The Huma Abedin Emails: Election Is Over but the Issues Persist

Maranda Fritz and Brian Waller, New York Law Journal, (November 9, 2016) -- In a Law Journal article last week, "The Huma Abedin Emails: Herein Lies the Danger of Overseizure," (Nov. 1, 2016), we discussed the government's practice of "overseizure" that resulted in the FBI accessing Huma Abedin's emails even though its warrant authorized a search for and seizure of the communications of Anthony Weiner. Since then, the legal machinations continued to their stunning conclusion when, on Sunday, FBI Director James Comey announced that the FBI had not located any new or significant evidence and that he was adhering to his earlier recommendation. Then, on Tuesday, the Republican candidate prevailed in the election.

The FBI investigation of Hillary Clinton's handling of emails may be closed—again—and the next president chosen, but in the process, troubling aspects of the criminal justice system became the subject of intense scrutiny and continuous commentary. Even as the media moves on to post-election coverage, the issues arising from the government's overseizure practices, and the actions of the FBI, remain crucial concerns for the legal community.

Is Overseizure Necessary?

First, the problematic practice of government "overseizure" was on display for the entire country to see, yet there was little hue and cry about the fact that the FBI had taken and was accessing the personal communications of a veritable bystander. That process of allowing the government to "overseize" the entire contents of a computer—where the government then uses that process as an opportunity to "search" the entire contents—arguably threatens to slowly but surely weaken and impair fundamental constitutional principles and privacy interests.

If that practice becomes the norm, the government could, in any case, obtain a properly particularized warrant, seize entire computers and hard drives, and then look through the contents and decide if there is any other material that is relevant to its investigation—or to an entirely different alleged offense. The government could then go back to the court, now armed with the fact that it has happened on files that were supposedly "in plain view," and obtain authorization to seize that information as well. Through that process, the government would have seized and examined the entire computer—without a warrant. Surely that seeming end run around the warrant requirement should not be permissible.

But, one might argue, that kind of unbridled review of the contents of a computer is the modern and electronic equivalent of any old-fashioned search: The government is allowed to "search" through one's belongings to locate that which is within the scope of the warrant. That assumption, though, fails on two grounds. First, when it comes to the contents of a computer, a general and unrestricted search constitutes a far greater interference with privacy rights than would a traditional search.

As noted by the court in *United States v. Abdellatif*, 2010 WL 5252852 at *5 (W.D.N.Y. 2010), "computers are capable of storing immense amounts of information and often contain a great deal of private information"; searches, therefore, "often involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches of other containers." Unlike a traditional search, the overseizure process allows the government prolonged access to a "computer hard drive [that is] akin to a residence in terms of the scope and quantity of private information it may contain." *United States v. Galpin*, 720 F.3d 436, 446 (2d Cir. 2013).

The Supreme Court in *Riley v. California*, 134 S.Ct. 2473, 2490 (2014), recognized the

daunting challenges that are presented by electronic searches precisely because they have the capacity to store vast amounts of material that include the most personal, private, and confidential subjects having nothing to do with a given warrant.

Technological innovation allows computers to function as "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers," and they can store "millions of pages of text, thousands of pictures, or hundreds of videos." Id. at 2489. These devices become "a digital record of nearly every aspect of [users'] lives—from the mundane to the intimate."

Citing *Ontario v. Quon*, 560 U. S. 746, 760 (2010).

Second, a generalized search of electronic data is, as a practical matter, unnecessary. With the advent of electronic storage came electronic means to search and locate data. There are any number of "sophisticated search tools" that "allow the government to find specific data without having to examine every file on a hard drive or flash drive." *In re Search of Apple iPhone*, 31 F.Supp.3d 159, 166-167 (D.D.C. 2014).

Search Protocols

Given those circumstances, the requirement of a narrowly tailored forensic search is a critical response to "overseizure," but that kind of targeted search process will be the norm only if counsel and the courts scrutinize the process by which a forensic review is conducted. Early in the jurisprudence concerning electronic seizures, the U.S. Court of Appeals for the Ninth Circuit suggested that, where an overseizure is necessary, the warrant should also set forth the protocols that would be employed to ensure that the government used the least invasive means by which to locate that which was within the scope of the warrant.

> We recognize that overseizing is an inherent part of the electronic search process and proceed on the assumption that, when it comes to seizure of electronic records, this will be far more common than in the days of paper records. This calls for greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures. *The process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect.*

United States v. Comprehensive Drug Testing, 621 F.3d 1162, 1177 (9th Cir. 2010) (emphasis added).

