The Huma Abedin Emails: Herein Lies the Danger of Overseizure

Maranda Fritz, New York Law Journal, (October 31, 2016) -- As we continue to be inundated with the cacophony surrounding the letter of FBI Director James Comey on Friday, we should not lose sight of the troubling legal procedures that resulted in the FBI gaining possession of Abedin's emails. According to press reports, certain "devices" containing emails were "seized" by the FBI approximately a month ago in connection with the investigation of Anthony Weiner. While details of the Weiner investigation are not public, it is likely that the government obtained a warrant that allowed for seizure of electronic files relating to *him*—not the communications of *his wife*.

In this age of massive quantities of electronic data, however, the practice of an initial "overseizure" by the government has become common. Conventional wisdom now holds that the government cannot conduct an on-site review of the volume of data on electronic devices and so it is permitted in the first instance to take or copy the contents of the computer. The clear danger presented by this Anthony Weiner seizure, and the seizures in many cases, is that the consideration that was extended to the government—to allow the initial overseizure for the purpose of complying with the warrant—is being used by the government to seize and retain any confidential, personal or even intimate communications that happen to reside on the seized computer.

'Overseizure'

With the proliferation of computers and electronic storage for business and personal use that can hold immense quantities of data, governmental authorities have argued that the conventional execution of a warrant through an on-site search became impractical and burdensome, and sought permission to image computer devices and then conduct their search of the data at off-site laboratories at a later time. That process, referred to as "overseizure," has been permitted not to dispense with the need to identify responsive material, but to allow the government time to conduct a forensic review off-site. *United States v. Mutschelknaus*, 564 F.Supp.2d 1072, 1077 (D.N.D. 2008); see also *United States v. Graziano*, 558 F.Supp.2d 304, 315 (E.D.N.Y. 2008) (discussing the subsequent forensic review of the computer for responsive material and emphasizing that "the manner of the execution of the warrant in searching the computer will also be subject to judicial review under a reasonableness standard"); *United States v. Soliman*, 06-CR-236, 2008 U.S. Dist. LEXIS 87304, at *1-2 (W.D.N.Y. Oct. 29, 2008) (confirming that "items outside of the scope of the search warrant should be identified and returned to defendant"); DOJ Computer Search Manual 92 ("The Fourth Amendment does require that forensic

analysis of a computer be conducted within a reasonable time.").

The court in *Doane v. United States*, 2009 U.S.Dist.LEXIS 61908, *25-30 (S.D.N.Y. June 1, 2009), focused on the "dilution" of one's right to privacy if the personal communications—even those of a third party—could be retained by the government because they resided on a device that was overseized.

Even where practical considerations permit the government to seize items that are beyond the scope of the warrant, once the fruits of the search are segregated into responsive and non-responsive groups, the 'normal' practice is to return the non-responsive items.… Permitting the government to retain items outside the scope of the warrant without such a showing would dramatically dilute the right to privacy in one's personal papers.

Impermissible Retention

The impermissibility of retaining and using material outside the scope of the warrant is arguably self-evident, but in case after case, the government has conducted a massive overseizure and then simply kept the data. In *United States v. Metter*, 860 F.Supp.2d 205 (E.D.N.Y. 2012), for example, the government seized a total of 61 hard drives from the defendants' offices and their personal computers from their homes. After 15 months, the government still held all of the data, notwithstanding repeated arguments by the defense that nonresponsive material had to be identified and returned. The court concluded that 15 months of inactivity after the original electronic data was seized was plainly unreasonable, found that the only appropriate remedy was suppression, and suppressed 61 hard drives.

The risk to Fourth Amendment protections occasioned by the overseizure issue was discussed in *United States v. Collins*, 2012 U.S. Dist. LEXIS 111583 (N.D. Cal. Aug. 8, 2012). In response to the government's assertions regarding the "usefulness" of retaining all of the data and the difficulty of the review of the enormous volume of seized data, the court pointed out that the government's position would eviscerate constitutional protections.

