SEARCHES WITHOUT BORDERS: DIGITAL A PRIMER ON SEARCHES AND THE PLAIN VIEW DOCTRINE[1]

In application, many aspects of the Fourth Amendment can be more challenging than putting together a jigsaw puzzle when all of the pieces are face down. Conversely, some aspects of the Fourth Amendment are so clear that any lay person can understand them without seeking the guidance of legal counsel. For instance, when government agents ("agents") execute a search warrant, where does the plain language of the warrant permit them to search, and what does that same plain language say they can seize?

This article addresses a continuing development in Fourth Amendment jurisprudence that a lay person may expect to be crystal clear – the scope of a warrant to search electronic data, *i.e.* computer servers, iPhones, and/or cloud storage. Let's pose the following question to a hypothetical lay person:

> If the Government is investigating a company or person for a fraud crime that began in 2021, should the Government be allowed to: (1) make a copy of the person's or company's entire computer server – which consists of millions of electronic files that will indisputably contain data created before the 2021 fraud scheme began; (2) search the *entire* server to determine whether each individual file (of millions) is responsive to a warrant permitting a search for evidence of a 2021 fraud; and (3) seize evidence of a totally unrelated crime (for example, tax evasion) during a totally unrelated time-period (lets say, 2019) discovered *during the search* on the basis that the

[1] Scott Gilbert handles federal criminal and civil litigation, with a focus on white collar crime, asset forfeiture and the False Claims Act. After serving as an Assistant United States Attorney for 10 years, Scott joined the White Collar practice group at Watkins & Eager, where he has worked for 7 years. Sidney Lampton also practices in the White Collar group at Watkins & Eager where she litigates criminal and civil cases. Now in her fourth year of law practice, Sidney previously clerked for United States District Judge David Bramlett.

> evidence was in 'plain view' of the Government as one of the millions of files opened to determine if it was subject to the contours of the warrant?

The average lay person may not understand the legal intricacies implicated by our question, but that same lay person will very likely have an innate belief that virtually unlimited access to private data is unreasonable and not consistent with the Fourth Amendment.

Those who are old enough will remember how we all collectively held our breath as Y2K came and went without shutting down every computer in the world. Since that time, there has been an exponential growth of digital devices and electronic data. Today, businesses and individuals have no option but to utilize digital storage in many aspects of their lives. Over the last 22 years, we have witnessed the death of the filing cabinet, the obsolescence of the photo album, the shuttering of music and video stores, and the end of caring how many gigabytes your hard drive can hold. Now, our private information lives inside cellphones, tablets, computers, and cloud storage. As a result, there are compelling reasons for innocent people to encrypt and secure their private data, *i.e.* "[the] protection of privacy, preservation of privileged communications, warding off industrial espionage or preventing general mischief such as identity theft."[2]

However, the evolution of the digital age did not miraculously avoid the corruption of crime. On the contrary, law breakers also avail themselves of digital

[2] *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010).

storage. They too have a significant incentive to encrypt and secure their private data to hide evidence of illegal activity. This digital evolution means that evidence of a crime may exist wherever an electronic device is located at any given moment. Evidence is no longer primarily found inside the marked drawers of filing cabinets, neatly stuffed into labeled file folders, or hidden in a cardboard box under a blanket in the top of a closet. Instead, it's on a phone, computer, or cloud storage.

The location and type of evidence may have changed but the need to protect people from vigorous criminal investigations exceeding the bounds of the Fourth Amendment has not. Likewise, neither has the government's need to identify and obtain evidence to prosecute wrongdoers. Yet, a search of digital data is far different than that of a physical filing cabinet. Digital storage intermingles and maintains data in ways that make it "difficult [for the government] to retrieve without a thorough understanding of the filing and classification systems used."[3] Moreover, "inexpensive electronic storage media … can store the equivalent of millions of pages of information."[4] That doesn't sound much like a filing cabinet.

Accordingly, law enforcement must now undergo a significantly more tedious and time-consuming process to locate and identify digital evidence. Realistically, agents cannot conduct a digital search like a traditional premises search wherein agents only

[3] *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1175.
[4] *Id.*

seize and remove items responsive to the warrant. Reviewing hundreds, thousands, or even millions of digital files can take weeks or months. This cannot be done in a single sitting. Accordingly, if agents are required to conduct a digital search while remaining on the premises covered by the warrant, the result would be an untenable law enforcement presence at a person's home or business. This leaves agents with one option – to seize, or at least copy, the digital storage device to subsequently search its contents ***off*** the premises.

Therefore, unlike a normal premises search, a digital search does not restrict agents to identify and physically take ***only those items the warrant permits*** to be seized. Agents searching a filing cabinet might need to briefly look over all the papers present, but they would not seize and *retain* papers outside the scope of the warrant. In a digital search, agents may opt to *take and hold on to the entire digital storage device* even though, in many cases, agents know that the vast majority of electronic files on the device fall outside the scope of the warrant.

