

Hidden Legal Lessons In Anthony Weiner's Laptop: Part 1

By **John Reed Stark**, former SEC internet enforcement chief

Law360, New York (November 21, 2016, 11:26 AM EST) -- Amid the exhaustive punditry and analysis concerning FBI Director James Comey's startling disclosure of a rejuvenated Hillary Clinton criminal investigation, some critical questions seem to have gotten lost in the shuffle. Namely, what are the legalities involved when handling Anthony Weiner's (or anyone else's) laptop computer; and could Anthony Weiner's lawyers have avoided this entire situation had they been more careful?

This is the first of a two-part article that comprehensively analyzes the multiple and complex legal issues relating to the Weiner laptop computer and offers some useful advice for managing these issues thoughtfully, cautiously, prudently and successfully.



John Reed Stark

Specifically, the first part of the article: 1) introduces the legal issues surrounding the government's acquisition of the Weiner laptop computer; and 2) analyzes the issues pertaining to the Weiner laptop computer arising in a criminal investigatory and prosecutorial context.

The second part of the article: 1) addresses the same issues when they arise in a civil investigatory, regulatory or administrative context such as with the U.S. Securities and Exchange Commission (which are dramatically different and require an altogether different analysis and approach); and 2) offers some practice tips and final thoughts.

What the Weiner Laptop Computer Might Contain

Not surprisingly, the Weiner laptop computer is an important piece of evidence. So-called ESDs (electronic storage devices, such as laptop and desktop computers, company servers, individual smartphones and tablets and any other hard drive, thumb drive or virtual storage contraption or facility) have time and again provided law enforcement with the 21st-century equivalent of the proverbial smoking gun.

Active Data

In Weiner's case, his alleged illicit sexting and possible unlawful relationship with a minor has accidentally engulfed Hillary Clinton — because his device contained "active data" such as actual emails or perhaps email headers or other related cache pertaining to Clinton's role as secretary of state or her role in any other possible criminal undertaking or conspiracy, including obstruction of justice.

But the evidentiary possibilities do not stop there. The "active data" on the Weiner laptop

computer might not only contain exculpatory or inculpatory email communications and other relevant data. The Weiner laptop computer likely also includes gigabytes of irrelevant private and personal information of Weiner, Huma Abedin or anyone else who used the device for any purpose, including Weiner and Abedin's friends, family, colleagues, etc.

The Weiner laptop computer could also include information protected by domestic or foreign statute or requiring notice of disclosure per contract; personal health information of Weiner, Abedin or other family and friends; or privileged communications with counsel or attorney work product.

Given the likely scenario that the FBI agents charged with analyzing the laptop did not have authority to review data other than that specified in the search warrant, some semblance of the Clinton/Abedin emails were probably active data "in plain view" during the review of the Weiner laptop computer, which triggered the heightened scrutiny and the need for a new search warrant.

Inactive Data

Most users have no idea of the contents of the "inactive data" on their ESDs, such as data within deleted recoverable files, unallocated and slack space or the boot sector, found during a digital forensic deep dive of a hard drive.

This kind of "inactive" evidence, which is rarely "in plain view" can contain unanticipated inculpatory information — and has ushered in an exciting and extraordinary era of a scientific approach toward identifying, capturing, harvesting, warehousing, perusing and ultimately introducing as evidence, critical, evidence at trial.

To illustrate the extraordinary impact of digital evidence, consider the history of traditional documentary evidence used in trials and prosecutions. For instance, the typical office worker has a trash bin in his or her office and disregards written documents in that trash bin throughout the day. At the end of the day or week, the contents of this trash bin are then emptied and transferred into a dumpster in the basement of the office building. At the end of the week, the trash dumpster is emptied and its contents are transported to a landfill or other trash facility. Historically, once emptied into a trash bin, discharged into a dumpster and/or transported to a landfill, any evidence contained in those places was very difficult, costly and challenging for law enforcement to recover.

But in today's virtual world of ESDs and universal digital communications, not only are the virtual trash bins, dumpsters and landfills immediately accessible to the government, even a sledgehammer or a blowtorch might not fully destroy the evidence contained therein.

Why is data so hard to destroy? Of course, with respect to an email, once sent, the sender typically loses any control over its contents and thereby has little chance of securing its deletion. With respect to documentary data, such as a letter, memorandum, presentation, notes from a meeting, etc., when that data file is deleted, its address is merely changed to unallocated space, but the text remains in free space unless it is overwritten, either intentionally or in the course of a device's normal operating processes.

Similarly, at the end of every saved file is "slack space," which contains various unexpected remnants, fragments and artifacts, including text from other files that were deleted then overwritten by shorter files and text that were never intentionally saved (perhaps forgotten, hidden on the device or otherwise in "not-so-plain" view).

