©JRB | AdobeStock

Cybercrime and the Fourth Amendment

Cybercrime has become a major problem in the electronic age. Crimes ranging from fraud, to internet hacking, to identity theft, to possession, solicitation and distribution of child pornography and beyond are being committed on the internet. The prevalence of the internet in current crimes makes the use of cellphones, tablets, and computers the focus of new Fourth Amendment law developments. The law is evolving to deal with products used to commit cybercrimes. Many of the existing Fourth Amendment doctrines such as plain view, inevitable discovery, and exigent circumstances have special applications in these sorts of cases. A review of the development in the law related to cybercrime and the use of various products to commit such offenses is discussed here along with strategies to suppress illegally seized and used information from cyber-use products. This article outlines some of the details and considerations a practitioner should keep in mind when involved in Fourth Amendment litigation that includes digital evidence. The information here hopefully will give defense attorneys a foundation for their next cyber suppression motion.

Fourth Amendment Law In the Electronic Age

No matter what the crime or how serious the charges, the Fourth Amendment still applies to search and seizure.[1] The constitutional protections afforded by the Fourth Amendment related to cybercrimes are no different than a Fourth Amendment action on a car, a house or any other private possession, but the application of these protections is evolving because of the nature of digital storage devices.[2] Computers, cloud servers, tablets, watches, phones, and the like run everyday activities. Dependency on the gadget world has become the norm, and each cyber access object used to preserve private and personal information once kept in phone books, on paper, in drawers at home, or file cabinets at the office is now an item protected by the Fourth Amendment.[3]

Generally, the content of digitally preserved information is not easy to access by law enforcement because most people protect their information with passwords.[4] Just as with locked compartments, such actions present a unique layer of privacy that enhances the protection of the Fourth Amendment to those devices.[5] Because searches of things such as personal computers and cellphones create such an intrusion into a person's privacy, the Supreme Court has indicated that these searches should be treated differently.[6] Further, even when a search is permitted, it may not be possible. For example, while there is some software to sidestep password protections, as the FBI's attempt to gain access to the San Bernardino shooter's iPhone demonstrates, these password protections and

BY MARCIA G. SHEIN

encryptions are getting better and harder to crack.[7]

One of the unique issues presented is that the content contained in an electronic device is not apparent from a visual inspection of the device and the content may be concealed by encryptions and misnaming files and documents.[8] (There are now Apps for inscriptions.) Law enforcement cannot get a dog to alert to cyber information on a particular computer that may point to illegal activity — at least not yet. Perhaps one day probable cause to search without a warrant will arise through use of a robot dog or insertion of a device or matrix bug that can access information with or without a person's knowledge and determine whether the contents of a particular electronic item contains illegal activity. As farfetched as this may sound, it may not be too far in the distant electronic future.[9] Until then, however, the reality is that, in the majority of cases, the government over-seizes digital data.[10]

Safeguard to Prevent Over-seizure

Recognizing that digital searches often involve an over-seizure and end up capturing materials unrelated to the substance of the warrant, in order to protect an individual's right to privacy courts have begun to require certain safeguards and protocols when police conduct a search on digital devices pursuant to a warrant.[11] For example, in *In the Matter of the Search of Black iPhone 4,* the District Court for the District of Columbia explained:

> The bottom line is this: even though the cellphones are currently seized by the government, the government must still explain to the court what the basis for the probable cause is to search for each thing it intends to seize, and it must explain how it will deal with the issue of intermingled documents.[12]

The district court also presented the questions that the search protocols must answer:

> Will all of these devices be imaged? For how long will these images be stored? Will a dedicated computer forensics team perform the search based on specific criteria from the investigating officers of what they are looking for, or will the investigating officers be directly involved? What procedures will be used to avoid viewing material that is not within the scope of the warrant? If the government discovers unrelated incriminating evidence, will it return for a separate search and seizure warrant?"[13]

Likewise, in a concurring opinion joined by four other judges, Chief Judge Kozinski of the Ninth Circuit in *United States v. Comprehensive Drug Testing, Inc.*, provided a five-step process that the government should follow when applying for a search warrant of electronic data:

1. Magistrate judges should insist that the government waive reliance upon the plain view doctrine in digital evidence cases.

2. Segregation and redaction of electronic data must be done either by specialized personnel or an independent third party. If the segregation is to be done by government computer personnel, the government must agree in the warrant application that the computer personnel will not disclose to the investigators any information other than that which is the target of the warrant.

3. Warrants and subpoenas must disclose the actual risks of destruction of information as well as prior efforts to seize that information in other judicial fora.

4. The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents.

5. The government must destroy or, if the recipient may lawfully possess it, return nonresponsive data, keeping the issuing magistrate informed.[14]

This was not, however, adopted by the full court in its per curium decision.

