'Weys' to Suppress Seized Electronic Data: Considerations for Prosecution and Defense

RODNEY VILLAZOR AND BRIAN T. BURNS

Federal white-collar criminal investigations almost invariably lead to the seizure of computers, servers, and portable electronic-storage devices. The start of the seizure process is relatively straightforward and can be somewhat dramatic: An assistant U.S. attorney (AUSA) obtains the search warrant from a federal magistrate judge, and shortly thereafter, dozens of federal agents descend upon the "subject premises" with the authority to seize or image computers, servers, electronic media, and the like.

But what happens after the seizure? The people whose devices were seized are often left in limbo for lengthy periods, sometimes years, waiting for the government to indict them or to buzz off (not to mention give them back their stuff). Meanwhile, federal law enforcement agents face the daunting task of sorting through and searching a massive amount of evidence. If potentially privileged materials were seized, "taint" agents must first cull those out. Then the federal case agents must sift through what can be terabytes of seized data to separate the wheat (materials responsive to the search warrant) from the chaff (everything else).

This whole process, of course, is subject to the limitations of the Fourth Amendment. And the manner and timing in which the government undertakes it is wrought with pitfalls for the prosecution and fertile grounds to cultivate for the defense.

The decision last June in *United States v. Wey,*[1] by U.S. District Judge Alison Nathan in the Southern District of New York, shows why. In that case, Judge Nathan suppressed all seized evidence—documents, email messages, business receipts, computer hard drives, and other records seized in the government's investigation—because of inadequacies in the government's search warrants and in the government's execution of the warrants. Judge Nathan ultimately granted the government's request to drop the criminal charges against Wey, and the SEC dropped its own charges against Wey the next month.

This article examines the shortcomings highlighted in the *Wey* case and discusses the practices a criminal defense attorney can use to safeguard a defendant's Fourth Amendment rights in the context of seizures of electronic information. It also proposes a practical solution that federal courts should adopt to avoid unreasonably protracted seizures of a defendant's property.

Background on the *Wey* Search Warrants

Wey was indicted in September 2015 on a variety of fraud-related charges. Wey—who was in the business of facilitating access to U.S. capital markets for Chinese companies by orchestrating "reverse mergers" of the Chinese companies into U.S.-based shell compa-

nies—allegedly ran a scheme of secretly amassing stakes in the shell companies, manipulating their stock prices, selling his holdings at the inflated prices, and laundering the proceeds through accounts in Switzerland and Hong Kong.

In January 2012, the FBI executed two search warrants, one at the offices of Wey's company, New York Global Group, and the other at his apartment in Manhattan. In these searches, the government seized almost 50 pieces of electronic equipment, including computers and cell phones, containing about 18 terabytes of data.

The warrants were broad, authorizing seizure of electronic equipment related to any of over 200 entities listed on the warrants' "Exhibit B." That list included New York Global Group (whose offices were being searched) and Wey and his wife (whose apartment was being searched). Judge Nathan described this structure as "circular" and the limits of Exhibit B as being "no constraint at all."[2] And the government indeed took a broad view of the items to be seized, taking items from the Weys' apartment such as medical records and X-rays of Wey family members.

After taking the electronic equipment, the government initially used a "taint" team to review the electronic data to separate out any privileged material. Wey's counsel aided in this effort by providing an extensive list of attorneys who may have provided legal advice to Wey. This privilege review took about six months, lasting from about June 2012 through the end of that year.

The government next undertook a review of the non-privileged material to identify electronic data responsive to the warrant. This review took place during "10 full-day" sessions conducted by one FBI agent who ran various searches—using a list of search terms that went beyond what was included in "Exhibit B"—and made determinations about whether individual documents, or whole swaths of documents based on a few samples, were responsive to the warrants. Documents tagged "pertinent" were "seized." This review was completed in September 2013, more than a year-and-a-half after the execution of the warrants; it would be two more years before the government would indict Wey.

In August or September 2015, as the government was preparing grand jury presentations aimed at indicting Wey, the government's tags for "pertinence" and "privilege" were somehow lost through a technical malfunction. According to one of the FBI agents, after learning of the lost tags, he instructed an FBI agent new to the case to find specific documents that previously were marked pertinent. But according to that new agent, who was unexpectedly called to testify by Wey's counsel during the suppression hearing and who did so with little-to-no preparation, she was given only general instructions and shown a few samples before searching through the entirety of the electronic data. The court thus concluded that the government ran searches and collected documents from all of the electronic data, not just the subset previously identified as responsive to the warrant.

Throughout the investigation, and through the time of Judge Nathan's decision, the government maintained possession of the nonresponsive data.

Shortcomings in the Warrants and Searches

Under the Fourth Amendment, warrants must be supported by probable cause and must be sufficiently particularized. Warrants cannot be overbroad "general warrants" that allow for "exploratory rummaging" through a person's belongings.[3] But even if a warrant itself is deficient, the items seized under it need not be suppressed if the executing officers acted in "good faith," meaning in "objectively reasonable" reliance on the later-invalidated warrant.[4] The warrants and the government's execution of them in the *Wey* case highlight how the government can botch this process. We review below some of these shortcomings.