If separating non-targeted data from targeted data and devices lawfully retained as criminal instrumentalities is too hard here, it presumably is too hard everywhere. In what case where a storage device is seized lawfully could a defendant or other subject of a search warrant ever secure return of data that the government had no right to take? Just about every storage device can be searched more easily with automated scripts than manually. Just about every storage device has non-targeted data that might prove useful to understanding the data that was targeted. Just about every storage device has deleted files in unallocated space. If the government's argument were accepted here, so that it need not return even one bit of data that is clearly outside the scope of the warrant, the court thus would render a nullity the government's pledge in just about every search warrant application it files in

this district that it will return data that it simply has no right to seize.

These concerns regarding overseizure were discussed, and exacerbated, by the decision and rehearing of the U.S. Court of Appeals for the Second Circuit in *United States v. Ganias*, 755 F.3d 125 (2d Cir. 2014); on reh. en banc, No. 12-240-cr (May 27, 2016). The government in the Ganias case had seized computer files as part of one investigation, properly identified files that were outside the scope of the warrant, but then held those nonresponsive files for literally years. When the FBI undertook a further investigation of the defendant on a different issue, it obtained another warrant for the files that were still in its possession and, based on those documents, ultimately charged him with tax fraud.

The defense argued that the retention of the material was unconstitutional and sought its suppression. The Second Circuit agreed, concluding that the government had "clearly violated" the defendant's Fourth Amendment rights by seizing and retaining for 2½ years the nonresponsive files.

But then the Second Circuit decided to rehear the matter en banc and, in a decision in May of this year, held that the files could be used in the subsequent prosecution. *United States v. Ganias*, on reh. en banc (2d Cir. May 27, 2016). In that en banc decision, the Second Circuit questioned whether the same precepts that have long governed the seizure of one's personal papers should also be applied to electronic seizures.

It then dug deep into the weeds of the creation and storage of electronic data and decided that the complexities of those technical issues might require that electronic retention be treated differently from traditional data, and might justify the retention of entirely nonresponsive files to facilitate either review or authentication. But, the court concluded, it would not actually decide the issue because it concluded that the agents were acting in "good faith" and so the material would not be suppressed.

In a dissenting opinion, Judge Denny Chin persuasively argued that the intricacies of electronic file storage cannot be used to so radically alter and diminish our Fourth Amendment protections.

The Anthony Weiner Seizures

Which brings us back to the process that is being employed in relation to the seizure in the Anthony Weiner investigation. The warrant would have permitted the seizure of Weiner's communications and so his wife's personal or business communications were not within its scope, the FBI never had authorization to seize it in the first place, and the FBI cannot retain or use it. Assuming the appropriateness of an initial overseizure, it is a simple forensic process to identify communications that Weiner sent, and leave the rest of the material alone. But that is clearly not what happened.

Instead, through some other kind of "review" process, the FBI determined that the computer contained emails of Huma Abedin. The FBI then decided that it wanted those emails too, but was apparently at least mindful that it had no legal right to review them. It therefore made the decision to seek a further warrant. While the details of the warrant were not made public, typically, when the government seeks a warrant to search data outside the scope of a previous warrant, it argues that the nonresponsive data were "in plain view."

While that use of the "plain view" doctrine is highly questionable in these circumstances, because a properly tailored forensic review would not have disclosed Abedin's communications, the seizure has occurred in the midst of an ongoing investigation and so there is little or no opportunity for anyone to challenge the issuance of a warrant for the "overseized" material. Thus, the Weiner seizure illustrates the process that so many privacy advocates feared: The overseizure becomes the opportunity for the government to, at its leisure, peruse the contents of a personal electronic device or email account and decide what additional information it wants to keep and use.

This is a dangerous circumstance.

Maranda Fritz *is a partner at Thompson Hine.*