What these cases demonstrate to the practitioner is the necessity of carefully examining the warrant to compare what officers seized and what officers viewed. As the National Association of Criminal Defense Lawyers (NACDL) has recognized, in addition to safeguards to prevent over-seizure, a requirement that the warrant disclose the actual risks that the information will be destroyed or concealed "would help the magistrate issue an appropriately limited warrant."[15] There may be several layers to a motion to suppress, particularly if other information is discovered on the device not included in the warrant that the government wants to use, whether incriminating or not.

Plain View in Electronic Searches

While the government is likely to argue plain view in support of anything it finds, it is important to keep in mind that this concept is arguably inapplicable to searches of computers and phones.[16] A search of a computer is inherently different than a search of a cabinet and, therefore, the plain view doctrine must evolve to address this reality.[17] Whether something is deemed in plain view on a computer or phone will depend on the crime being investigated and the authorization in the warrant.[18] For example, if the warrant is for child pornography files, the argument can be made that the government may only access those files that have names that implicate child pornography.[19] The government, however, will likely counter this argument by arguing that file names may be manipulated to conceal what is contained in the file.[20] This argument is analogous to the past when agents made every word a "drug word" in wire taps. There is a fight to be had here just as defense attorneys have done with so-called "drug words."

In *Comprehensive Drug Testing, Inc.,* the Ninth Circuit recognized the slippery slope that the government's plain view argument may present in electronic searches. The *en banc* court explained:

> Once a file is examined, however, the government may claim (as it did in this case) that its contents are in plain view and, if incriminating, the government can keep it. Authorization 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.

> Where 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.[21]

Does the warrant identify any sorting or filtering procedures for information that does not fall within the probable cause statement?

The three-judge panel and the *en banc* court were concerned with the government's conduct and the plain view argument it expounded. In fact, one judge asked, "Whatever happened to the Fourth Amendment? Was it ... repealed somehow?"[22] While not eliminating the possibility of a plain view argument entirely, the Ninth Circuit stated that the process of segregating data that is seizable must be vigilantly maintained in order to strike the right balance:

> We recognize the reality that over-seizing is an inherent part of the electronic search process and proceed on the assumption that, when it comes to the 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.[23]

It is precisely because of this slippery slope that courts have required search warrants for electronic searches to contain sufficient particularity as to what is to be searched.[24] As the Second Circuit noted in *United States v. Galpin*, the threat that the government will claim every file on a hard drive is in plain view once access is gained "demands a heightened sensitivity to the particularity requirement in the context of digital searches."[25] Likewise, the District of Kansas in *In re Application for Search Warrants for Info. Associated with Target Email Address* refused to issue a warrant that did not contain the requisite level of particularity. The court explained:

> The court finds the breadth of the information sought by the government's search warrant for either the fax or email account — including the content of every email or fax sent to or from the accounts — is best analogized to a warrant asking the post office to provide copies of all mail ever sent by or delivered to a certain address so that the government can open and read all the mail to find out whether it constitutes fruits, evidence or instrumentality of a crime. The Fourth Amendment would not allow such a warrant. The Fourth Amendment should therefore not permit a similarly overly broad warrant just because the information sought is electronic communications versus paper ones.[26]

Similarly, in *United States v. Bonner*, the Southern District of California implicitly rejected the government's attempt to claim plain view in an electronic search case involving a warrant to search for evidence that would show that the defendant "submitted false claims for business expenses and false claims for lost wages."[27] In reaching this conclusion, the district court explained that "[t]he forensic examination was overbroad, and not directed exclusively to identify data within the scope of the authorized search."[28]

As NACDL detailed in its 2014 report, *What's Old Is New Again: Retaining Fourth Amendment Projections in Warranted Digital Searches*, courts have taken four different approaches with regards to the plain view doctrine in electronic searches — apply it to electronic searches, require the discovery be inadvertent, use filter teams, or abandon the use of plain view entirely.[29] A practitioner who has lost the argument that plain view does not apply to electronic searches at all should look closely at the procedures followed to segregate irrelevant electronic materials and the authorization in the search warrant for actual materials that are associated with any alleged criminal conduct. If proper procedures were not specified or followed, or if the warrant was not properly tailored, or if the discovery was not inadvertent, the defense can mount a strong attack on the government's plain view argument.

Inevitable Discovery in Electronic Searches

Likewise, if the government attempts to claim inevitable discovery, this too can be rebuked. The government is required to return the electronic equipment when the search is finished and should be required to destroy any nonresponsive documents found.[30] Therefore, if the government is not on a fishing expedition and is only searching documents that fall within a carefully tailored warrant and is following the proper protocol, inevitable discovery will have no application.[31]

In applications for search warrants, courts are insisting that the government let the court know what will happen to data law enforcement seizes that is outside the scope of the warrant. For example, in *In re Search of Black iPhone* 4, the District Court for the District of Columbia directed as follows for data that is seized but is outside the scope of the warrant:

> The government must specify what will occur — although it is admonished that any response other than "the information will be returned or, if copies, destroyed" within a prompt period of time will likely find any revised application denied.[32]

Likewise, on another occasion, in *In re Search of Information Associated with the Facebook Account Identified by the Username Aaron.Alexis that Is Stored at Premises Controlled by Facebook,* the district court explained that "some safeguards must be put in place to prevent the government from collecting and keeping information indefinitely to which it has no right," and there may be secondary orders that "explicitly require that contents and

records of electronic communications that are not relevant to an investigation must be returned or destroyed and cannot be kept by the government."[33]

Accordingly, a practitioner facing a claim of inevitable discovery can argue against this claim by pointing out the fact that any nonresponsive data was to be immediately returned and destroyed and, therefore, no inevitable discovery would have occurred.

