Published in The State of Criminal Justice 2015.

CHAPTER 6

DIGITAL PRIVACY AND E-DISCOVERY IN GOVERNMENT INVESTIGATIONS AND CRIMINAL LITIGATION

Justin P. Murphy and Louisa K. Marion

A growing avalanche of electronically stored information ("ESI") continues to present challenges and overwhelming costs for clients, prosecutors, and defense attorneys in criminal litigation. Paradigms developed to curb ESI discovery abuses in civil litigation are often ineffective in the criminal system due to the one-sided nature of ESI burdens, demands in government investigations and criminal matters, and the absence of cost-effective methods sanctioned by courts to resolve criminal discovery disputes. Yet neither courts nor the current criminal procedural rules provide clear guidance on parties' ESI obligations or the tools to combat such abuses. This chapter examines the challenges faced by the criminal bar relating to ESI, particularly in the contexts of subpoena compliance, Constitutional issues, post-indictment discovery, and social media and the Internet.

I. INVESTIGATIONS: THE DUTY TO PRESERVE ESI

When does a duty to preserve ESI that may be relevant to a government investigation arise? Service of a subpoena or another government demand is an obvious trigger. However, the duty can arise prior to that point. In civil litigation, the basic rule is fairly well-developed: "Whenever litigation is reasonably anticipated, threatened or pending against an organization, that organization has a duty to preserve relevant information."[1] In general the same principle applies to the criminal arena: The duty to preserve potentially relevant information arises when a government investigation is contemplated, threatened, pending, or can be reasonably anticipated. The obstruction-of-justice provisions in the Sarbanes-Oxley Act of 2002, enacted in reaction to Arthur Andersen LLP's conduct during the Enron case, mimic this standard, making it clear that a government investigation need not have commenced and a subpoena need not have been issued for the duty to preserve to arise.[2]

The consequences of failing to preserve potentially relevant ESI may be far reaching and more extensive in criminal cases. As an initial matter, a failure to preserve relevant ESI, or at least construct a record of thorough, good-faith efforts to preserve, can influence the views of prosecutors and agents at the outset of a case. This may shape judgments about culpability and cooperation, which in turn may impact charging decisions and plea negotiations. In addition, failing to preserve potentially relevant information may negatively impact calculations under the Sentencing Guidelines by increasing a defendant's culpability score.[3]

---

[1] Sedona Conference Commentary on Legal Holds, Sept. 2010; Zubulake v. UBS Warburg, 229 F.R.D. 422 (S.D.N.Y. 2004).
[2] *See* 18 U.S.C. § 1519 (punishing document destruction in "contemplation" of a federal investigation).
[3] *See* U.S.S.G. § 8C2.5.

Importantly, preservation failures can also expose a defendant to additional investigation for obstruction of justice.[4] If the government encounters efforts to destroy evidence, it may assume bad intent unless good faith can otherwise be demonstrated. Where bad intent can be established, any number of obstruction-of-justice statutes can be brought to bear. Because obstruction is often easier to prove than the underlying crime, which may involve complicated issues ill-suited to a jury trial, some prosecutors may favor the use of these statutes.[5]

The government also has a duty to preserve ESI, and its failure to do so also may present significant consequences. For example, in *United States v. Suarez*,[6] the government failed to preserve numerous text messages exchanged between a key cooperating witness and FBI agents involved in a public corruption investigation.[7] As a result of the FBI's failure to preserve the text messages, the court, relying on civil e-discovery sanctions principles and case law, issued an adverse inference instruction that permitted the jury to infer that the missing text messages were relevant and favorable to the defendants.[8] The court declined, however, to suppress other text messages introduced by the government, absent a showing that the government had deleted the messages in bad faith.[9] The jury nevertheless acquitted the defendant, who argued that the missing text messages were important.[10]

The Ninth Circuit went further in *United States v. Sivilla*,[11] vacating a conviction on drug charges after the district court declined to issue a remedial jury instruction absent a finding that the government had destroyed physical evidence in bad faith. The Ninth Circuit directed that "[b]ad faith is the wrong legal standard for a remedial jury instruction."[12] Rather, "[c]ourts must balance the quality of the Government's conduct against the degree of prejudice to the accused, where the government bears the burden of justifying its conduct and the accused of demonstrating prejudice."[13] Balancing these interests, the panel found that the government was negligent when it failed to take "any affirmative action" to preserve the evidence in question, which left the defendant without any means to present his only defense.[14] Finding that the prejudice to the defendant

---

[4] *See generally* United States v. Kurt Mix, No. 2:12-cr-00171 (E.D. La.) (convicting ex-BP engineer for the deletion of text messages to obstruct federal investigation of company's 2010 oil spill in the Gulf of Mexico).

[5] *But see* United States v. Katakis, Cr. No. 2:11-511 (WBS) (E.D. Cal. May 9, 2014) (obstruction of justice set aside where government failed to demonstrate that defendant intended to destroy records to obstruction or impede an investigation. "Although the jury heard extensive and complicated evidence regarding the … charge and the government resorted to every theory possible, none of the evidence was sufficient for the jury to find beyond a reasonable doubt that Katakis knowingly destroyed or concealed the emails with the intent to obstruct an FBI investigation that he knew of or contemplated.").

[6] United States v. Suarez, No. 09-932 (JLL), 2010 WL 4226524 (D.N.J. Oct. 21, 2010).

[7] *Id.* at *1.

[8] *Id.* at *8.

[9] *Id.* at *7.

[10] *See also* Freeman v. State, No. 2012-KM-00192-SCT (Miss. May 30, 2013) (reversing conviction where government failed to preserve video evidence of event).

[11] 714 F.3d 1168 (9th Cir. 2013).

[12] *Id.* at 1173.

[13] *Id.* (citing United States v. Loud Hawk, 628 F.2d 1139 (9th Cir. 1979) (Kennedy, J., concurring), and asserting that Judge Kennedy's concurring opinion was controlling on this issue) (internal quotation omitted).

[14] The only other evidence available to the defendant's expert witness—whose testimony was critical to proving the defendant's primary defense—was "grainy and indecipherable photographs" upon which no expert could rely. 714 F.3d at 1174.

outweighed the prosecutor's negligence, the panel held that the defendant was entitled to a remedial jury instruction and remanded the case for a new trial.[15]

While spoliation sanctions are increasingly common in civil litigation, it is uncommon for such conduct to be charged as criminal obstruction of justice.[16] But, more recently, the Department of Justice ("DOJ") has started doing just that. For example, in a trade secrets theft case, DOJ charged the defendant, Kolon Industries, Inc., with obstruction of justice, in addition to conspiracy and trade-secret-theft counts, as a result of conduct undertaken in a private civil case. The obstruction charge was based on the intentional deletion of documents by Kolon employees shortly after they found out about a related civil suit filed by DuPont, in an apparent effort to deprive DuPont of relevant evidence. Both Kolon and the five individuals involved were charged with violating 18 U.S.C. § 1512(c)(1) and (2), which imposes severe criminal penalties for document destruction aimed at obstructing a "federal proceeding."

The prospect of criminal charges for spoliation in civil litigation raises the stakes for civil litigants, particularly where a parallel criminal investigation is a possibility because obstruction counts can easily be tacked on to substantive criminal charges. Even the harshest of civil sanctions can pale in comparison to the criminal penalties a corporate litigant could face for obstruction and the significant jail time to which individuals could be exposed.

II. INVESTIGATIONS: SEARCH & SEIZURE OF ESI WITH A WARRANT

The distinctive challenges presented by ESI create problems in the context of search warrants. Specifically, the modern day phenomenon of immense amounts of intermingled data has collided with the Fourth Amendment's search and seizure strictures. On one hand, computers can store virtually unlimited data, some of which can be hidden or disguised to frustrate a government search; given this, searches pursuant to lawful warrants need to be somewhat invasive. On the other hand, this invasiveness must be reconciled with the Fourth Amendment's particularity requirement in identifying "the place to be searched and the . . . things to be seized."