These hidden files on laptops and other ESDs can include an almost infinite hoard of evidence, which a user perhaps believed had already been intentionally deleted or even worse, simply never knew existed. This is probably why Hilary Clinton or her advisers instructed her information technology team to use BleachBit to delete her files, a data wiping tool that purports to wipe disks so clean of data that, "even God can't read them."

Whether active data or inactive data, electronic evidence can also present challenges relating to its authenticity and relevance, when seeking its admissibility in a civil or criminal proceeding. For instance, a teenage child, a family friend, or even a visiting contractor could be using the Weiner/Abedin computer for unlawful purposes and could have, for instance, left evidence along those lines in unallocated or slack space — wrongly implicating Weiner or Abedin.

The Law Regarding the Weiner Laptop Computer

There are grave consequences when the government obtains a laptop from a witness, object, target, defendant or any other investigatory classification, and the risks of turning over a device to the government, without defense counsel's proper review of that device, are considerable.

Defense counsel must not only understand the technological results of the review, examination, analysis or forensic deep dive of an ESD but must also understand the legal issues triggered when the government requests, subpoenas, seizes via search warrant, or otherwise obtains or recovers the ESD of an American citizen.

Search Warrants and ESDs

First and foremost, the Fourth Amendment to the Constitution states that no search warrant can be issued unless it "particularly describes the place to be searched and the things to be seized."

The law has developed that with respect to federal criminal search warrants for ESDs, the government must limit its searches of ESDs with the same particularity required of any search, and the government must: (1) explain how relevant data will be distinguished from irrelevant data; (2) note how the information will relate specifically to the underlying allegations; and (3) follow detailed protocols to avoid revealing nonresponsive information, privileged information and other protected information. These search warrants of federal criminal authorities are subject to judicial oversight, when the prosecutor applies for the search warrant from a federal judge before their issuance.

Along these lines, an affidavit and application for a warrant to search a computer are in most respects the same as any other search warrant affidavit and application:

- The affiant swears to facts that establish that there is probable cause to believe that evidence of crime (such as records), contraband, fruits of crime, or instrumentalities of crime is present in a private space (such as a computer's hard drive, or other media, which in turn may be in another private space, such as a home or office); and
- The warrant describes with particularity the things (records and other data, or perhaps the computer itself) to be searched and seized.

By the same token, like any other warrant describing with particularity the "things to be seized," a search warrant for an ESD has two distinct elements. First, the warrant must describe the things to be seized with sufficiently precise language so that it tells the officers how to separate the items properly subject to seizure from irrelevant items. Second, the description of the things to be seized should be limited to the scope of the probable cause established in the warrant. Considered together, the elements forbid government investigators from obtaining "general warrants" and instead require them to conduct narrow seizures that attempt to "minimize" unwarranted intrusions upon privacy.

Particularity

The most critical distinction between a traditional search warrant and a search warrant of an ESD is the heightened level of particularity expected. When probable cause to search relates in whole or in part to information stored on the computer, the warrant must identify that information with particularity, focusing on the content of the relevant files rather than on the storage devices that may happen to contain them. In cases where the computer is merely a storage device for evidence, failure to focus on the relevant files may lead to a Fourth Amendment violation.

For instance, FBI agents cannot simply request permission to seize "all records" from an operating business unless agents have probable cause to believe that the criminal activity under investigation pervades the entire business. Likewise, seeking in a warrant "any and all data, including but not limited to" a list of items, a similarly dangerous phrase, also lacks particularity and has also been held to turn a computer search warrant into an unconstitutional general warrant.

Along these lines, search warrants for ESDs should also include some sort of temporal particularity with respect to the relevant time period of any potential criminal violation or are otherwise subject to a successful challenge.

This notion of particularity is critical. Even in its own guidelines pertaining to the search and seizure of computers, the U.S. Department of Justice itself acknowledges that the law prefers searches of all things, including computer data, to be as discrete and specific as possible, and advises federal prosecutors and agents to describe with particularity the specific set of techniques they will use to distinguish incriminating documents intermingled with innocuous ones.

Forensic Imaging

If possible, Weiner's counsel should have bargained for keeping a forensic copy of the hard drive of the Weiner laptop computer, rather than the laptop itself; this way, counsel could have an opportunity to review the same evidence that the government is reviewing.

In many cases, rather than seize an entire computer for on-site review, FBI agents can instead create a digital copy of the hard drive that is identical to the original in every relevant respect. This copy is called a "forensic image copy" — a copy that identically duplicates every bit and byte on the ESD, including the unallocated space, the slack space, the boot sector, master file table and metadata, in exactly the order they appear on the original. The forensic image copying also uses a process that does not disrupt the data contained on the ESD, such as the "creation date" of a Word document, the "read date" of an email, or the "last accessed date" of a presentation.

