in online accounts is stored on both an individual's hard drive and on third-party servers. For this reason, when the federal government wants access to certain personal information for investigations or other law enforcement activity, it need not ask the individual or business that created the data, but can turn to the party controlling the servers on which the data is stored. Today, companies like Google and Facebook are the entities responding to government search warrants and subpoenas for individuals' personal information.

Federal courts continue to struggle—and sharply disagree—over the scope of Fourth Amendment protections for this data. One especially contentious issue has been whether the Fourth Amendment mandates certain restrictions on government search warrants for ESI controlled by third-parties.

> Two federal magistrate judges have generated controversy by denying ESI warrants sought under Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure.

Two federal magistrate judges—Magistrate Judge John M. Facciola of the District of Columbia and Magistrate Judge David J. Waxse of the District of Kansas—have generated controversy by denying ESI warrants sought under Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure.[1] Rule 41 contemplates a "two-step" search-and-seizure process in which officers seize or copy an entire data set that they later subject to off-site analysis or review. The warrants rejected by Judges Facciola and Waxse would have directed email providers to turn over *all* ESI from certain accounts for off-site review. The warrant applications proposed no search protocols limiting the scope of the information to be seized, no time limits on the government's retention of the seized information, and no requirement for the destruction or return of information found to be irrelevant to the investigation.

Judges Facciola and Waxse held that such unrestricted ESI warrants violated the Fourth Amendment. Because the requested warrant permitted the government to seize *all* data associated with a specific account, it would almost certainly entail the seizure of emails, documents, and other information that were in no way relevant to the government's investigation. While probable cause existed to seize some of the information associated with the account, that justification did not extend to all the extraneous information implicated by the unrestricted warrant. For this reason, Facciola and Waxse concluded that these unrestricted ESI warrants amounted to nothing more than an "exploratory rummaging" through an individual's personal data, in violation of the Fourth Amendment.

To comply with the requirements of the Fourth Amendment, Facciola and Waxse held that the federal government must tailor the scope of its ESI warrant applications to meet a particularized probable cause justification. They also advocated incorporating certain "minimization procedures" or "procedural safeguards" to limit the amount of ESI to be seized and to provide for the appropriate treatment of non-responsive data. These minimization procedures might include having the data's custodian or a third-party vendor apply specified search criteria to a data set and disclose to the government only the responsive files. They could also involve "secondary orders" requiring the government to destroy irrelevant data after a specified period of time.

Revolt and Resistance

The Facciola and Waxse decisions prompted some commentators to declare a "magistrates' revolt" against unrestricted ESI warrants. That revolt—to the extent it actually existed—recently ran into some resistance. On Aug. 8, Chief Judge Richard W. Roberts of the District of Columbia reversed one of Judge Facciola's key decisions denying an ESI warrant application.[2] On July 18, Southern District Magistrate Judge

BEN BARNETT *is a partner at Dechert, based in Philadelphia, and* REBECCA KAHAN WALDMAN *is a New York-based associate.* NATHANIEL HOPKINS, *an associate in the Philadelphia office, contributed to this article.*

Gabriel W. Gorenstein granted exactly the kind of broad, unrestricted ESI warrant that Facciola and Waxse rejected.[3]

The Roberts and Gorenstein opinions take direct aim at the earlier Rule 41 rulings by Judges Facciola and Waxse. Roberts and Gorenstein both emphasized the "practical need" for law enforcement to seize large swaths of ESI for off-site analysis. Citing case law authorizing the seizure and copying of entire computer hard-drives for subsequent analysis, both judges concluded that the federal government must be permitted to seize and analyze entire sets of ESI as important evidence may be hidden within a haystack of irrelevant data. Because the government cannot effectively search all this data at the location where it is stored, Roberts and Gorenstein argue that it is necessary to seize the lot and perform the necessary search procedures off-site.

Roberts and Gorenstein also rejected proposals for minimization procedures and other safeguards intended to restrict the government's access to and use of ESI. They argued that mandatory minimization procedures needlessly increase the costs of the investigation and expose the government to potential security breaches. They also argued that it would be unnecessary and onerous to involve the ESI custodian in the data review process because of the conflicts of interest involved in "deputizing" an email provider to search through its customers' accounts.

Finally, Roberts and Gorenstein criticized the idea of court-imposed "secondary orders" controlling the government's treatment of non-responsive, irrelevant, or privileged data. They argue that these ex ante restrictions are unnecessary due to the host of ex post remedies available to address ESI that the government has improperly seized and retained, including judicial review of the manner in which a warrant was executed, suppression of evidence at trial, and a motion for the return of property under Fed. R. Civ. P. 41(g).

Developing Arguments

The debate regarding ESI warrants under Rule 41 will no doubt continue. In the meantime, practitioners should account for this sharp divide within the federal judiciary and consider applying the following arguments when a client is faced with an overly broad ESI warrant.