Debates surface from the government "over-seizing" ESI and, by doing so, creating a risk that an ESI warrant will be a general warrant and that the plain view exception to the Fourth Amendment will be rendered meaningless. Courts continue to question how much they should control the government's conduct; whether computers, smartphones, and other devices deserve special treatment in digital evidence cases; and whether these devices are analogous to more traditional personal papers, effects, and/or document containers (e.g., filing cabinets).

---

[15] Although the panel remanded the case for a new trial, it rejected defendant's argument that government spoliation violated his due process rights and warranted complete dismissal of the indictment. The panel concluded that bad faith—or a showing that the exculpatory nature of spoliated evidence was apparent to the government—remained necessary for complete dismissal under Supreme Court precedent in *Arizona v. Youngblood*, 488 U.S. 51 (1988). 714 F.3d at 1172.

[16] Courts have also referred cases to U.S. Attorneys for criminal investigation of electronic discovery abuses, including by third parties. *See* Gutman v. Klein, No. 03-1570, 2008 WL 5084182 at *2 (E.D.N.Y. Dec. 2, 2008); Bryant v. Gardner, 584 F. Supp. 2d 951 (N.D. Ill. 2008) (court ordering defendant to show cause why issue of false declaration should not be referred to U.S. Attorney's office, rather than a direct referral). *See also* SonoMedica, Inc. v. Mohler, No. 1:08-cv-230 (GBL) 2009 WL 3271507 (E.D. Va. July 28, 2009).

The Ninth Circuit's Standards

Two decisions by the Ninth Circuit in the *Comprehensive Drug Testing* matter provided some of the most interesting, in-depth and specific analyses of the Fourth Amendment and its application to ESI. In August 2009, the Ninth Circuit *en banc* issued new and enhanced guidelines for warrants seeking ESI.[17] The court confronted the ESI search debate head-on, stating in the opening paragraph of its opinion that the case was about "the procedures and safeguards that federal courts must observe in issuing and administering search warrants and subpoenas for electronically stored information."

The court rejected the government's argument that data beyond that specified in the warrant was in "plain view." Such an approach, the court held, would "make a mockery" of procedures designed to "maintain the privacy of materials that are intermingled with seizable materials, and to avoid turning a limited search for particular information into a general search of office file systems and computer databases."[18] The court determined that "greater vigilance on the part of judicial officers" is required due to "the reality that . . . over-seizing is an inherent part of the electronic search process . . . ."[19] In an attempt to ensure such vigilance, the court established the following explicit requirements:

> Magistrates should insist that the government waive reliance upon the plain view doctrine in digital evidence cases.
>
> Segregation of non-responsive materials must be done by specialized personnel who are walled off from the case agents, or an independent third party.
>
> Warrants must disclose the actual risks of destruction of information, as well as prior efforts to seize that information in other judicial fora.
>
> 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.
>
> The government must destroy or return non-responsive data, keeping the issuing magistrate informed about when it has done so and what it has kept.[20]

In September 2010, the court *en banc* issued an amended opinion, demoting the above requirements to suggested guidance when dealing with the over-seizure of ESI.[21] In support of the court's change in position, it opined that the five guidelines are hardly revolutionary, and are essentially the Ninth Circuit's solution to the problem of necessary over-seizing of evidence outlined in its prior decision in *United States v. Tamura.*[22] Adhering to its ruling in *Tamura*, the Ninth Circuit applied a two-step process. First, a

---

[17] *See* United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989 (9th Cir. 2009) (finding third parties in contempt for violation of court's orders, including spoliation of ESI, and referring case to U.S. Attorney's office for criminal investigation).
[18] *Id.* at 998.
[19] *Id.* at 1006.
[20] *Id.*
[21] *See* United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1177-80, 1183 (9th Cir. 2010).
[22] *Id.* at 1180 (citing *Tamura*, 694 F.2d 591 (9th Cir. 1982)).

court should consider whether large scale removal of materials can be justified, which it may where officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site.[23] Second, a Magistrate Judge should approve conditions and limitations on further search of those documents. The "essential safeguard required is that wholesale removal must be monitored by the judgment of a neutral, detached magistrate."[24] The court further explained that "*Tamura* has provided a workable framework for almost three decades, and might well have sufficed in this case had its teachings been followed. We have updated *Tamura* to apply to the daunting realities of electronic searches."[25]

Although the amended opinion demoted the five explicit restrictions to guidelines, Chief Judge Kozinski noted in his concurring opinion that these guidelines offer "the government a safe harbor, while protecting the people's right to privacy and property in their papers and effects. District and magistrate judges must exercise their independent judgment in every case, but heeding this guidance will significantly increase the likelihood that the searches and seizures of electronic storage that they authorize will be deemed reasonable and lawful."[26]

The *Comprehensive Drug Testing* decisions represented one of the first serious attempts by a federal appellate court to fashion specific, comprehensive guidance for lower courts confronted with the inevitable clash between the strictures of the Fourth Amendment and increasingly common broad seizures of intermingled ESI. As the court observed: "[t]his pressing need of law enforcement for broad authorization to examine electronic records . . . creates a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant."[27] However, as described below, other courts continue to grapple with these same issues.

Other Courts' Treatment of the Particularity Requirement and the Plain View Doctrine

Other Circuits have weighed in on the tension between the particularity requirement under the Fourth Amendment and the plain view doctrine. For example, the Second Circuit, acknowledging the concerns raised by the Ninth Circuit in *Comprehensive Drug Testing*, has also recognized that a "heightened sensitivity to the particularity requirement in the context of digital searches" is necessary.[28] In affirming the district court's determination that a warrant application failed to establish probable cause, the panel noted that:

> Where, as here, the property to be searched is a computer hard drive, the particularity requirement assumes even greater importance. As numerous courts and commentators have observed, advances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of

[23] 621 F.3d at 1169, 1171.
[24] *Id.* (quoting *Tamura*, 694 F.2d at 596).
[25] 621 F.3d at 1177.
[26] *Id.* at 1178; *see also* In Re Application for Search Warrant, 2012 VT 102 (holding that magistrate judges have discretion to restrict warrants to protect privacy and rejecting blanket prohibitions on ex ante search warrant instructions).
[27] *Id.* at 1176.
[28] United States v. Galpin, No. 11-cr-4808 at *16 (2d Cir. June 25, 2013).

> private information it may contain…The potential for privacy violations occasioned by an unbridled, exploratory search of a hard drive is enormous. This threat is compounded by the nature of digital storage. Where a warrant authorizes the search of a residence, the physical dimensions of the evidence sought will naturally impose limitations on where an officer may pry; an officer could not properly look for a stolen flat-screen television by rummaging through the suspect's medicine cabinet, nor search for false tax documents by viewing the suspect's home video collection. Such limitations are largely absent in the digital realm, where the size or other outwardly visible characteristics of a file may disclose nothing about its content.[29]

Another example is *United States v. Richards*, [30] where the Sixth Circuit acknowledged that, "[o]n one hand, it is clear that because criminals can – and often do – hide, mislabel, or manipulate files to conceal criminal activity, a broad, expansive search of the hard drive may be required. . . . On the other hand . . . granting the government a *carte blanche* to search *every* file on the hard drive impermissibly transforms a limited search into a general one."[31]

The Sixth Circuit applied "the Fourth Amendment's bedrock principle of reasonableness on a case-by-case basis," [32] and found that an FBI warrant was not overbroad, even though it made no distinction made between seizing servers maintained by third parties that contained information belonging to others, and servers exclusively maintained by the defendant.[33] Notably, Judge Moore, in her concurring opinion, expressed concern with the majority's ruling, explaining that it "would authorize the government to invade the privacy of any number of unidentified individuals or companies without any probable cause, just because they may, without their knowledge, share server space with suspected criminals.[34] Judge Moore highlighted that the FBI agents had made no showing that they had probable cause to believe that every directory on a particular server was accessible to the operators of the child pornography website under investigation.[35] Judge Moore noted that "[w]hen the government has probable cause to search for drugs in a specific apartment, we have never held that the existence of a landlord with keys to every other apartment in the building creates probable cause to search every apartment."[36]