Federal Criminal Grand Jury Subpoenas for ESDs

Aside from the legal standards involved, the two most significant practical differences between a grand jury subpoena seeking an ESD and a search warrant allowing for the seizure of an ESD are: 1) the opportunity for counsel to object and negotiate a response to the subpoena's specific demands; and 2) the opportunity to create a forensic image of the ESD that the government has subpoenaed.

When subpoena recipients do not want to comply with a grand jury subpoena, they can challenge it by filing a motion to quash with the court that supervises the grand jury. The motion to quash says, essentially, that the subpoena should not be enforced for specific reasons, such as the subpoena would violate the attorney-client privilege, the subpoena lacks sufficient particularity, or the subpoena is overbroad.

By moving to quash a grand jury subpoena, defense counsel in effect raises the bar for the government because, unlike a search warrant, the government issues grand jury subpoenas without any showing of probable cause, with only limited constitutional restrictions, or without any other reason to believe relevant evidence will be produced. In fact, a grand jury "can investigate merely on suspicion the law is being violated, or even just because it wants to assure that it is

not." This power to investigate, based on mere suspicion, makes defending against grand jury subpoenas extremely difficult.

With respect to grand jury subpoenas for actual ESDs, there is only a small amount of emerging case law and precedent. The few cases addressing this issue have recognized the centrality of relevance and particularity, in the ways in which they balance the two. Thus, with respect to federal criminal grand jury subpoenas for ESDs, the government does not necessarily avoid the probable cause and particularity requirements of a search warrant. Criminal subpoenas for devices capable of being used for data storage with no express safeguard against a subsequent rummaging through, and seizure of, irrelevant as well as relevant data (such as a judicially sanctioned search methodology), do not withstand Fourth Amendment reasonableness scrutiny.

The FBI Discovery of Abedin/Clinton Emails on the Weiner Laptop Computer

Finding commingled data on one single laptop like the Weiner laptop computer, e.g. belonging to Abedin and pertaining to irrelevant activities, is not unusual and will trigger certain important law enforcement protocols.

Few computers are dedicated to a single purpose; rather, computers can perform many functions, such as "postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more." Thus, almost every hard drive encountered by law enforcement will contain records that have nothing to do with the investigation. The Fourth Amendment governs how investigators may search among the commingled records to isolate those records that are called for by the warrant.

The U.S. Supreme Court has noted that in a search of commingled records, "it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized." Therefore, responsible officials, including judicial officials, must take care to assure that searches are conducted "in a manner that minimizes unwarranted intrusions upon privacy."

For instance, when an FBI agent encounters data on a laptop outside the scope of a search warrant, such as with the Abedin/Clinton emails found during its ostensibly unrelated search of the Weiner laptop computer, courts have set forth guidelines for an agent's review of commingled records to identify data (such as emails) that fall within the scope of a warrant.

Some older cases appear to suggest that when agents executing a search encounter commingled records, they should seize the records, and then seek additional approval from the magistrate before proceeding — which appears to be the situation with the Weiner laptop computer.

For example, the Ninth Circuit, writing about a search of paper files in an age before computer searches were common, suggested that in the "comparatively rare instances" where "documents are so intermingled that they cannot feasibly be sorted on site," law enforcement "can avoid violating fourth amendment rights by sealing and holding the documents pending approval by a magistrate of a further search."

One leading case allows a "brief perusal" of each document, and requires that "the perusal must cease at the point of which the warrant's inapplicability to each document is clear," just like, "the police may look through ... file cabinets, files and similar items and briefly peruse their contents to determine whether they are among the documentary items to be seized."

The Second Weiner Search Warrant

If a document falls outside the scope of the warrant but nonetheless is incriminating, that document's "seizure" is permissible only if during that brief perusal the document's "otherwise incriminating character becomes obvious." This was probably the situation with the Weiner laptop

computer: while the existence of the Clinton/Abedin emails was clear, their relevance and inculpatory value was probably not.

It appears that Comey's team was following DOJ guidelines, which state that when it becomes necessary for an investigator to personally examine a computer file to determine whether it falls within the scope of the warrant, the investigator must take all necessary steps to analyze the file thoroughly, but the investigator should cease the examination of that file as soon as it becomes clear that the warrant does not apply to that file. This is perhaps why Comey appeared to have little idea of the content of the actual Clinton/Abedin emails — and only knew of their existence.