Jurisprudence relating to electronic searches also opens the door to getting information returned to the client as quickly as possible that concerns unrelated matters that is of a personal or professional nature. That is, courts have been concerned with and even rejected warrants when the warrant did not indicate "how the search would occur and how the government will avoid overseizure by avoiding keeping documents and other information outside the scope of [the warrant's attachments]."[34]

Search of Electronics Incident to Arrest and Exigent Circumstances

Although the government may try to claim a search incident to an arrest justified the search of an entire computer or phone, the U.S. Supreme Court has made clear that this argument will not succeed. Specifically, in *Riley v. California*, the Supreme Court explained that a search of a cellphone was not permitted as a search incident to a lawful arrest because "digital data stored on a cellphone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape" and because after the officer seizes the phone there is little chance of destruction of evidence.[35] With regard to the destruction of evidence, the Court rejected the government's argument that the phone could be encrypted or wiped by a third party after it is seized, explaining that it has "been given little reason to believe" that either problem is prevalent, and that officers can prevent remote wiping by turning the phone off or removing the battery.[36]

The Court did, however, leave the door open for exigent circumstances justifying a search. The Court explained:

> If "the police are truly confronted with a 'now or never' situation," — for example, circumstances suggesting that a defendant's phone will be the target of an imminent remote-wipe attempt — they may be able to rely on exigent circumstances to search the phone immediately.[37]
>
> . . .
>
> Such exigencies could include the need to prevent the imminent destruction of evidence in individual cases, to pursue a fleeing suspect, and to assist persons who are seriously injured or are threatened with imminent injury.[38]

The Court's specific description of the exigencies clearly implies that a general claim that evidence of the crime may be found on the phone will not prevail. The Court stated:

> The sources of potential pertinent information are virtually unlimited, so applying the *Gant* standard to cellphones would in effect give "police officers unbridled discretion to rummage at will among a person's private effects.[39]

When facing a claim of exigent circumstances, a practitioner should closely examine the facts to determine if any real exigency existed.[40] As *Riley* makes clear, the Court is protective of an individual's expectation of privacy in electronic devices, and a generic claim of exigency is vulnerable to a strong attack.

Third-Party Forensic Searches

Practitioners should also keep in mind that it can be argued that computer forensic search protocols and specialists should be in place to protect innocent information from being accessed. The Third Circuit noted in *In re Search of Odys Loox Plus Tablet* that it expects a detailed explanation of the search to be conducted:

> The law enforcement officer affiant must include details in his affidavit about how that computer forensics specialist intends to complete his search. The court expects to receive an overview that uses whatever technical terms are necessary to explain how the search will be done. No sophisticated search should occur without a detailed explanation of the methods that will be used, even if the explanation is a technical one, and no search protocol will be deemed adequate without such explanation.[41]

It has been pointed out, however, that there are "concerns that the use of a filter team could invite overbroad searches, which would lead to minimization of the invasion of privacy and Fourth Amendment interests after-the-fact.[42]

Just as in the privilege context, while some courts refer to third-party forensic teams or independent experts as desirable, other courts will permit those "filter teams" or "privilege teams" or "taint teams" to be part of the law enforcement agency.[43] It is hard to think of a situation in which an independent filter team would not be desirable and, therefore, in the rare instance when a practitioner is aware of a search before it is to take place, the practitioner should petition the court to require an independent filter team.

If the court denies the defense request for an independent filter team and the filter team will be part of the government's office, it is important to remember the following:

> (1) the members of the taint team must not have been and may not be involved in any way in the investigation or prosecution of the defendants subject to indictment — presently or in the future; (2) the taint team members are prohibited from (a) disclosing at any time to the investigation or prosecution team the search terms submitted by the defendants, and (b) disclosing to the investigation or prosecution team any emails or the information contained in any emails, subject to review until the taint team process is complete and in compliance with its terms; (3) the defendants must have an opportunity to review the results of the taint team's work and to contest any privilege determinations made by the taint team before a superior court judge, if necessary, prior to any emails being disclosed to the investigation or prosecution team; and (4) the members of the taint team must agree to the terms of the order in writing.[44]