The Third Circuit's opinion in *United States v. Stabile* also addresses the issue of "over-seizure" of evidence under the plain view doctrine.[37] In *Stabile*, agents went to the defendant's home to question him regarding allegations that he was involved in counterfeiting and other financial crimes.[38] The defendant was not home when the agents arrived, but his wife was, and consented to a search of the entire house for evidence of financial crimes.[39] The agents seized several computer hard-drives from the home, and discovered child pornography on the hard-drives.[40] While the court in *Stabile* declined to

---

[29] *Id.* at *15-16.
[30] United States v. Richards, 659 F.3d 527 (6th Cir. 2011).
[31] *Id.* at 538.
[32] *Id.*
[33] *Id.* at 541.
[34] *Id.* at 552 (Moore, C.J., concurring).
[35] *Id.* at 558 (Moore, C.J., concurring).
[36] *Id.*
[37] United States v. Stabile, 633 F.3d 219 (3d Cir. 2011).
[38] *Id.* at 224.
[39] *Id.* at 225.
[40] *Id.*

follow the Ninth Circuit's suggestion in *Comprehensive Drug Testing*[41] to "forswear reliance on the plain view doctrine" whenever the government seeks a warrant to examine a computer hard drive, *Stabile* did hold that "the exact confines of the [plain view] doctrine will vary from case to case in a common-sense, fact-intensive manner. What is permissible in one situation may not always be permissible in another."[42] The court supported the general framework articulated in *Comprehensive Drug Testing*, "agree[ing] that '[a] measured approach based on the facts of a particular case is especially warranted in the case of computer-related technology, which is constantly and quickly evolving.'"[43]

Few federal appeals courts have disagreed with the *Comprehensive Drug Testing* rationale. In *United States v. Williams*,[44] the Fourth Circuit held that a search warrant implicitly authorized police officers to open each file on a computer to view its contents, at least on a cursory basis, to determine whether the file fell within the scope of the warrant's authorization.[45] There, the court reasoned that, in order to be effective, a search cannot be limited to reviewing only file designations or labeling, as such things can easily be manipulated.[46] The court further explained that "[o]nce 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."[47]

Applications for search warrants are, of course, *ex parte* proceedings and more often than not the government's requests are granted. But judicial skepticism of the need for dragnet seizures of ESI seems to be increasing. Several federal judges have issued decisions holding that unrestricted ESI warrants violate the Fourth Amendment where the government only has probable cause to seize and search *some* of data associated with a particular e-mail account, for example.[48] These courts argue that the government must tailor the scope of its ESI warrants to meet the particularized probable cause justification.

---

[41] *Comprehensive Drug Testing*, 621 F.3d at 1178 (Kozinski, CJ, concurring).
[42] *Id.* at 241.
[43] *Id.* at 241, n.16 (quoting *Comprehensive Drug Testing*, 621 F.3d at 1184). Similarly, the Seventh Circuit's decision in *United States v. Mann* acknowledged the value of the guidelines articulated in *Comprehensive Drug Testing.* 592 F.3d 779, 785 (7th Cir. 2010). In *Mann*, the court found that "the more considered approach 'would be to allow the contours of the plain view doctrine to develop incrementally through the normal course of fact-based case adjudication.'" *Mann*, like *Stabile*, found that "jettisoning the plain view doctrine entirely in digital evidence cases is an efficient but overbroad approach." *Id.*
[44] United States v. Williams, 592 F.3d 511, 515-17 (4th Cir. 2010).
[45] *Id.* at 521-22.
[46] *Id.* at 22.
[47] *Id.*
[48] In the Matter of the Search of Information Associated with [redacted] @mac.com that is Stored at Premises Controlled by Apple, Inc., 2014 WL 1377793 (D.D.C. April 7, 2014) ("The government wants to seize the target's entire e-mail account, search through it for relevant data, and then keep indefinitely the irrelevant data that is outside the scope of the warrant. There is no question that the Renewed Application violates the Fourth Amendment, and this Court *cannot* issue it"), *rev'd by* In the Matter of the Search of Information Associated with [redacted] @mac.com that is Stored at Premises Controlled by Apple, Inc., (D.D.C. Aug. 8, 2014); In re Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts, 2013 WL 4647554 (D. Kan. Aug. 27, 2013) (In finding warrant applications overbroad, court noted it was "Most troubling that … 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… "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 Court finds the breadth of the information sought by the government's search warrant for the target accounts—including the content of every email 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."); In re [Redacted]@gmail.com, Case No. 14-MJ-70655 (PSG) (N.D. Cal. May 9, 2014) ("Search warrant applications like

Limits on the Search of Data Seized Pursuant to a Warrant

Courts have held that the Fourth Amendment is violated when the government indefinitely holds seized computer files that are not responsive to a search warrant. In *United States v. Ganias*, the Army secured a search warrant in connection with an investigation of the defendant's business.[49] It did not seize computers but, instead made forensic mirror images of the hard drives, "including files beyond the scope of the warrant, such as files containing Ganias's personal financial records."[50] The following year, based on evidence derived from paper records it also seized, the IRS began investigating the defendant and was provided copies of the imaged hard drives. Both agencies extracted files that were within the scope of the warrant but did not purge or delete non-responsive files. In 2005, the investigation expanded into possible tax violations and in 2006, two-and-a-half years after the forensic images had been made, the government secured a warrant to search for the defendant's personal financial records. "Because Ganias had altered the original files shortly after the 2003 warrant, the evidence obtained in 2006 would not have existed but for the Government's retention of those images."[51] The defendant was indicted for tax evasion. He moved to suppress the evidence derived from the 2006 search. The motion was denied and the defendant was convicted.

The Second Circuit vacated the conviction, noting that

> [i]f the 2003 warrant authorized the Government to retain all the data on Ganias's computers on the off-chance the information would become relevant to a subsequent criminal investigation, it would be the equivalent of a general warrant. The Government's retention of copies of Ganias's personal computer records for two-and-a-half years deprived him of exclusive control over those files for an unreasonable amount of time. This combination of circumstances enabled the Government to possess indefinitely personal

---

the one presently before the court bring this role into view. The tools of modern crime have evolved beyond a ski mask and a burlap sack. Like the rest of society, the modern criminal uses computers and mobile devices to do his 'work.' As such, evidence of crime and evidence of daily life unrelated to crime are often intertwined in software files, folders and databases. Even with a warrant issued under Fed. R. Crim. P. 41, this often leaves the government in the unenviable position of having to spend many, many hours of sifting through data by brute force or complex and cumbersome sorting algorithms. Where the computers at issue are at a suspect's home, courts have recognized the impracticality of reviewing the data on site by approving a "seize first, search second" methodology… But what about those computers that are not at a suspect's home, but at a third-party cloud provider like Google? Following a standard format used by the Department of Justice, the government draws no distinction and commonly seeks approval for the same seize first, search second methodology whether the data of interest is local or remote. For example, the supporting affidavit here is divided into three sections in which the first section gives background and the reasons sufficient to establish probable cause. In a second section, labeled 'Attachment A,' the property to be searched is identified as a particular email account stored on the premises of Google's headquarters. No date restriction is included. The third section, labeled 'Attachment B,' includes two subsections. Subsection I describes particular information within the account to be comes from the government. No defendant or defense counsel is present. Indeed, no defendant yet exists, as no case has yet been filed. There are no hearings, no witnesses, no briefs and no debate. Instead, a magistrate judge is left to predict what would or would not be reasonable in executing the warrant without any hard, ripe facts. This is hardly a recipe for success.").

But see In the Matter of a Warrant for All Content and Other Info. Associated with the Email Account xxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc., No. 14 Mag. 309 (S.D.N.Y. July 18, 2014) (granting a broad search warrant and concluding that the government must be permitted to seize and analyze entire sets of ESI as significant evidence may be hidden within a haystack of irrelevant data).

[49] United States v. Ganias, 755 F.3d 125 (2d Cir. 2014).

[50] *Id.* at 128.

[51] *Id*. at 130.