The government now has possession of *all* of a company's electronic files. This may include confidential documents, trade secrets, proprietary information, and any other entirely legal document that a company does not want to surrender to the government – even if the government promises to return it (at a date uncertain). This process – even though a necessity under some circumstances – is facially and conceptually incongruent with the Fourth Amendment.

Further, it raises two questions: First, is the government conducting a "general search" when viewing every electronic file contained on a seized digital storage medium as a means to identify and seize digital evidence covered by the scope of a warrant? Second, when agents identify evidence of a crime that falls outside the scope of the warrant – because it was necessary to open the electronic file to determine if it is responsive – should the "plain view" doctrine legitimize that discovery?

I. THE SPECIFICITY REQUIREMENT OF THE FOURTH AMENDMENT

When the Bill of Rights was ratified on December 15, 1791, the Fourth Amendment was as straightforward in concept as it was in application: "[N]o Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[5] All warrantless searches are presumed to be unreasonable, absent one of those pesky enumerated exigent circumstances. In an overly simplified explanation, if a search is unreasonable, either because the search was warrantless or it fell outside the scope of the warrant, then any evidence discovered as a result of the unreasonable search is excluded. The exclusionary rule deters unconstitutional searches because the discovered evidence cannot be used in trial. As such, the validity and scope of a warrant is often at the forefront of criminal defense.

[5] United States Constitution, Fourth Amendment.

To be facially valid, a search and seizure warrant must specifically identify the place to be searched and the items to be seized. When agents obtain a warrant to search your house, that same warrant does not permit agents to drive across town and search your place of business. Similarly, the government cannot get a warrant to seize a particular item without a supporting affidavit that "make[s] it apparent … that there is some nexus between the items to be seized and the criminal activity being investigated."[6] Warrants only authorize agents to seize items connected to the crime described in the warrant, *i.e.* the crime for which a judge has determined there is probable cause.

Requiring a warrant that specifies the place to be searched and the items to be seized makes general searches "impossible."[7] The Supreme Court of the United States noted as such, explaining: "General warrants of course, are prohibited by the Fourth Amendment. '[T]he problem (posed by the general warrant) is not that of intrusion per se, but of a general, exploratory rummaging in a person's belongings…'"[8] Simply put, general searches of private property do not meet constitutional muster.

II. SEARCHES MUST BE EXECUTED WITHIN THE SCOPE OF THE WARRANT

Moreover, agents may not use a facially valid warrant to "get in the door" but subsequently extend their search outside the scope of the warrant. Agents may only search areas where the items approved for seizure can reasonably be located. This is a

[6] *Kohler v. Englade*, 470 F.3d 1104, 1109 (5th Cir. 2006) (citing *Illinois v. Gates*, 462 U.S. 213, 239 (1983)).
[7] *Andresen v. Maryland*, 427 U.S. 463, 480 (1976).
[8] *Id.* (citing *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971)).

relatively simple concept. A warrant that authorizes agents to search for a stolen vehicle does not extend into spaces where a vehicle cannot be found. Agents cannot look for a Ford F-150 in the kitchen cabinets, bedroom dresser, or even a safe. Conversely, a warrant that permits agents to search for very small items, like bullets, will extend into very small spaces, such as a medicine cabinet, a jewelry box, or even down in the tips of the shoes sitting in a closet.

Because agents are authorized to investigate spaces where there is probable cause of a crime, it is not uncommon for agents to find evidence of *additional unrelated* illegal activity. Recognizing that such discoveries are not the result of improper conduct by agents – *i.e.*, unreasonable searches meant to be deterred by the exclusionary rule – Courts created the "plain view doctrine." If agents have a legal right to be at a certain place, they may legally seize evidence of ***any*** crimes discovered within the scope of the search warrant. As stated above, agents may look ***anywhere*** that they reasonably determine a bullet may be hidden. Anything illegal that agents find while poking around is fair game. Therefore, agents can seize a bag of cocaine – discovered in the toe of your shoe – despite not having a specific warrant to do so. The cocaine is in "plain view." Easy enough, right? Not in the context of a digital search.

III. OPENING EVERY FILE IN A DIGITAL DATABASE CONSTITUTES A GENERAL SEARCH

As discussed above, the Fourth Amendment does not allow for general search warrants. However, "[b]y necessity, government efforts to locate particular files will

require examining a great many other files to exclude the possibility that the sought-after data are concealed there."[9] As a result, there is a "serious risk" that "every warrant for electronic information will become a general warrant."[10] The article discusses *infra* proposed methods a court can impose on the government to ensure that a "general search" of electronic data does not occur. Such methods will necessarily be case specific. Practically, there is no clear "blanket solution" that could apply in every case to circumvent the necessity of agents individually examining non-responsive electronic files when determining they're outside the scope of the warrant.