The Ninth Circuit ultimately declined to impose a requirement that protocols be included in a warrant application. The U.S. Court of Appeals for the Second Circuit has likewise declined to require search protocols but has emphasized the "potential for privacy violations occasioned by an unbridled, exploratory search of a hard drive" and indicated that the plain view exception might not apply to searches of electronic materials. *United States v. Galpin*, 720 F.3d at 451. Other courts have stated that, given the absence of protocols or other judicial guidance, they will scrutinize the treatment of "overseized" data to ensure that the government has performed searches specifically designed to ensure compliance with a particularized warrant. See *United States v. Graziano*, 558 F.Supp.2d 304, 315 (E.D.N.Y. 2008); *Borden v. United States*, 2010 U.S. Dist. LEXIS 71406 (M.D. Fla. 2010). As observed in *Graziano*,

> …the rejection of the blanket rule [requiring search protocols] does not give law enforcement a license to turn every search of a computer into a general search; rather,

> there are Fourth Amendment limits to every search that apply with equal force to searches of computers. Thus, although courts are ill-suited to micromanage in advance how the computer will be searched, law enforcement must establish the basis for searching the computer and particularize the evidence being sought during such search.

Graziano, 558 F.Supp.2d at 316.

Handling of Weiner Computer

We now know that the seizure and search of Anthony Weiner's computer constituted a textbook example of an overseizure. By last Sunday, the press reported that the FBI had gone back to the judge with an application for authorization to seize the emails of Huma Abedin based on the presence of those emails on the computer and an analysis of the associated metadata. But those steps that were taken to obtain that further warrant arguably illustrate the precise circumstances that make unrestrained overseizure so dangerous.

First, there appears to have been no need or justification for the government to have been browsing through the computer. Responsive material could and should have been located using simple forensic searches that would identify and extract his communications. Even if the warrant also called for seizure of, for example, explicit materials, that too could have been located through targeted searches for files with certain characteristics. Reviewing the contents of the computer, and even reviewing Abedin's emails, would not appear to be the least invasive or the appropriate means by which to identify the materials within the scope of the Weiner warrant.

Further, even if the FBI had inadvertently located Abedin's emails on the computer, Fourth Amendment law requires that they cease any further review. Her emails were clearly not within the scope of the warrant nor are they criminal contraband. According to published reports, however, the FBI did not step away from the nonresponsive material. Instead, it went the additional step of analyzing metadata associated with those emails and then used that analysis in an application to obtain a further warrant. The metadata were not, however, "in plain view," and that additional scrutiny of Abedin's communications appears not to be permissible.

Given these clear issues associated with the FBI's handling of Weiner's computer, and the incessant discussion of the issue over the last week, it is surprising that there was not more attention paid to a fundamental question: Do we accept the premise that the FBI can seize a computer pursuant to a particularized warrant but then rifle through it and thereby discover, purportedly "in plain view," other evidence, or did we just witness an almost nonchalant reaction to an apparently impermissible use of overseizure?

The Comey Communications

While there was little reaction in the public discourse to the electronic seizure issue, there was obviously an outcry regarding the actions of FBI Director Comey. His actions, as well as reported FBI leaks, implicated the Hatch Act, 5 U.S.C. §7323(a)(1), which prohibits the use of office "for the purpose of interfering with or affecting the result of an election." While many argue that he did not intend to affect the results of the election, we all know the basic tenet that one will be considered to intend the natural and foreseeable consequences of his actions, and the aggressive use of Comey's communication by one of the candidates, and its immediate and dramatic

impact on the presidential race, was unquestionably foreseeable.

In addition, his actions violated long-standing Department of Justice policies regarding "Election Year Sensitivities," so much so that nearly 100 former prosecutors and DOJ officials felt compelled to question publicly his decision to violate those policies. The damage done to the credibility of the FBI is perhaps even more painful because we now know that it was pointless: Had the FBI reviewed the material first, instead of making a public announcement that it was going to review documents that may or may not be relevant (and assuming that FBI agents could be trusted to not improperly disclose that investigative activity), the proper course would have been followed without the seismic impact on the presidential race.

The Justice Department, through the Yates Memo,[1] recently adopted a significant change in its policies regarding the focus of prosecutions, mandating that a corporation, to receive cooperation credit and avoid being charged, had to develop and provide evidence with respect to the individuals who engaged in the conduct under investigation; an organizational claim that "mistakes were made," absent the "who, what and when" of how that conduct occurred, would no longer be acceptable. Having now watched as the FBI director's statements in July, and his letter of last week, were used to demonstrably alter the presidential race, these issues of the FBI's communications and its leaks should be scrutinized and, if misconduct is found, should be subject to the same standard.

Endnote:

1. Memorandum of Deputy Attorney General Sally Yates dated September 9, 2015, Individual Accountability for Corporate Wrongdoing, located at https://www.justice.gov/dag/file/769036/download.

Maranda Fritz is a partner at Thompson Hine. Brian Waller is counsel at the firm.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or ALM Media Properties, LLC., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

Copyright 2016. ALM Media Properties, LLC. All rights reserved.