> records of Ganias that were beyond the scope of the warrant while it looked for other evidence to give it probable cause to search the files. This was a meaningful interference with Ganias's possessory rights in those files and constituted a seizure within the meaning of the Fourth Amendment.[52]

The court concluded that "without some independent basis for its retention of those documents in the interim, the Government clearly violated Ganias' Fourth Amendment rights by retaining the files for a prolonged period of time and then using them in a future criminal investigation."[53]

In addition, courts have also found that the government must take at least some action on seized data within a reasonable amount of time. In *United States v. Metter*, the government seized large amounts of data pursuant to a valid search warrant but then failed to do anything with the seized images for over 15 months.[54] While the search warrant itself was proper, the process afterwards was not: The Fourth Amendment requires the government to complete its review within a "reasonable" period of time. The court noted that delays of several months have been found to be reasonable but that there was no available guidance as to when a delay becomes presumptively unreasonable. The court found:

> The parties have not provided the Court with any authority, nor has the Court found any, indicating that the government may seize and image electronic data and then retain that data with no plans whatsoever to begin review of that data to determine whether any irrelevant, personal information was improperly seized. The government's blatant disregard for its responsibility in this case is unacceptable and unreasonable.[55]

The court suppressed the electronic evidence seized from the defendant, noting:

> The Court has not reached this conclusion lightly. However, the Court cannot, in the interest of justice and fairness, permit the government to ignore its obligations. Otherwise, the Fourth Amendment would lose all force and meaning in the digital era and citizens will have no recourse as to the unlawful seizure of information that falls outside the scope of a search warrant and its subsequent dissemination.[56]

The government is on notice that it must do something with lawfully seized evidence in a reasonable amount of time. At least one court has determined that "reasonable" falls somewhere between a few and 15 months.

---

[52] *Id.* at 137.
[53] *Id.*
[54] United States v. Metter, No. 10–CR–600 (DLI) (E.D.N.Y May 17, 2012).
[55] *Id.*
[56] *Id.*

III. INVESTIGATIONS: WARRANTLESS SEARCHES & SEIZURES OF ESI

Warrantless Searches of Cellular Telephones

As of 2011, there were more mobile phones than people in the United States.[57] This proliferation of phones—and particularly smart phones—fed a key issue taken up by the Supreme Court in 2014. In *Riley v. California*,[58] the Court examined the Fourth Amendment protections that extend to smartphones in searches incident to a lawful arrest. In its groundbreaking opinion, the Court examines the unique challenges posed by modern technologies and gives its clearest directive on electronic privacy to date: In no uncertain terms, the Court instruct law enforcement to "get a warrant" before searching a suspect's mobile device (or, as the Court characterized it, "mini-computer").[59] *Riley v. California* reflects an important evolution of the Supreme Court's thinking about modern digital technology—from *City of Ontario v. Quon*,[60] where the Court was hesitant to tread into digital privacy, to the adoption in *Riley v. California* of a modernist view of not only the role of technology in today's society, but also of evolving expectations of privacy in the modern digital age.

In *Riley v. California*, the U.S. Supreme Court considered the different rules of law drawn by the California Fourth District Court of Appeal in *People v. Riley*[61] and by the First Circuit in *United States v. Wurie*.[62] In *Wurie*, law enforcement officers searched the defendant's cell phone incident to his arrest on suspicion that he was dealing drugs. While at the police station, Wurie's phone received repeated incoming calls from a number identified as "my house." After reviewing the phone's call log and retrieving the phone number, officers obtained a search warrant for the property associated with that number. A search of the property turned up drugs, drug paraphernalia, and firearms, and Wurie was charged with drug possession and distribution and firearms charges. Wurie moved to suppress what he alleged were the fruits of an unlawful cell phone search. The Court denied the motion and Wurie was convicted. On review, the First Circuit panel reversed, eschewing a fact-specific approach in favor of a bright-line rule: "[T]he search-incident-to-arrest exception does not authorize the warrantless search of data on a cell phone seized from an arrestee's person." The panel held that the evidence should have been suppressed and vacated Wurie's conviction.

The search in *People v. Riley* was much broader. Police stopped Riley for driving with expired registration tags. After an inventory search of Riley's vehicle revealed two handguns, police arrested Riley and searched him incident to the arrest. The officers found gang-related materials on his person and seized and searched Riley's smartphone, which also revealed information connecting Riley to the same gang. A few hours later, a detective specializing in gangs further examined the contents of Riley's phone. The officer found text ("presumably in text messages or a contacts list") that appeared to relate to "Crip Killers," videos seemingly connecting Riley to a gang, and a picture of Riley in front of a car that officers suspected had been involved in a recent shooting. Riley was charged in connection

---

[57] Number of cellphones exceeds U.S. population: CTIA trade group, Cecilia Kang, *The Washington Post*, October 11, 2011.
[58] Riley v. California¸ 134 S.Ct. 2473 (2014)
[59] *Id.* at 2495.
[60] 560 U.S. 746 (2010).
[61] People v. Riley, No. D059840, 2013 WL 475242 (Cal. Ct. App. Feb. 8, 2013) (unpublished opinion), *review denied* (May 1, 2013), *cert. granted in part*, No. 13-132, 2013 WL 3938997 (Jan. 17, 2014).
[62] United States v. Wurie, 728 F.3d 1 (1st Cir. 2013), *cert granted* Jan. 17, 2014.

with the shooting and moved to suppress all evidence obtained from his cell phone. The lower court denied the motion and Riley was convicted on all charges. The California Court of Appeal affirmed, and the California Supreme Court denied review.

The omnipresence of cell phone use in today's society is a key theme underlying the Supreme Court's *Riley v. California* decision. Chief Justice Roberts noted at the outset that "modern cell phones . . . are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude that they were an important feature of human anatomy."[63] When the court aligned the pervasiveness of cell phone use with smartphones' computer-like storage capacity, it was left with the inescapable conclusion that "minicomputer" searches are *different* than physical searches. This far-reaching acknowledgment concedes that we are indeed in a new digital age.

In fact, Chief Justice Roberts categorically rejected the government's argument that cell phones are "materially indistinguishable" from physical containers, noting that "[t]hat is like saying a ride on a horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together."[64] In support of the Court's conclusion that digital devices are different than physical containers, Chief Justice Roberts highlighted key differences between digital devices and physical containers:

- Modern cell phones have immense storage capacity, and are minimally limited by physical constraints. While individuals cannot "lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read [—] if they did, they would have to drag behind them a trunk of the sort held to require a search warrant[]"— they could easily do so on their mobile device; and the "gulf between physical practicability and digital capacity will only continue to widen in the future."[65]

- Modern cell phones can provide distinctive insight into an individual's past. Where previously an individual might have carried a photo or two in his wallet, today the sum of his private life can be reconstructed through the thousands of digital photographs (labeled with dates, locations and descriptions) and other data that might predate the phone.[66]

Chief Justice Roberts also acknowledged significant qualitative differences. Cell phones contain:

- Enormous volumes and types of information, and could as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps or newspapers[67]; as such, they present a digital record of nearly every aspect of their owner's life, from the intimate to the ordinary.[68]

---

[63] *Riley v. California*, 134 S. Ct. at 2484.
[64] *Id.* at 2488.
[65] *Id.* at 2489.
[66] *Id.*
[67] *Id.*
[68] *Id.* at 2490.

- Internet search histories, which reveal an individual's private interests and concerns.[69]

- Data that reveal where a person has been and when they were there.[70]

- Mobile application software ("apps"), which offer a range of tools for managing detailed information about all aspects of a person's life and "together can form a revealing montage of the user's life."[71]

In light of these key differences, Chief Justice Roberts found the balance between intrusions upon individual privacy and government interests weighed differently in the digital context. Under *U.S. v. Robinson*,[72] the government interest in preventing potential harm to officers and destruction of evidence—present in all custodial arrests—outweighed a privacy interest diminished by the fact of arrest. In the digital context, however, the Court found no comparable risk of harm to officers or data, but a significant privacy interest: Since cell phones "place vast quantities of personal information literally in the hands of individuals, [a] search of the information on a cell phone bears little resemblance to the type of brief physical search considered in *Robinson*."[73] As such, the Court found that officers must generally secure a warrant before searching for data on cell phones.