Therefore, if agents are allowed to conduct what amounts to a general search of electronic data to ensure responsive evidence is not missed, is all of the data stored in a particular medium in "plain view" of the agent? This is the position that the government took during its investigation into the Bay Area Laboratory Co-Operative ("BALCO") in connection with Major League Baseball players steroid use.[11] During the BALCO investigation, the government executed a search warrant for the drug testing records of 10 specific players.[12] When the government executed the warrant, it seized and reviewed drug testing records of "hundreds of players in Major League Baseball" because the

[9] *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1176.
[10] *Id*.
[11] *Id*.
[12] *Id*. at 1166.

electronic files of the 10 specific players were intermingled with the electronic files of the non-named players.[13]

The government took the position that, since it had to open each electronic file to find the 10 files covered by the warrant, the remaining files were "in plain view" and were subject to lawful search and seizure.[14] According to the government, "[a]uthorization to search *some* computer files therefore automatically becomes authorization to search all files in the same sub-directory, and all files in an enveloping directory, a neighboring hard drive, a nearby computer or nearby storage media."[15] Taken to its logical conclusion, the government's theory means that "[w]here computers are not near each other, but are connected electronically, the original search might justify examining files in computers many miles away, on a theory that incriminating electronic data could have been shuttled and concealed there."[16]

Multiple courts ultimately disagreed with the government, suppressing the seizure of the records of players not specifically identified by the warrant, and quashing subsequent grand jury subpoenas seeking the records of the additional players.[17] The Ninth Circuit affirmed those decisions.[18]

IV. FEDERAL RULE OF CRIMINAL PROCEDURE 41

[13] *Id*.
[14] *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1176.
[15] *Id*.
[16] *Id*.
[17] *Id.* at 1169-70.
[18] *Id.*

While the BALCO case was working its way through the courts, Congress made changes to Federal Rule of Criminal Procedure 41, which set out a framework for how the government must approach identifying, segregating, and returning electronic data that falls outside the scope of a search warrant. In 2009, Congress amended subdivision (e)(2) of Rule 41 to address searches of electronic storage media.[19] Rule 41(e)(2) recognizes that the amount of data contained in "electronic storage media" makes it "impractical for law enforcement to review all of the information during execution of the warrant at the search location."[20]

The commentary provides that agents must engage in a "two-step process" to ensure that the government identify and return to the property owner any ***copied*** electronic items outside the scope of the warrant. The second step requires agents to "determine what electronically stored information falls within the scope of the warrant."[21] The rule recognizes that agents may initially seize electronic data that likely falls outside the scope of the warrant, but requires agents to subsequently determine what electronic data was not authorized for seizure and to divest itself of possession of that property. Rule 41 does not authorize general searches of electronically stored data or "papers." However, Rule 41 does not explicitly address the issue of the "plain view doctrine." As such, it is up to the courts to ensure that Fourth Amendment protections remain strong in the realm of electronic data.

[19] *See* Advisory Committee Note, Fed.R.Crim.P. 41, 2009 Amendments.
[20] *Id*.
[21] *Id*.

To ensure that searches of digital databases do not become general searches, courts issuing search warrants should impose several requirements on the government consistent with Rule 41 to ensure that the government quickly identifies and returns to the property owner all data not covered by the warrant. One such requirement is for the government, prior to opening a single electronic file, to conduct an initial high-level search of the seized data to identify any files that were created or last modified prior to or after the temporal scope of the conduct alleged in the warrant application. Such "date scoping" as it is called, is an easy way to identify digital files that could not be subject to the scope of the warrant.

Courts should also require the government to commit to a specific time frame within which it will identify and return all files that are not subject to seizure pursuant to the warrant. The government should not be able to hang on to documents for months, or even years, under the guise of determining what electronic files are responsive to the warrant. At the very least, there should be a rolling release of documents that are deemed non-responsive. To that end, courts should include in the language of the warrant that the government must delete all copies of seized digital data that do not fall within the scope of the warrant.

Finally, as in the BALCO case, courts should prohibit the investigative or prosecution team from performing any searches until the non-responsive data has been

segregated by a filter team, returned to the property owner, and all copies in the government's possession have been deleted.

The "plain view doctrine" question is substantially more difficult to address, and, because of size constraints, cannot be substantively discussed in this article. It will suffice to say that at least two other courts have reached opposing conclusions as to whether the "plain view doctrine" should apply in the unique circumstances of a digital search.[22] When faced with requests for digital search warrants, courts should consider making a determination prior to the execution of the search exactly what constitutes a discovery of evidence in "plain view." Once the warrant has been executed, and prior to any substantive search by the government, the court should allow all parties to participate in a dialogue about how seized digital data can be searched without the need to open or expose files that are not subject to the scope of the warrant. It is imperative that defense counsel be proactive about the scope and method of the search.

Congress has given the courts a useful tool in Rule 41 to help ensure warrants for digital evidence are executed in a manner that preserves the Fourth Amendment prohibition against general searches and continues to limit the "plain-view doctrine" to its traditional parameters. If courts are vigilant in setting out conditions for review of seized electronic data at the time a warrant is issued, the Fourth Amendment's

[22] *See United States v. Williams*, 592 F.3d 511, 521-22 (4th Cir. 2010); *see also United States v. Carey*, 172 F.3d 1268, 1275-76 (10th Cir. 1999).

particularity and specificity requirements can still be applied, and the prohibition on general searches can be effectively enforced.