In the more common occurrence of learning about the search after it has taken place, counsel should argue, when appropriate, that the lack of an inde-

pendent filter team has tainted the search in an effort to encourage the use of independent filter teams in the future.[45] If an attack on the filter team cannot be mounted, it is important to examine the warrant and the procedures followed to determine if the government was instructed to follow certain procedures to avoid over-seizure and if it followed those procedures. As the Western District of Washington's decision denying a warrant application in the *Edward Cunnius* case illustrates, courts are increasingly skeptical of warrants that do not provide for safeguards against over-seizures that turn into general fishing expeditions. Recognizing that over-seizures are an inherent part of electronic searches, the court in *Edward Cunnius* explained:

> A balance must be struck between the government's investigatory interests and the right of individuals to be free from unreasonable searches and seizures. … Almost every hard drive encountered by law enforcement will contain records that have nothing to do with the investigation. To maintain the balance between the government's investigatory interests and the Fourth Amendment, the court is ready to grant the government's instant application on the conditions set forth in this opinion. But the government, much like it did in the *CDT* line of cases, does not seek to perform the search with constitutional safeguards, i.e., a filter team or foreswearing reliance on the plain view doctrine. The government's warrant application therefore does not pass constitutional muster.[46]

Likewise, in *Bonner*, the Southern District of California found that a defendant's Fourth Amendment rights had been violated because "[a] fair reading of the warrant did not include authorization to seize any item in defendant's residence with a date and time stamp or authorization to seize photographic images marked with a date and time stamp." The court also determined that "the forensic analysis employed search protocol not directed to identify data within the scope of the warrant and violated the defendant's rights under the Fourth Amendment."[47]

As these cases demonstrate, courts are aware that searches of electronics may result in an over-seizure, but they are wary of allowing it to become a general fishing expedition. Therefore, it is important to make sure that the warrant contained proper procedures to limit the search and that those procedures were followed.

Good Faith in Searching Electronic Devices

One way courts are upholding searches of electronic data is by referencing the good faith exception. For example, the District of Oregon in *United States v. Taylor* upheld a search of a cellphone based on the good faith exception without even examining whether the warrant had the required specificity. In refusing to even examine the warrant, the district court explained that "no reasonably well-trained officer would have known that the search was illegal in light of all the circumstances[.]"[48] The court continued, finding that because the warrant authorized the search of the cellphone (not just the seizure), the good faith and plain view exception applied "despite the lack of protocols to limit the scope of the search" given the state of the law governing searches of digital devices.[49]

While the good faith exception provides a significant hurdle, it is not insurmountable. As the Eastern District of Virginia recognized in *United States v. Shanklin*, the warrant cannot be "so lacking in indicia of probable cause as to render an officer's belief in its existence unreasonable."[50] In that case, the detective relied on "conclussory and speculative assertions" and the district court determined that no reasonable officer would be able to "infer through normal inferences that electronic devices owned by child abusers in general or the defendant specifically contain evidence related to the criminal activity being investigated." The court said there was no evidence that the defendant had a history of "using multimedia to engage in sexual battery, abduction or child exploitation."[51]

Further, as the Southern District of California recognized in *Bonner*, the protocols used to conduct the search must be reasonable in light of what is authorized in the warrant. As that court explained in finding that the officer's conduct was not reasonable,

> The forensic examination was overbroad, and not directed exclusively to identify data within the scope of the authorized search. The Court concludes that suppression of any evidence extracted from all 35 items of electronic media, including four computers, 20 external hard drives, eight floppy disks, two flash drives, and a smartphone is the proper remedy in this case.[52]

The foregoing cases demonstrate that the clearer the requirement for specificity in warrant applications for searches of electronic devices becomes and the more exact the required protocols become to protect from over-seizure, the less an officer will be able to rely on the good faith exception to the exclusionary rule. Further, if the warrant contains proper protocols and limits and the officer ignores them, the good faith exception will fail.[53]

Practice Pointers

It is likely that most practitioners will face a case that involves an electronic search. If counsel is lucky enough to be aware of the warrant application before the seizure and search has taken place, she should make sure that the warrant is specific as to what is to be searched and includes safeguards necessary to ensure that there is not an over-seizure, such as a third-party forensic team.[54] In fact, counsel should argue that the warrant contain "pre-search mandates when necessary to ensure particularity of places to be searched or things to be seized[,]" "provisions for the destruction or return of digital information as appropriate[,]" and a provision that the "[a]gents must retain records of the particularities of the digital search, which should be shared with the defendants[.]"[55]

If counsel only learns of the search after it has occurred and has decided to file a suppression motion, counsel may want a bifurcated hearing. In the first part of this hearing, counsel should examine whether the warrant was valid and whether it was specific enough so as not to be a general fishing expedition through a person's personal information.[56] That is, Fourth Amendment litigation that involves a search of digital data should involve a close examination of the warrant to ensure that it involves a narrowly tailored description of what was to be searched for to exclude an unreasonably high risk of over-seizure. The warrant also needs to be examined to determine if it contains adequate cyber-specific protocols for searching

digital information. As discussed above, courts have indicated that if the warrant is not sufficiently tailored to cyber-information as is necessary to limit the possibility of an over-seizure of sensitive digital information, then the warrant is susceptible to a Fourth Amendment attack.