The Court also analyzed the officer safety concerns recognized in *Chimel v. California*.[74] As the Court explained, digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or aid in an arrestee's escape. In fact, once a phone is secure and other *physical* threats are removed, the data will not endanger anyone. The reason for that is simple, as the Court noted: When you search a phone, you know exactly what you will find—*data*.[75] Addressing the government's arguments that a search of a cell phone would alert officers that *accomplices* of the arrestee were headed to the scene of the arrest, Chief Justice Roberts reminded the government that *Chimel* focused on the *arrestee* and whether the *arrestee* might grab a weapon and use it against an officer. The Court concluded that the "interest in protecting officer safety does not justify dispensing with the warrant requirement across the board."[76] Chief Justice Roberts also addressed *Chimel*'s second rationale: preventing the destruction of evidence. He concluded that, once law enforcement officers have secured a cell phone, the danger that the arrestee could destroy any data from the phone is eliminated. With regard to potential dangers of remote wiping or remote encryption of data, the Court noted that officers could turn off the cell phone, remove its battery, or place the device in a Faraday Bag, which isolates the device from radio waves.[77]

Although groundbreaking, the Court's holding was not absolute: The "exigencies of situation [might] make the needs of law enforcement so compelling that a warrantless search is objectively reasonable under the Fourth Amendment."[78] The Court provided

---

[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] 414 U.S. 218 (1973).
[73] *Riley*, 134 S. Ct. at 2485.
[74] 395 U.S. 752 (1969).
[75] *Riley*, 134 S. Ct. at 2485.
[76] *Id.* at 2486.
[77] *Id.* at 2487.
[78] *Id.* at 2494.

examples of such exigent circumstances, including the need to prevent imminent destruction of evidence in individual cases or to assist persons seriously injured or threatened with imminent injury, among others.

One important element of the decision is the underlying assumption that individuals have a reasonable expectation of privacy in the data on their cell phones. This continues a shift in the Supreme Court, previously addressed by Justice Sotomayor in her concurrence in *United States v. Jones* (discussed more fully below). There, Justice Sotomayor cautioned of the privacy implications of lengthy GPS surveillance: "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[79] Now, with *Riley v. California*, those privacy concerns are adopted by the full Court, at least as it relates to cell phones searched incident to arrest.

Warrantless Collection of Real-Time and Historic Geolocational Information

Both before and in the wake of *Riley v. California*, courts have struggled to define the bounds of the Fourth Amendment as applied to technologies that track, trace, and record geolocational information—information that in the aggregate can create a comprehensive picture of an individual's movements, the individuals with whom one associates, the religious, cultural, or political institutions he visits, and so on. While the Supreme Court has held that attaching a global positioning system ("GPS") unit to a criminal suspect's car constitutes a "search" requiring a showing of probable cause,[80] it has remained silent on other key questions regarding geolocational privacy, including whether and when such GPS searches require a warrant, whether the Fourth Amendment ever protects geolocational (and other) information conveyed to third parties, and whether any (or different) protections apply to real-time versus historical geolocational information. Lower courts have struggled to fill this void, resulting in a patchwork of jurisprudence ripe for Supreme Court review and/or legislative guidance.[81]

GPS Tracking Devices

In its only treatment of geolocational privacy to date, the Supreme Court addressed in *United States v. Jones* whether the warrantless use of a GPS tracking device attached to a suspect's vehicle to monitor his movements on public streets violated the Fourth Amendment.[82] The underlying case[83] involved two nightclub owners in the District of Columbia under investigation for narcotics violations.[84] During the investigation, officers attached a GPS device to the defendant's vehicle without a warrant,[85] which tracked his movements 24 hours a day for a month.[86] The D.C. Circuit found that this round-the-clock

[79] *See* United States v. Jones, 132 S. Ct. 945, 956 (2012).
[80] *See id*.
[81] A number of pending legislative proposals seek to provide clarity on privacy protections for geolocational information. *See, e.g.*, H.R. 1312 (Geolocational Privacy Act); H.R. 983 (Online Communications and Geolocation Protection Act); S. 639 (GPS Act).
[82] United States v. Jones, 132 S. Ct. 945 (2012).
[83] United States v. Maynard, 615 F.3d 544, 559 (D.C. Cir. 2010).
[84] *Id.* at 549.
[85] *Id.* at 558–59.
[86] *Id.*

warrantless surveillance violated the Fourth Amendment by "reveal[ing] more about a person than does [surveillance of] any individual trip viewed in isolation."[87]

The Supreme Court affirmed, but on narrower grounds. Writing for the majority, Justice Scalia found the installation of the GPS monitoring device to be a search because the government had trespassed upon the defendant's car—i.e., the government "physically occupied private property for the purpose of obtaining information." Although the majority noted that its "cases suggest that [extensive] visual observation is constitutionally permissible," it nevertheless hinted that "achieving the same result through electronic means, without an accompanying trespass, [may be] an unconstitutional invasion of privacy[.]"[88]

Justice Alito—in a concurrence joined by Justices Ginsburg, Breyer, and Kagan—would have gone further. Justice Alito advocated for a different test, arguing that the Court should have analyzed whether GPS monitoring intrudes on an expectation of privacy that society recognizes as reasonable. Under this test, he would have found that long-term monitoring by a GPS device necessitates a warrant: While "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable . . . [,] the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[89] Noting that "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period," Justice Alito would have found four weeks of monitoring to be a search.[90]

Finally, while joining in the majority opinion, Justice Sotomayor authored a groundbreaking concurrence signaling that she may be willing to adopt a much broader interpretation of privacy rights in the digital age. Justice Sotomayor concluded that even short-term warrantless GPS surveillance of a suspect moving on public streets could intrude on the suspect's constitutionally protected privacy. She asserted that, in determining whether such an invasion occurred, she "would [have] ask[ed] whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on,"[91] and questioned whether an individual in the digital age surrenders his expectation of privacy in information voluntarily disclosed to third parties (e.g., cellular providers).[92] Taken together, and as will be discussed further below, Justices Sotomayor's and Justice Alito's concurrences called into question the soundness of many of the precepts underlying Fourth Amendment jurisprudence and reasonable expectations of privacy in the digital age, and laid the foundation for many of the questions the Court grappled with in *Riley v. California* (discussed above).

---

[87] *Id.* at 559, 562. *But see* United States v. Sparks, 750 F. Supp. 2d 384, 392–93 (D. Mass. 2010) (court rejecting the defendant's reliance on *Maynard* and describing the "aggregate travels" test as "vague and unworkable"); *see also* United States v. Pineda-Moreno, 591 F.3d 1212, 1214–15 (9th Cir. 2010) (warrantless GPS tracking of the defendant did not violate the Fourth Amendment because the defendant could not claim a reasonable expectation of privacy in his driveway, even if a portion of the driveway was located within the curtilage of the home).
[88] 132 S. Ct. at 954.
[89] *Id.* at 964 (Alito, J. concurring).
[90] *Id.*
[91] *Id.* at 956 (Sotomayor, J. concurring).
[92] *Id.* at 957.

Although *Jones* found that attaching a GPS device to an individual's private property constitutes a Fourth Amendment search by law enforcement, and although the concurrences were revolutionary in many respects, the *Jones* majority nevertheless did not address certain key questions. For example, the majority did not address whether a GPS search is necessarily unreasonable absent a warrant, or whether GPS tracking absent a physical intrusion into the defendant's property is nevertheless a search.