Lack of Particularity

The particularity requirement has three parts: first, the warrant must identify the crime for which there is probable cause; second, it must describe the place to be searched; and third, it must specify the items to be seized by their relation to the crimes.[5]

Probably the easiest of these three for the government to satisfy is the first: identification of the crime. Just make sure the warrant lists the suspected crime and the relevant statute. But the government didn't do that in Wey's case. The warrants did not identify any specific crime. While this seems like a no-brainer, it's not the first case in which the government failed to identify a crime in a warrant.[6] For defense counsel, this is an easy deficiency to identify. And while it might not on its own result in suppression, it's a starting point for showing that a search was not "reasonable" under the Fourth Amendment.

More substantively, the warrants in Wey's case lacked particularity because of the "circular" structure that essentially authorized seizure of all records relating to New York Global Group or the Weys, whose premises were searched. Thus, even though the warrants in the *Wey* case had some ostensible limits on the categories of materials that could be seized, their "circular" structure rendered those limits illusory.

Overbreadth

The warrants in *Wey* were also overbroad because, largely as a consequence of the "circular" structure, they authorized seizure of items for which there was no probable cause. And as noted, the government took a broad approach to the items it seized, taking, for example, medical records and X-rays from the Weys' apartment (and, later, making strained justifications for how those items related to the potential crimes).

No Good-Faith Exception

Judge Nathan rejected the government's reliance on the good-faith exception, for a number of reasons.

One of those reasons was a lack of evidence that anything but high-level generalities about the investigation had been given to the executing officers. One way to help justify the good-faith exception is to show that the executing officers relied on their independent knowledge of the investigation to cabin their discretion in executing the warrant, rather than on the defective warrant itself.[7] But in Wey's case, the executing officers were given only a general overview of the matter, even though one FBI agent swore out a lengthy, detailed affidavit outlining the alleged scheme. None of the executing officers read that affidavit.

Another reason the government couldn't rely on the good-faith exception was that the officers overseized. The court cited the X-rays, for example, as items plainly outside the scope of the suspected fraud schemes and further criticized the government for its after-the-fact, strained efforts to justify the seizure of such items.

For the electronic data, the court criticized the government for "return[ing] to the proverbial well" and searching items previously

deemed nonresponsive without getting a new warrant. Such new searches by the government, without a fresh warrant, of material previously deemed nonresponsive, are problematic. That conduct might independently violate the Fourth Amendment, as Wey argued, or, at least, it is evidence that the government was not acting in good faith, as Judge Nathan found.

Lessons From *Wey*

So what can lawyers—both defense and prosecution—learn from *Wey*?

Standards for Reasonable Analysis

First, federal prosecutors and agents should be able to easily avoid overall sloppiness with discipline and organization (see some of the bullets below). The Department of Justice (DOJ) instructs its attorneys to resist limitations on forensic techniques, such as court-mandated protocols or limited search terms, based on the belief that the general reasonableness requirement of the Fourth Amendment still applies to protect a defendant's rights.[8] Nevertheless, *Wey* should factor into every defense attorney's strategy, particularly on cross-examination, on the reasonableness of the execution of the warrant. Some specific points on this issue:

- *Particularity*. Statutes and the specific types of documents that are tied to those statutes—and not catch-all phrases—at a bare minimum, must be spelled out in the warrant.
- *Operational Briefing*. The prosecutors and case agent who best understand the focus of the investigation should ensure that the agents executing the search warrant are given sufficient briefing. For prosecutors, maybe even read the affidavit supporting the warrant to the agents. Nobody did that in *Wey*, and it hurt the government. Without sufficient briefing, agents may indiscriminately seize nonresponsive evidence. For defense attorneys, probe the sufficiency of the briefing.
- *Rule 41(g) Motion to Return Property*. Defense attorneys should promptly file a motion under the Federal Rules of Criminal Procedure's Rule 41(g) for the return of material not responsive to the warrant. While the Second Circuit Court of Appeals, sitting *en banc* in *United States v. Ganias*, outlined reasons why the government's retention of such materials might be appropriate,[9] such a motion can force the government to justify the reasonableness of any prolonged seizure.
- *Taint Review.* As soon as practical, the defense attorney should advise the AUSA of the names of any attorneys or legal staff for the government's taint review. The taint agents, who spend exhaustive hours reviewing and segregating material, will have to employ sufficient measures to identify such specific potentially privileged material.

Standard for Reasonableness of Length of Analysis

Second, once the government takes the devices, what is a reasonable amount of time for it to review the electronic information? There is, of course, authority upholding lengthy delays in even beginning the forensic analysis.[10] However, in *United States v. Metter*,[11] U.S. District Judge Dora Irizarry in the Eastern District of New York found that a 15-month delay before even beginning to review a defendant's hard drive was unconstitutional.[12] Similarly, U.S. District Judge Jed Rakoff of the Southern District of New York, in *United States v. Debbi*,[13] found an eight-month delay unconstitutional.[14] The DOJ, however, maintains that "neither the Fourth Amendment nor Rule 41 imposes any specific limitation on the time period of the government's forensic examination."[15] The underlying justification is that analysis of computers is a "difficult and time-consuming process."[16] In any event, a lengthy delay is likely to provide at least some basis for defense counsel to begin questioning the reasonableness of the government's efforts.