In the second part of the bifurcated hearing, counsel should examine the protections the government used to ensure that it did not seize or search data or documents that were beyond the scope of the warrant.[57] If the government did not use the protections directed by the warrant, or did not independently use adequate protections, the search is susceptible to a Fourth Amendment attack and a practitioner should argue for suppression.[58] A practitioner can also argue that if the search uncovered information not covered under the warrant, the plain view and inevitable discovery doctrines do not apply and all evidence seized after this discovery should be suppressed if law enforcement did not obtain a second warrant.[59]

Courts are concerned with the personal intrusion that searches of computers and phones and servers will entail because of the vast amounts of personal information contained on each device. Thus, there is a need for an independent viewing and separation of incriminating versus other information not subject to search or seizure.

Practitioners should continue to push for protections to ensure that the government does not use a search of a computer as a fishing expedition to find evidence of an unknown nature about unknown crimes. Moreover, practitioners should continue to clarify the law regarding the necessary specificity and procedures so that the government may no longer rely on the good faith exception to justify an overexpansive and intrusive search.

Special thanks to attorney Elizabeth Brandenburg and Leigh Schrope for their research assistance.

Notes

1. In fact, the Fourth Amendment applies even if there is no crime involved as long as the government is the actor. *See, e.g., Hudson v. City of Rivera*, 982 F. Supp. 2d 1318, 1339 (S.D. Fla. 2014) ("The Fourth Amendment protects individuals from unreasonable searches conducted by the government. It is well settled that the Fourth Amendment's protection "extends beyond the sphere of criminal investigations,"' 'without regard to whether the government actor is investigating crime or performing another function.'" (quoting *City of Ontario v. Quon,* 560 U.S. 746, 130 S. Ct. 2619, 2627 (2010))).

2. *See, e.g., Riley v. California*, 134 S. Ct. 2473 (2014) (under the Fourth Amendment, officer safety and prevention of destruction of evidence did not justify warrantless searches of cellphone data); *United States v. Warshak*, 631 F.3d 266, 283-86 (6th Cir. 2010) (Fourth Amendment protections apply to emails on a third-party server); *Doe v. Prosecutor, Marion County*, 566 F. Supp. 2d 862, 879 (S.D. Ind. 2008) ("The voluntary use of the mails or telephone lines does not mean the user gives up her rights under the Fourth Amendment, and the same reasoning applies to computer and internet use."); *In re Application for Search Warrants for Info. Associated with Target Email Address*, 2012 WL 4383917, at *5 (D. Kan. Sept. 21, 2012) ("an individual has a reasonable expectation of privacy in emails or faxes stored with, sent to, or received through an electronic communications service provider").

3. *See* note 2, *supra.*

4. *See, e.g., United States v. Griswold*, 2011 WL 7473466, at *12 (W.D.N.Y. June 2, 2011) ("the use of special forensic software to override the password protection is no less offensive to the Fourth Amendment than the use of a bolt cutter to break open the locked file cabinet. At the very least, a reasonably well-trained police officer would know that further inquiry was required before relying on the consent of the third party to search a password-protected and locked computer belonging to another.").

5. *See, e.g., id.* at *6 ("When it comes to the search of personal computers, the use of passwords implicates the same privacy concerns as the search of a locked container. 'Password-protected computers or files have been likened to private, locked compartments, so that where officers know that the person offering consent lacks the key, or password, they cannot reasonably conclude that the person in question has the authority to consent to a search of any *locked* areas.'").

6. *See Riley*, 134 S. Ct. at 2491 ("A phone not only contains in digital form many sensitive records previously found in the home, it also contains a broad array of private information never found in a home in any form — unless the phone is." "To further complicate the scope of the privacy interests at stake, the data a user views on many modern cellphones may not in fact be stored on the device itself. Treating a cellphone as a container whose contents may be searched incident to an arrest is a bit strained as an initial matter. But the analogy crumbles entirely when a cellphone is used to access data located elsewhere, at the tap of a screen.") (internal citations omitted).

7. *See, e.g., United States v. Andrus*, 483 F.3d 711, 723 (10th Cir. 2007) (McCay, J., dissenting) ("The fact remains that EnCase's ability to bypass security measures is well known to law enforcement."). *But see* http://abcnews.go.com/US/judge-orders-apple-unlock-san-bernardino-shooters-phone/story?id=36989123.

8. *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1168 (9th Cir. 2010) ("In essence, the government explains, computer files can be disguised in any number of ingenious ways, the simplest of which is to give files a misleading name … or a false extension. … In addition, the data might be erased or hidden; there might be booby traps that 'destroy or alter data if certain procedures are not scrupulously followed[.]'").