Two lower courts have helpfully addressed the warrant question. In *United States v. Katzin*,[93] in a 2013 opinion later vacated for rehearing *en banc*,[94] a panel of the Third Circuit delved deeper into the question of whether police placement of a "slap-on" GPS unit on a defendant's car required a warrant.[95] The Court explained that "[i]t remains a cardinal principle that searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions."[96] After analyzing numerous such exceptions (e.g., *Terry* stops, the automobile exception, and "special needs" beyond a general law enforcement interest), the court concluded that none permitted warrantless GPS tracking of a burglary suspect for two days, and held that "the police must obtain a warrant prior to a GPS search."[97] Although the *en banc* court did not address (after vacating the panel opinion) whether the slap-on GPS device was an unreasonable search, it nevertheless "caution[ed] that, after *Jones,* law enforcement should carefully consider that a warrant may be required when engaging in such installation and surveillance."[98]

The Wisconsin Supreme Court likewise concluded that a warrant is required for a GPS search in *State v. Brereton.*[99] There, a defendant moved to suppress geolocation information from a GPS tracker attached to his car pursuant to a warrant. While declining to suppress the evidence, the Wisconsin Supreme Court provided helpful instruction on the warrant question, explaining:

> Although the Court's majority opinion in *Jones* discussed the Fourth Amendment violation in terms of the government's trespass upon an individual's property, warrantless GPS tracking would constitute a search 'even in the absence of a trespass, [because] a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.' The privacy interest at issue in *Jones*, and in this case, where the government has utilized [defendant's] property to apply GPS technology to monitor his movements, is government usurpation of an individual's property 'for the purpose of conducting surveillance on him, thereby invading privacy interests long afforded, and undoubtedly entitled to, Fourth Amendment protection.'[100]

---

[93] 732 F.3d 187 (3d Cir. 2013), *vacated by* United States v. Katzin, No. 12-2548, Order Granting Re-Hearing En Banc, 2013 WL 7033666 (Dec. 12, 2013).
[94] *See id*.
[95] 732 F.3d 187 (3d Cir. 2013).
[96] *Id.* at 197.
[97] *Id.* at 191.
[98] United States v. Katzin, 769 F.3d 163 (3d Cir. 2014) (en banc) (finding that the good faith exception to the exclusionary rule saved the GPS evidence from suppression).
[99] *State v. Brereton*, 2013 WL 440512, No. 2010AP1366–CR (Wis. Feb. 6, 2013).
[100] *Id.* at *8 (internal citation omitted).

The court concluded "that the decision to install a GPS device on [the defendant's] car required officers to obtain a warrant because the use of a GPS constituted a search that extended beyond the scope of the automobile exception for warrantless searches."[101]

Finally, by relying on a trespass theory rather analyzing the question in terms of reasonable expectations of privacy, the Supreme Court has left unanswered the question of whether GPS tracking without any physical intrusion into an individual's property is a search. New technologies increasingly permit law enforcement to capture comprehensive location information emitted on public streets without any such physical intrusion. The ACLU has reported, for example, that police broadly use "stingray" devices (also known as "cell site simulators" and "IMSI catchers"), which prompt users' cell phones to disclose the device's identifying and location information; moreover, the stingrays collect this information indiscriminately from all in the area.[102] The ACLU likewise has asserted in pending litigation that law enforcement uses stingrays to track suspects without a warrant, and has sought to keep secret both its use of such devices and the process it requires before such use.[103]

Cell Site Tracking and Other "Business Records" Collection

Despite the gaps left by the *Jones* majority, the concurrences in *Jones* and the Supreme Court's unanimous and forward-looking opinion in *Riley v. California* signal that the Court is poised to—or at least open to—reexamining certain precepts of Fourth Amendment jurisprudence in the digital age. The most obvious such precept is the third-party doctrine established by *Smith v. Maryland*,[104] according to which an individual has no reasonable expectation of privacy in business record information voluntarily transmitted to a third party. In a modern era in which every aspect of our lives is "voluntarily" transmitted to and recorded by third parties—from our location information (through location-based Google Maps, cell phone towers, our cars, or our miscellaneous "check-ins"), to our Cloud-stored emails, Fitbit-recorded exercise regimens, and lists of Facebook "friends"—the characterization of such disclosures as "voluntary" and the surrender of all expectations of privacy in such information makes less and less sense.

Justice Sotomayor was the first on the Court to recognize this concern explicitly, in her concurrence in *Jones*. She explained:

> [It] may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service

---

[101] *Id*. at *10.
[102] *See* Stingray tracking devices, Am. Civil Liberties Union, https://www.aclu.org/node/37337 (last visited Feb. 5, 2015).
[103] *See* Plaintiff's Verified Emergency Petition for Writ of Mandamus, Am. Civil Liberties Union of Florida v. City of Saratoga, No. 2014-CA-3248-NC (Circuit Court of the Twelfth Judicial Circuit of Florida, Sarasota County, Florida), *removed by*, American Civil Liberties Union of Florida, Inc. et al v. City of Sarasota, No. 8:14cv1606 (M.D. Fla. 2014); *see also* Kim Zetter, *U.S. Marshals Seize Cops' Spying Records to Keep Them From the ACLU*, WIRED, June 3, 2014, http://www.wired.com/2014/06/feds-seize-stingray-documents/.
[104] 99 S.Ct. 2577 (1979).

> providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, as Justice ALITO notes [in his *Jones* concurrence], some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable,". . . and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[105]

Although the Court in *Riley v. California* took care to note that its decision was limited to the context of a search incident to arrest and was *not* a broader consideration of Fourth Amendment privacy in the digital age,[106] it nevertheless recognized and found persuasive some of these same concerns. First, the Court recognized the pervasiveness of cell phone ownership and use, citing a poll showing that "nearly three-quarters of smart phone users report being within five feet of their phones most of the time" and that 12% of users admit that they use their phones in the shower.[107] Second, the Court noted that "[d]ata on a cell phone can . . . reveal where a person has been" through which law enforcement "can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building"[108]—a fact the Court found justified treating cell phones differently than traditional "containers" in a search incident to arrest. Finally, although the Court did not address the third party doctrine explicitly, it was clearly troubled that a search of a cell phone incident to arrest could provide a portal to content stored in the Cloud[109]—content that traditionally, under the third-party doctrine, would have no Fourth Amendment protection since it was voluntarily conveyed to a third party cloud provider.[110] The Court's concern about the pervasive use of technologies that collect and convey to third parties comprehensive location and content data suggests that it may be willing to reconsider the logic of the third party doctrine in the digital context.[111]

Until that sea change occurs, lower courts remain constrained by the third-party doctrine. The numerous courts to have taken up the question of whether a warrant is required for the government to obtain, for example, cell site location information and other geolocational information from third-party providers have almost uniformly found that such data is not accorded Fourth Amendment protection.[112]

---

[105] *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

[106] 134 S.Ct. at 2489 n.1 ("Because the United States and California agree that these cases involve *searches* incident to arrest, these cases do not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances.").

[107] 134 S.Ct. at 2490.

[108] *Id*. (citing Justice Sotomayor's concurrence in *Jones*).

[109] *Id.* at 2491.

[110] *Id*.

[111] *But see* United States v. Guerrero, 768 F.3d 351, 360-61 (5th Cir. 2014) (speculating that "[i]t may be that the 'technology is different' rationale that led the *Riley* Court to treat an arrestee's cell phone differently from his wallet will one day lead the Court to treat historical cell site data in the possession of a cellphone provider differently from a pen register in the possession of a pay phone operator," but citing battling commentary on whether the Supreme Court is likely to overrule the third-party doctrine).

[112] *See, e.g.*, United States v. Rogers, No. 13-cr-952, 2014 WL 5152543, at *4 (N.D. Ill. Oct. 9, 2014) (individual users have no reasonable expectation of privacy in historic electronic location records, which "fit squarely into the

In 2013, for example, the Fifth Circuit held in *In re Application of the United States of America for Historical Cell Site Data* that a warrant is not required for the government to obtain cell site information from cellular providers.[113] There, the government had filed applications under the Stored Communications Act ("SCA") (18 U.S.C. §§ 2701-2712) for an order compelling disclosure of 60 days' worth of historical cell site data from several cell phones. Assessing whether the government's failure to obtain a warrant for the cell site information provided violated the cell user's Fourth Amendment rights, the Fifth Circuit focused its analysis on three primary issues: 1) *who* had collected the cell site information, 2) for what ends, and 3) whether, in using the cell phone, the user had voluntarily transmitted his location information to his provider.