In the Ninth Circuit, a computer-search protocol mandated for warrants offers a practical solution to this problem. Under that protocol, all magistrate judges impose a 120-day limitation on the government's computer analysis but allow for unlimited 120-day extensions. The protocol is used as an attachment for search warrants issued within the Ninth Circuit and provides the following:

> If the original digital device was seized, law enforcement personnel will perform an initial search of the original digital device within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If, after conducting the initial search, law enforcement personnel determine that an original digital device contains any data falling within the list of items to be seized pursuant to this warrant, the government will retain the original digital device to, among other things, litigate the admissibility/authenticity of the seized items at trial, ensure the integrity of the copies, ensure the adequacy of chain of custody, and resolve any issues that potentially might be raised regarding changed conditions of the evidence. If the government needs additional time to determine whether an original digital device contains any data falling within the list of items to be seized pursuant to this warrant, it may seek an extension of the time period from the court within the original 120-day period from the date of execution of the warrant. Once it is determined that the device contains evidence of the above-noted federal offenses, law enforcement may view and handle the device as law enforcement would any other seized piece of evidence.

While it is true that—due to legitimate concerns about the usual sheer volume of data in seized computers and media—the DOJ instructs its prosecutors to oppose the imposition of time limitations,[17] and that the Committee Notes to Rule 41 expressly state that there is "no basis for a 'one size fits all' presumptive [time] period," the Ninth Circuit's 120-day search protocol is not a time limitation, but rather a check on the federal government's ability to unduly delay or unreasonably expand its searches. The protocol does not impair the government from completing its search and review of terabytes of seized data. There are no limitations on the techniques the federal agents decide to employ (other than, of course, the Fourth Amendment's standard of reasonableness). And there are no deadlines for the government to complete the search, only benchmarks for the prosecution to advise the judge of its progress and need for additional time.

If a similar approach had been employed in the *Wey* search warrants (setting aside their facial defects), suppression would have been unlikely. The investigation team in *Wey* would have had to revisit with the magistrate judge every four months to refresh the probable cause finding, and as they discovered evidence of potentially new crimes, they would have submitted new warrant applications to expand the scope of the warrant and continue their

continued on page 47

Search Warrant *continued from page 41*

analysis. The concern of frequent petitions to the courts, expressed in the comments to Rule 41,[18] would also be obviated. In the three years between the issuance of the *Wey* warrants and the indictment, law enforcement would have had to submit fewer than 10 extension requests. And at the very least, by going back to the judge for new warrants and fresh assessments of probable cause, the government likely could have avoided suppression through a successful invocation of the good-faith exception.[19] ⊙

Rodney Villazor is a founding partner of Smith Villazor LLP. He is a trial lawyer representing companies, executives, and other professionals in white collar criminal cases and high-stakes complex civil litigation disputes. Brian T. Burns is an associate at Smith Villazor LLP. He focuses his practice on securities-enforcement defense, complex civil litigation, and white-collar defense. He previously served as a law clerk to U.S. district judges Richard J. Holwell and William H. Pauley III in the Southern District of New York.

Endnotes

[1]*See United States v. Wey*, ___ F. Supp. 3d ___, 2017 WL 2574026 (S.D.N.Y. June 14, 2017) (decision granting suppression).

[2]*Id.* at *22.

[3]*Id.* at *17 (quoting *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013)).

[4]*Id.* at *28.

[5]*Id.* at *17.

[6]*See, e.g.*, *United States v. Romain*, 678 F. App'x 23, 2017 WL 442175, at *2 (noting that "the supporting documents but not the warrant itself detailed the relevant criminal offenses being investigated").

[7]*See Wey*, 2017 WL 2574026, at *30, *33-34.

[8]*See* Exec. Office for U.S. Attorneys, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 79-80 (2009), *available at* https://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf [hereinafter *DOJ Manual*].

[9]*United States v. Ganias*, 824 F.3d 199, 210-16 (2d Cir. 2016).

[10]*See DOJ Manual* at 92 (reviewing cases).

[11]*United States v. Metter*, 860 F. Supp. 2d 205 (E.D.N.Y. 2012).

[12]*Id.* at 215.

[13]*United States v. Debbi*, 244 F. Supp. 2d 235 (S.D.N.Y. 2003).

[14]*Id.* at 238.

[15]*See DOJ Manual* at 91.

[16]*Id.* at 93.

[17]*DOJ Manual* at 93.

[18]*See* Federal Rules of Criminal Procedure 41, Committee Notes on 2009 Amendments ("[T]o arbitrarily set a presumptive time period for the return could result in frequent petitions to the court for additional time.").

[19]*Compare Ganias*, 824 F.3d at 200 (upholding good-faith exception where government obtained fresh warrant to search data deemed nonresponsive to previous search warrant).