First, there is clear potential for government abuse of data seized through an unrestricted ESI warrant or subpoena. In *United States v. Ganias*, No. 12-240-cr, 2014 WL 2722618 (2d Cir. June 17, 2014), the government used extraneous ESI seized during a fraud investigation of a military contractor to subsequently convict the contractor's accountant of tax evasion on his personal returns.

The U.S. Court of Appeals for the Second Circuit vacated the conviction, holding that, since the evidence used in the tax evasion case was beyond the scope of the original warrant from the fraud investigation, the government was not permitted to retain the data for use in this unrelated prosecution. Although *Ganias* might be read to show the efficacy of ex post judicial remedies regarding ESI, it also perfectly illustrates the reason why court-imposed minimization procedures and secondary orders should demarcate the government's access to and use of ESI.

Second, the U.S. Supreme Court has demonstrated increasing sensitivity to the privacy of personal data and has recently extended Fourth Amendment protection to such data on mobile devices. In *Riley v. California*, 134 S. Ct. 2473 (2014), the court unanimously held that, because today's cell phones can contain "vast quantities of personal information," police are prohibited from searching a detained suspect's cell phone without first obtaining a warrant. *Riley* suggests that the court will recognize increased privacy expectations when new technology allows large amounts of sensitive ESI to be concentrated in a single location, as with an email account. Similarly, in *United States v. Jones*, 132 S. Ct. 945 (2012), the court held that affixing a GPS tracking device to a suspect's car constituted a "search" under the Fourth Amendment.

> Advancing technology always presents new legal challenges, but it also creates opportunities to develop practical ESI search methods that protect constitutional rights without overburdening legitimate law enforcement investigations.

While the majority opinion in *Jones* based this holding on the trespassory nature of the physical intrusion, the two concurring opinions (one from Justice Sonia Sotomayor and another from Justices Samuel Alito, Stephen Breyer, Ruth Bader Ginsburg, and Elena Kagan) focused on the government's ability to use new GPS technology to engage in long-term, highly accurate locational tracking. Although no expectation of privacy exists with regard to one's movements on public streets, the data recovered from prolonged GPS tracking could, in the aggregate, reveal intimate details about an individual's personal life, and that information deserves Fourth Amendment protection. While *Jones* and *Riley* involved warrantless searches, they nevertheless demonstrate the court's willingness to extend Fourth Amendment protections to large collections of personal data regardless of location in today's mobile society.

Finally, strong arguments can be made against the reasoning in the Roberts and Gorenstein opinions. For example, both rely predominantly on cases involving the seizure of ESI held on personal hard drives, rather than the seizure of ESI held by third-party companies. A major concern in hard-drive cases is data destruction—the fear that the investigation's target will tamper with or erase locally saved data. This concern should not exist with respect to ESI held by a third-party company, like an email provider.

Also, both the Roberts and Gorenstein opinions focus on the "practical need" for the government to seize entire data sets. However, courts could easily mandate the use of various techniques to limit the scope of the government's seizure. By requiring the use of metadata filtering, predictive coding, and other forms of technology-assisted review, a court could strike a practical balance between the government's demand for relevant information and an individual's concern for data privacy. No satisfactory explanation exists as to why these tools—now common tools developed in civil discovery—ought not be applied where privacy concerns reach a constitutional level. Since some members of the judiciary may not fully understand these new technologies, defending parties should be prepared to explain them to the court and advocate for their incorporation into the terms of a warrant, subpoena, or discovery request.

Striking a Balance

As more Americans entrust sensitive ESI to third-parties, it becomes increasingly necessary for courts to develop constitutional and workable limitations on government search warrants for that data. To protect their clients' rights, practitioners must be prepared to educate the judiciary about new techniques for limiting the scope of overly broad ESI warrants. Advancing technology always presents new legal challenges, but it also creates opportunities to develop practical ESI search methods that protect constitutional rights without overburdening legitimate law enforcement investigations. For now, the battle to strike that balance continues.

1. Judge Facciola's foremost opinion on this topic is *In re Search of Info. Associated with [redacted]@Mac.com that is Stored at Premises Controlled by Apple, Inc.*, No. 14-228 (D.D.C. March 7, 2014), and Judge Waxse's is *In the Matter of Applications for Search Warrants for Information Associated with Target Email Accounts/Skype Accounts*, Nos. 13-MJ-8163-JPO, 13-MJ-8164-DJW, 13-MJ-8165-DJW, 13-MJ-8166-JPO, 13-MJ-8167-DJW (D. Kan. Aug. 23, 2013).

2. *In re Search of Info. Associated with [redacted]@Mac.com that is Stored at Premises Controlled by Apple, Inc.*, No. 14-228 (D.D.C. Aug. 8, 2014).

3. *In the Matter of a Warrant for All Content and Other Info. Associated with the Email Account xxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc.,* No. 14 Mag. 309 (S.D.N.Y. July 18, 2014).

Reprinted with permission from the September 10, 2014 edition of the NEW YORK LAW JOURNAL © 2014 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382 or reprints@alm.com. # 070-09-14-15