The court found no Fourth Amendment violation under *Smith v. Maryland*, since the cell phone user had no reasonable expectation of privacy in business record information voluntarily transmitted to his cellular provider. The court explained that unlike the GPS data collected by law enforcement in *Jones*, cellular providers collect and store cell site data "for [their] own business purposes, perhaps to monitor or optimize service on [their] network[s] or to accurately bill [their] customers for the segments of [the] network[s] that they use."[114] Moreover, "[t]he Government does not require service providers to record this information or store it."[115] Consistent with *Smith v. Maryland*, the court explained that "[t]o the extent an individual knowingly exposes his activities to third parties, he surrenders Fourth Amendment protections, and, if the Government is subsequently called upon to investigate his activities for possible violations of the law, it is free to seek out these third parties, to inspect their records, and to probe their recollections for evidence."[116] The court disagreed with arguments that users' conveyance of cell site information is not voluntary. The court asserted that users indeed understand that their phones must send location-based signals to cell towers in order to connect calls to in-range towers, and that service agreements inform users that providers use, maintain, and may disclose to law enforcement users' location information. Finally, although the court recognized that "technological changes can alter societal expectations of privacy," it also recognized a corresponding need for law enforcement to have tools to ensure that criminals cannot circumvent the system. It advised that "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative" and that "[a] legislative

---

type of records the Supreme Court contemplated in *Smith*"); United States v. Thousand, 558 Fed. Appx. 666, 670 (7th Cir. 2014) (appellant never asserted that government's § 2703(d) order lacked probable cause, and even if she had, court was unable to find "any federal appellate decision accepting Thousand's premise that obtaining cell site data from telecommunications companies—under any factual scenario—raises a concern under the Fourth Amendment") (citing cases); United States v. Guerrero, 768 F.3d 351, 360-61 (5th Cir. 2014) (finding that *Riley* did not overrule the third-party doctrine, but noting that "[t]his is not to say that the Supreme Court may not reconsider the third party doctrine in the context of historical cell site data or some other new technology"); United States v. Shah, Crim. Case No. 5:13cr328, 2015 WL 72118, at *9 (E.D.N.C. Jan. 5, 2014); United States v. Giddins, No. WDQ-14-0116, 2014 WL 4955472, at *8 (D. Md. 2014); United States v. Banks, 2014 WL 4594197, at *3-4 (D. Kan. Sept. 15, 2014); United States v. Graham, 846 F.Supp.2d 384, 389-390 (D.Md. 2012). *But see* United States v. Davis, 754 F.3d 1205, 1217 (11th Cir.) (agreeing with the Fourth Circuit and finding no voluntary sharing of cell site location information where users are unlikely aware that providers collect and store such information), *reh'g en banc granted, opinion vacated*, 573 F. App'x 925 (11th Cir. 2014); In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 317 (3d Cir. 2010).

[113] *In re: Application of The United States of America for Historical Cell Site Data*, 724 F.3d 600, 614 (5th Cir. 2013).

[114] *Id.* at 611-12.

[115] *Id.*

[116] *Id.* at 610.

body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[117]

The previous year, the Sixth Circuit likewise upheld cell site tracking in *United States v. Skinner*,[118] albeit on different grounds. Relying primarily on *United States v. Knotts*,[119] the court concluded that cell site data obtained by pinging a defendant's cell phone merely "aided the police in determining [the defendant's] location" while he was moving drugs on a public street, and that "that same [location] information could have been obtained through visual surveillance."[120] The court so found even though, at the time the cell phone was pinged, police had never obtained a visual mark on the defendant, did not know the make or model of his vehicle, and did not know the defendant's actual identity.[121] Noting that law enforcement "could have simply monitored [the defendant's coconspirators'] whereabouts to discover [the defendant's] identity," the court explained that "using a more efficient means of discovering this information does not amount to a Fourth Amendment violation."[122] Ultimately, the court found "no inherent constitutional difference between trailing a defendant and tracking him via such technology," and asserted that "[i]f a tool used to transport contraband gives off a signal that can be tracked for location, certainly the police can track the signal."[123] Finally, the court distinguished *Jones*, finding no physical trespass on the defendant's property nor "extreme comprehensive tracking" (comparing the three days of police-tracking in *Skinner* with the 28 days of tracking in *Jones*).[124]

The Seventh Circuit noted in a 2014 opinion that it "ha[d] not found any federal appellate decision accepting Thousand's premise that obtaining cell site data from telecommunications companies—under any factual scenario—raises a concern under the Fourth Amendment.[125] The Fifth Circuit likewise concluded that historical cell site data is not governed by the Fourth Amendment.[126]

Indeed, the only Circuit to have concluded differently is the Third Circuit. In the case of *In re Application of the United States for an Order Directing a Provider of Electronic Communication Services to Disclose Records to the Government*,[127] the court reversed a magistrate judge's denial of a section 2703(d) court order (see discussion of the Stored Communications Act, below) for cell site location information, finding nothing in the statutory language that required the government to show probable cause in all applications for a Section 2703(d) order for cell site location information. Nevertheless, the Third Circuit concluded that the lower court had *discretion* to require the government, in appropriate instances, to obtain a warrant for such information. Most significantly, the court found unpersuasive the government's argument that cell site location information is never protected by the Fourth Amendment because it is voluntarily given to a third party; it concluded that "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way" since "it is unlikely that cell phone

[117] *Id.* at 614 (quoting *Jones*, 132 S.Ct. at 964) (Alito, J., concurring in the judgment)).
[118] United States v. Skinner, 690 F.3d 772, 777 (6th Cir. 2012), *cert. denied*, 133 S. Ct. 2851 (2013).
[119] 460 U.S. 276 (1983).
[120] 690 F.3d at 778.
[121] *Id.* at 779.
[122] *Id*.
[123] *Id.* at 777-78.
[124] *Id.* at 780.
[125] 558 Fed.Appx. 666, 670 (7th Cir. 2014).
[126] United States v. Guerrero, 768 F.3d 351, 360-61 (5th Cir. 2014).
[127] 620 F.3d 304, 317 (3d Cir. 2010).

customers are aware that their cell phone providers collect and store historical location information."[128]

Looking forward, it is hard to guess how the circuits would rule if not bound by *Smith v. Maryland*'s third party doctrine. Although users are increasingly aware that cellular providers collect and store their location data as business records, it remains unclear whether users voluntarily transfer such information to their providers—particularly if the alternative is to eschew use of a cellular phone.

Electronic Searches at the Border

In 2013, the Ninth Circuit in *United States v. Cotterman* revisited the long-standing rule permitting suspicion-less searches at the U.S. border.[129] The Circuit held *en banc* that government officials must have "reasonable suspicion" before conducting forensic searches of laptops at the border—drawing a line between these more intensive searches and "quick view" searches, neither of which have traditionally required reasonable suspicion.[130] The *Cotterman* matter arose after a Ninth Circuit panel reversed the suppression of electronic evidence of child pornography, which border agents found in the unallocated space of the defendant's laptop hard drive during a forensic search.[131] The Ninth Circuit took the matter up *en banc* to reconsider the contours of the Fourth Amendment "reasonableness" limitations in a border search. The court concluded that a "comprehensive and intrusive" forensic search of a laptop requiring the use of software "implicat[es] substantial personal privacy interests" because of the nature and volume of "private and sensitive" information individuals carry on their electronic devices—rendering these devices more akin to "personal papers" afforded special protection under the Fourth Amendment than mere personal property. The court also found the oft-advanced rationale for a broad border search exception—i.e., that travelers have advance notice of a border search and can choose to leave sensitive materials behind—to be less compelling in the electronic search context since electronic devices "often retain . . . information far beyond the perceived point of erasure."[132] The court concluded that "[a] person's digital life ought not be hijacked simply by crossing a border," and that absent reasonable suspicion, the government may not conduct a "computer strip search."[133] Nevertheless, the court reversed the district court's suppression order, finding the agents had had reasonable suspicion where the defendant had a previous child molestation conviction, was a "frequent traveler," had password protected files on his laptop, and was traveling to a country known for sex-tourism (Mexico).