Obtaining the second warrant can be critical. In a 1999 federal case, detectives obtained a warrant to search the defendant's computer for records of narcotics sales. Searching the computer back at the police station, a detective discovered images of child pornography. At that point, the detective "abandoned the search for drug-related evidence" and instead searched the entire hard drive for evidence of child pornography. The Tenth Circuit suppressed the child pornography, holding that the subsequent search for child pornography exceeded the scope of the original warrant because law enforcement may not expand the scope of a search beyond its original justification.

Weiner's Consent to Search His Laptop

The issue of consenting to a search, whether of a computer, a premises or even of a person, can be a confusing one. In computer crime cases, where devices such as a laptop are at issue, two consent issues arise particularly often.

First, when does a search exceed the scope of consent? For example, when someone consents to the search of a location, to what extent does the consent authorize the retrieval of information stored in computers at the location?

Second, who is the proper party to consent to a search? Do spouses (or estranged spouses like Weiner), roommates, friends, and parents have the authority to consent to a search of another person's computer files?

With respect to the search of Weiner's laptop, the nature and scope of Weiner's consent was probably an issue — which is another reason why the FBI had to request that the DOJ apply for a second search warrant.

Computer cases often raise the question of whether general consent to search a location or item implicitly includes consent to access the memory of electronic storage devices encountered during the search. In such cases, courts look to whether the particular circumstances of the investigator's request for consent implicitly or explicitly limited the scope of the search to a particular type, scope, or duration. Because this approach ultimately relies on fact-driven notions of common sense, results reached in published judicial decisions have hinged upon subtle (if not entirely inscrutable) distinctions.

In matters like those involving the Weiner laptop computer, when FBI agents obtain consent for one reason (a possible illicit relationship with a 15-year-old girl) but then conduct a search for another reason (misuse of classified information), the FBI agents must be careful to make sure that the scope of consent encompasses their actual search.

Search Protocol

Whatever method the FBI is using to review the Weiner laptop computer is probably permissible, even if Weiner's counsel negotiated a specific method for the electronic review of the Weiner laptop computer. The scope of consent usually relates to the target item, location and purpose of the search, rather than the search methodology used.

For example, in a 2005 federal case, an FBI agent received permission to conduct a “complete search” of the defendant’s computer for child pornography. The agent explained that he would use a “pre-search” disk to find and display image files, allowing the agent to easily ascertain whether any images contained child pornography. When the disk, for unexplained reasons, failed to function, the agent conducted a manual search for images, eventually discovering several pieces of child pornography. Although the agent ultimately used a different search methodology than the one he described to the defendant, the court approved the manual search because it did not exceed the scope of the described disk search.

Spousal Consent

Even though both he and Abedin use it, Weiner can likely give consent to search the Weiner laptop computer. Absent an affirmative showing that the consenting spouse has no access to the computer searched (physical access, as in a separate locked room, or technological access, as in password-protected), the courts generally hold that either spouse may consent to a search of all of the couple’s property. Even a wife who had left her husband could consent to search of a jointly owned home even though the husband had changed the locks.

Most spousal consent searches are valid, sometimes even when estranged, as is the case between Weiner and Abedin. For example, in one 1998 Illinois case, a man named Smith was living with a woman named Ushman and her two daughters. When allegations of child molestation were raised against Smith, Ushman consented to the search of his computer, which was located in the house in an alcove connected to the master bedroom.

Although Ushman used Smith’s computer only rarely, the district court held that she could consent to the search of Smith’s computer. Because Ushman was not prohibited from entering the alcove and Smith had not password-protected the computer, the court reasoned, she had authority to consent to the search. Even if she lacked actual authority to consent, the court added, she had apparent authority to consent.

ESDs and Privileged Communications

With respect to any communications on the Weiner laptop computer with specially protected relationships, such as communications with a counsel or a doctor, FBI agents must exercise special care when orchestrating a computer search, which could result in the seizure of legally privileged documents such as medical records or attorney-client communications.

Two issues must be considered. First, agents must make sure that the search will not violate the attorney general’s regulations relating to obtaining confidential information from disinterested third parties. Second, agents should devise a strategy for reviewing the seized computer files following the search so that no breach of a privilege occurs.

Along those lines, the FBI agents performing the search of the Weiner laptop computer likely have devised a post-seizure strategy for screening out the privileged files and have likely described that strategy in their search warrant affidavit.

John Reed Stark is president of John Reed Stark Consulting LLC, a data breach response and digital compliance firm, and former chief of the U.S. Securities and Exchange Commission's Office of Internet Enforcement. He has also served for 15 years as an adjunct professor at the Georgetown University Law Center. He is the author of "The Cybersecurity Due Diligence Handbook."

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., 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.