9. Law enforcement's ability to evolve their techniques with the times is evidenced by the canine in Connecticut that has been trained to sniff the chemicals commonly used in USB storage devices, which often contain illegal child pornography. *See* http://www.bloomberg.com/news/2014-09-23/a-police-dog-for-the-digital-age-she-can-smell-the-usb-drive-you-re-hiding.html.

10. *See Comprehensive Drug Testing, Inc.,* 621 F.3d at 1176 ([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.").

11. *See, e.g., United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013) ("Once the government has obtained authorization to search the hard drive, the government may claim that the contents of every file it chose to open were in plain view and, therefore, admissible even if they implicate the defendant in a crime not contemplated by the warrant. There is, thus, 'a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant.' This threat demands a heightened sensitivity to the particularity requirement in the context of digital searches.") (internal citations omitted); *In re Application for Search Warrants for Info. Associated with Target Email Address*, 2012 WL 4383917, at *5 (D. Kan. Sept. 21, 2012) (in denying application for search warrant, the District of Kansas explained: "Most troubling is that these sections of the warrants fail to limit the universe of electronic communications and information to be turned over to the government to the specific crimes being investigated. Second, even if the court were to allow a warrant with a broad authorization for the content of all email and fax communications without a nexus to the specific crimes being investigated, the warrants would still not pass constitutional muster. They fail to set out any limits on the government's review of the potentially large amount of electronic communications and information obtained from

the electronic communications service providers. The warrants also [do] not identify any sorting or filtering procedures for electronic communications and information that are not relevant and do not fall within the scope of the government's probable cause statement, or that contain attorney-client privileged information."); *United States v. Barthelman*, 2013 WL 3946084, at *11 (D. Kan. July 31, 2013) (finding warrant that sought "all emails, pictures, friends and groups. There was no limitation on these requests to Yahoo and Apple" was not sufficiently particular); *In re Applications for Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts*, 2013 WL 4647554, at *9 (D. Kan. Aug. 27, 2013) ("Even had the government shown probable cause for the providers to disclose the content of all email communications and information connected to the target accounts, the court is concerned by the lack of any limits on the government's review of the information, such as filtering procedures for emails and information that do not fall within the scope of probable cause or contain attorney-client privileged communications."); *In re Search of Information Associated with the Facebook Account Identified by the Username Aaron.Alexis that is Stored at Premises Controlled by Facebook,* 21 F. Supp. 3d 1, 7 (D.D.C. Nov. 26, 2013) ("This court will insist, however, that some safeguards must be put in place to prevent the government from collecting and keeping indefinitely information to which it has no right. … This court is satisfied — for the time being — that it can lessen any potential Fourth Amendment violation by enforcing minimization procedures on the government."); *In re Search of Black iPhone 4*, 2014 WL 1045812, *4 (D.D.C. Mar. 11, 2014) ("The bottom line is this: even though the cellphones are currently seized by the government, the government must still explain to the court what the basis for probable cause is to search for each thing it intends to seize, and it must explain how it will deal with the issue of intermingled documents.").

12. *In re Search of Black iPhone 4*, 2014 WL 1045812 at *4.

13. *Id.*

14. *Comprehensive Drug Testing, Inc.,* 621 F.3d at 1180. *See also* NACDL's report, Steven R. Morrison, What's Old Is New Again: Retaining Fourth Amendment Protections in Warranted Digital Searches (2014) [hereinafter Morrison, Fourth Amendment Protections in Warranted Digital Searches], *available at* http://www.nacdl.org/reports.

15. Morrison, Fourth Amendment Protections in Warranted Digital Searches, *supra* note 14, at 14.

16. *See* note 14, *supra*. *See also United States v. Bonner,* 2013 WL 3829404, at *19 (S.D. Cal. July 23, 2013); *In re Search of Odys Loox Plus Tablet, Serial Number 4707213703415 in Custody of United States Postal Inspection Serv., 1400 New York Ave NW, Washington D.C. 14-265 (JMF),* 2014 WL 1063996, *5 (D.D.C. Mar. 20, 2014) ("the government needs to provide a sophisticated technical overview of how it plans to conduct the search" to assure the court that it was not authorizing a "general, exploratory rummaging in a person's belongings"). *But see United States v. Williams*, 592 F.3d 511, 522 (4th Cir. 2010) ("Once it is accepted that a computer search must, by implication, authorize at least a cursory review of each file on the computer, then the criteria for applying the plain-view exception are readily satisfied.").

17. *United States v. Carey*, 172 F.3d 1268, 1275 (10th Cir. 1999) ("Relying on analogies to closed containers or file cabinets may lead courts to 'oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern computer storage.'").

18. *See, e.g., Id.* ("Under this approach, law enforcement must engage in the intermediate step of sorting various types of documents and then only search the ones specified in a warrant."); *United States v. Will*, 2015 WL 3822599 (N.D. W.Va. June 19, 2015) ("Unlike *Williams,* the connection between the designated offense of battery and child pornography is more attenuated" but finding that the plain view doctrine still applied). *But see Williams*, note 16, *supra.*

19. *Carey*, 172 F.3d at 1275 ("With the computers and data in their custody, law enforcement officers can generally employ several methods to avoid searching files of the type not identified in the warrant: observing files types and titles listed on the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory.").

20. *Williams*, 592 F.3d at 522 ("To be effective, such a search could not be limited to reviewing only the files' designation or labeling, because the designation or labeling of files on a computer can easily be manipulated to hide their substance. Surely, the owner of a computer, who is engaged in criminal conduct on that computer, will not label his files to indicate their criminality.").

21. *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1176.

22. *Id.* at 1177.

23. *Id.*

24. *Galpin*, 720 F.3d at 447.

25. *Id.*

26. *In re Application for Search Warrants for Info. Associated with Target Email Address*, 2012 WL 4383917 at *9.

27. *Bonner,* 2013 WL 3829404 at *19.

28. *Id.*

29. Morrison, Fourth Amendment Protections in Warranted Digital Searches, at 10-11.

30. *In re Search of Black iPhone 4*, 2014 WL 1045812 at *5; *In re Search of Information Associated with the Facebook Account Identified by the Username Aaron.Alexis that is Stored at Premises Controlled by Facebook,* 21 F. Supp. 3d at 7.

31. The inevitable discovery doctrine still applies if the incriminating evidence is also located in another location that the government is permitted to search. *See, e.g., United States v. Cyr,* 2015 WL 4773099, at *6 (D. Vt. Aug. 12, 2015) ("The government would have inevitably obtained a search warrant to search the hard drives for child pornography after reviewing the Ann Clancy Facebook records and finding that Ann Clancy had asked K.P. to produce child pornography. Therefore, the court declines to put the government in a worse position than it would have otherwise occupied if the hard drives had not been searched.").

32. *In re Search of Black iPhone 4*, 2014 WL 1045812 at *5.

33. *In re Search of Information Associated with the Facebook Account Identified by the Username Aaron.Alexis that is Stored at Premises Controlled by Facebook,* 21 F. Supp. 3d at 7

34. *In re Search of Odys Loox Plus Tablet, Serial Number 4707213703415 in Custody of United States Postal Inspection Serv., 1400 New York Ave NW, Washington D.C. 14-265 (JMF),* 2014 WL 1063996 at *4. *See also In re Search of Black iPhone 4*, 2014 WL 1045812 at *5 ("The related question to the overbreadth issue — and one that was touched on in *Tamura* and in this court's opinions —

(Continued on page 62)

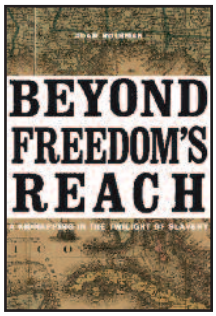
About the Author

Marcia G. Shein, who served as president of the Georgia Association of Criminal Defense Lawyers in 2013, is a life member of NACDL. She represents clients nationally in white collar, drug and cybercrime cases including trial, sentencing, appellate, and post-conviction litigation.

Marcia G. Shein
Shein & Brandenburg
Federal Criminal Law Center
2392 North Decatur Road
Decatur, GA 30033
404-633-3797
E-MAIL marcia@msheinlaw.com

Beyond Freedom's Reach
A Kidnapping in the Twilight of Slavery

By Adam Rothman
Harvard University Press (2015)
Reviewed by Maureen L. Rowland



Lincoln freed the slaves, right? Not exactly. The Emancipation Proclamation, effective Jan. 1, 1863, only applied to those states that took up arms against the Union. It did not apply to slaveholding states that remained loyal to the Union. And, it was an Executive Order, not an Act of Congress. Lincoln issued it while the war still raged, so he dedicated Federal troops to the enforcement of the Proclamation. The Emancipation Proclamation did apply to Louisiana. This is where the story begins.

In May 1862, Union forces captured New Orleans and held it for the rest of the war. At this time our heroine, Rose Herera, was married to a free man of color and had four young children. James De Hart and his wife, Mary De Hart, owned Rose and her children. Apparently, seeing the writing on the wall, the De Harts made arrangements to move to Cuba — a very slave-friendly place. Many of the Confederates went to Cuba where they could sell their slaves. James De Hart left for Cuba in the fall of 1862. Mary De Hart did not leave for Cuba until Jan. 15, 1863. In between their departures, the president issued the Emancipation Proclamation. So, when Mary De Hart took Rose Herera's children to Cuba, she was taking free children, that were not her own, and for whom she did not have permission, away from their mother. Kidnapping. Unbelievably, not everyone saw it this way.

So begins the odyssey of Rose Herera to get her children back from captivity in Cuba. Her journey began in 1863 with the able advocacy of Thomas Jefferson Durant. It appears he handled the case to its conclusion *pro bono.* One of the first acts of the Union when it took over New Orleans was to set up a military court. It was not clear, however, the extent of its jurisdiction. Contemporaneously, there existed a fully functioning local court predominately biased toward the slaveholders. Obviously, there was tension. And, unfortunately, the military court was weakened by changing leadership that had varying philosophies. Rose was dissatisfied with the justice she was receiving in New Orleans, so the next step was to appeal to the authorities in Washington, D.C. The relief she sought was an intervention in Cuba seeking their help in returning the children to their mother. Finally, in 1866, mother and children were reunited.

The persistence of Rose Herera and her lawyer finally paid off. It is easy to see why Adam Rothman chose her story as the subject for a book. He remarks that the horrors of slavery can best be told through the stories of individuals.

The subject matter of *Beyond Freedom's Reach* is fascinating. However, readers may find themselves distracted from the story by the author's constant reference to other events, other characters, and discussing events out of chronological order. Readers may find it difficult to follow. Lawyers may want more of the legal wrangling: motions, arguments, and rulings. Some people prefer a more emotional text, but others may prefer this style. ■

About the Reviewer

Maureen L. Rowland is an Assistant Public Defender, Felony Trial Division, in Baltimore City, Maryland.

Cybercrime and the Fourth Amendment

(Continued from page 44)

is what will occur with data that is seized by the government and is outside the scope of the warrant. … In *Tamura,* the government acted improperly by not returning documents that were seized but "not described in the warrant." … Will such information be returned, destroyed, or kept indefinitely? The government must specify what will occur — although it is admonished that any response other than "the information will be returned or, if copies, destroyed" within a prompt period of time will likely find any revised application denied.").

35. *Riley*, 134 S. Ct. at 2486.

36. *Id.*

37. *Id.* at 2488.

38. *Id.* at 2494.

39. *Id.* at 2492.

40. *See, e.g.*, MORRISON, FOURTH AMENDMENT PROTECTIONS IN WARRANTED DIGITAL SEARCHES, at 40.

41. *In re Search of Odys Loox Plus Tablet, Serial Number 4707213703415 in Custody of United States Postal Inspection Serv., 1400 New York Ave NW, Washington D.C. 14-265 (JMF),* 2014 WL 1063996. *See also Comprehensive Drug Testing, Inc.,* 621 F.3d at 1180.

42. MORRISON, FOURTH AMENDMENT PROTECTIONS IN WARRANTED DIGITAL SEARCHES, at 13.

43. *United States v. Bonner,* 2013 WL 3829404 (agents conducted forensic exam). *See also United States v. Taylor*, 764 F. Supp. 2d 230, 234 (D. Maine 2011) (discussing a filter agent and explained that a "number of cases have permitted its use. At the same time, there is a healthy skepticism about the reliability of a filter agent or Chinese or ethical wall within a prosecutor's office. … Courts exhibit particular concern over use of filter agents or taint teams in searches of lawyers' offices, where privileged materials of many clients could be compromised. There, judges have sometimes required alternatives such as appointment of a special master, a wholly independent third party."); *In re Search of Black iPhone 4*, 2014 WL 1045812 at *5 ("Will a dedicated forensics team perform the search based on specific criteria from the investigating officers of what they are looking for, or will the investigating officers be directly involved?").

44. *Preventive Med. Assoc., Inc. v. Commonwealth*, 992 N.E. 2d 257, 272 (Mass. 2013).

45. MORRISON, FOURTH AMENDMENT PROTECTIONS IN WARRANTED DIGITAL SEARCHES, at 21.

46. *In re Application for a Search Warrant to Seize and Search Electronic Devices from Edward Cunnius*, 770 F. Supp. 2d 1138. 1151 (W.D. Wash. 2014).

47. *Bonner,* 2013 WL 3829404 at *19.

48. *United States v. Taylor*, 2016 WL 633890, at *3 (D. Ore. Feb. 17, 2016) (internal quotations omitted).

49. *Id.*

50. *United States v. Shanklin*, 2013 WL 6019216, at *9 (E.D. Va. Nov. 13, 2013).

51. *Id.*

52. *Bonner,* 2013 WL 3829404, at *19.

53. *United States v. Metter*, 860 F. Supp. 2d 205, 216 (E.D.N.Y. May 17, 2012) (finding that government's actions indicated a lack of good faith and "[t]he government's own conduct and statements indicate that it had no intention of fulfilling its obligations as promised in the search warrants. Nor has the government presented any evidence or arguments to the effect that it failed to fulfill this obligation due to limited resources, such as it has argued in other cases").

54. *See* notes 11-29, 42-53, *supra.*

55. MORRISON, FOURTH AMENDMENT PROTECTIONS IN WARRANTED DIGITAL SEARCHES, at 16-22.

56. *See* notes 11-29, *supra.*

57. *See* notes 41-47, *supra.*

58. MORRISON, FOURTH AMENDMENT PROTECTIONS IN WARRANTED DIGITAL SEARCHES, at 19.

59. *Id.* at 20-21; *see also* notes 17-34, *supra.* ■