At least one out-of-circuit court has followed *Cotterman*'s lead in 2014. In *United States v. Saboonchi*,[134] the U.S. District Court for the District of Maryland concluded that

---

[128] In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 317 (3d Cir. 2010); *accord United States v. Davis*, 754 F.3d 1205, 1217 (11th Cir.) (agreeing with the Third Circuit and finding no voluntary sharing of cell site location information where users are unlikely aware that providers collect and store such information), *reh'g en banc granted, opinion vacated*, 573 F. App'x 925 (11th Cir. 2014).

[129] 709 F.3d 952 (9th Cir. 2013), *cert. denied* Jan. 13, 2014.

[130] *See, e.g.*, United States v. Linarez-Delgado, 259 F. App'x 506, 508 (3d Cir. 2007); United States v. Ickes, 393 F.3d at 506–07.

[131] The unallocated space of the hard drive is an area containing data deleted by and unavailable to the average user, yet not overwritten by new data. 709 F.3d at 958, n.5

[132] *Id.* at 965.

[133] *Id.* at 966.

[134] 990 F. Supp. 2d 536, 539 (D. Md. 2014) *reconsideration denied*, No. 13-cr-100, 2014 WL 3741141 (D. Md. July 28, 2014).

under the facts of the case, reasonable suspicion was required before a forensic computer search was performed at the border.

Nevertheless, not all courts have agreed. The Southern District of New York reached a contrary conclusion in *Abidor v. Napolitano*.[135] There, plaintiffs sought to invalidate Department of Homeland Security regulations permitting government agents to inspect, copy, and/or detain electronic devices crossing the U.S. border, without reasonable, individualized suspicion that the devices contain contraband subject to their agencies' jurisdiction. The court rejected plaintiffs' as-applied and facial challenges to the regulations on two bases. First, the court found that the plaintiffs lacked standing in an action seeking (as plaintiffs were) a declaratory judgment, given the low likelihood that they would be subject to *future* suspicionless searches—let alone forensic searches—of their electronic devices at the border. Second, the court rejected the plaintiffs' argument that reasonable suspicion is required for forensic searches of electronic devices at the border. The court fell back on traditional rationales supporting suspicionless border searches but noted that, "if suspicionless forensic computer searches at the border threaten to become the norm, then some threshold showing of reasonable suspicion should be required."[136]

Although the question of whether reasonable (or any) suspicion is required for forensic searches at the border, the case law suggests that the standard remains low: In all three cases, the courts declined to invalidate the searches, finding that the border agents had had "reasonable suspicion" for their searches.

IV. FIFTH AMENDMENT PRIVILEGE AND DATA ENCRYPTION

Encryption software may shield information from government search and seizure, but whether it will do so will depend on the government's knowledge of the existence of encrypted incriminating data and of who has possession, ownership, and/or control of the data.

It is well settled that the Fifth Amendment's protection that individuals may not be compelled to be witnesses against themselves prohibits the government from compelling incriminating testimonial statements, but not incriminating non-testimonial acts. Courts have long approved government-compelled, incriminating field sobriety tests, handwriting samples, medical tests, and more, even where they would not approve a government-compelled statement suggesting the same conclusion. Although non-verbal acts ordinarily fall outside of the Fifth Amendment's protection, courts have nevertheless recognized that some actions can be testimonial, if they require an individual to disclose the contents of her mind. For this reason, courts have held that requiring a criminal defendant to produce documents or other evidence may be testimonial if the act of production communicates the existence of evidence demanded, the defendant's possession and control over that evidence, or its authenticity. Nevertheless, if the contents of that communication is a foregone conclusion—that is, does not communicate anything new at all—the act is non-testimonial and outside of the Fifth Amendment's protection.

In recent years, courts have considered whether forced decryption of encrypted devices is more akin to a non-testimonial act (like the production of a physical key) or a testimonial act (like the production of an safe combination or other information that

[135] No. 1:10-cv-04059-ERK (S.D.N.Y., Dec. 31, 2013).
[136] *Id.* at 30.

communicates content from the defendant's mind). They have also grappled with the question of in what circumstances that production may simply be a foregone conclusion.

A Virginia court took on two of the easier iterations of these questions in late 2014 in *Commonwealth v. Baust*.[137] The government there sought to compel the defendant either to disclose his passcode or provide a fingerprint that would permit access to his cell phone, which the government suspected contained evidence of an assault. The court noted that it is well settled that the Fifth Amendment does not protect an individual from compelled incriminating conduct unless that conduct is testimonial. Since compelling the fingerprint would not require the defendant to divulge his mental processes or communicate any knowledge at all, the court granted the government's motion to compel the fingerprint. It took the opposite view regarding the passcode, however: compelling the passcode would require the defendant to disclose the contents of his mind, and "[c]ontrary to the Commonwealth's assertion, the password [wa]s not a foregone conclusion because … [if it were,] the Commonwealth would not need to compel Defendant to produce it because they would already know it."[138]

Both federal and state courts have now addressed the more complicated question of whether and when a defendant may be compelled to enter his password and produce unencrypted data (rather than disclose the secret passcode to law enforcement).

The Eleventh Circuit addressed the question in In *In re Grand Jury Subpoena Duces Tecum*.[139] There, the government seized encrypted hard drives that it believed contained child pornography and sought to compel the defendant to decrypt the drives over his Fifth Amendment objection. The circuit court held that compelling the suspect to decrypt and produce the drives "would require the use of the contents of [the defendant's] mind" and that "the decryption and production would be tantamount to testimony by [the defendant] of his knowledge of the existence and location of potentially incriminating files; of his possession, control, and access to the encrypted portions of the drives; and of his capability to decrypt the files."[140] In so holding, the court rejected the government's position that decrypting the device was more akin to producing a physical key (a non-testimonial act) than producing a safe combination (a testimonial act requiring use of the contents of one's mind). Finally, the court found that the compelled testimony would not be a foregone conclusion, since the record did not show that the government knew that files existed on the drives, where the purported files were located, or that the defendant was able to access the encrypted data.[141] The court explained that although the government need not "identify exactly the documents it seeks," it "does require some specificity in its requests" and that "categorical requests for documents the Government anticipates are likely to exist simply will not suffice."[142]

---

[137] No. CR14-1439 (2d Judicial Circuit, Va. Oct. 28, 2014).
[138] *Id.* at 5; *see also* In re Grand Jury Subpoena to Boucher, 2007 WL 4246473, at *5-6 (D.Vt. Nov. 29, 2007), *rev'd on other grounds* (act of producing the password itself was testimonial since it required defendant to reveal the contents of his mind); *United States v. Kirschner*, 823 F. Supp. 2d 665, 668–69 (E.D.Mich. March 30, 2010) (same).
[139] 670 F.3d 1337 (11th Cir. 2012).
[140] *Id.* at 1346.
[141] *Id.* at 1349.
[142] *Id.* at 1347-48 (quoting United States v. Hubbell, 530 U.S. 27, 45 (2000) ("The Government cannot cure this [lack of prior knowledge] through the over broad argument that a businessman such as respondent will always possess general business and tax records that fall within the broad categories described in this subpoena.").

A district court addressed similar questions under a different set of facts in *United States v. Fricosu*, reaching the opposite result.[143] There, federal agents obtained a warrant and searched the defendant's home for evidence of a mortgage scam, seizing three computers, one of which was encrypted. During a subsequent recorded jailhouse conversation, defendant and her husband discussed whether Ms. Fricosu "took [her] laptop" when she "went there," whether she had "anything on [her] computer to protect it," that "it would have been on there," and that she "[did not] know if they c[ould] get to it." Defendant Fricosu further stated: "My lawyer said I'm not obligated by law to give them any passwords or anything they need to figure things out for themselves."[144] The court granted a writ requiring Ms. Fricosu to decrypt and produce the laptop's contents over her Fifth Amendment objection, finding that the act of decrypting the computer was not "testimonial" since the government knew of the existence and location of incriminating files on the computer; that that the government "[did] not know the specific content of any specific documents [was] not a barrier to production."[145]

A more recent decision applying the same analysis, however, came out the other way. In *In re Decryption of a Seized Data Storage System*,[146] the FBI seized numerous storage devices from the defendant's home and found encrypted data on nine of them. On one of the encrypted devices, the FBI found files with titles indicative of child pornography. The court found that the government had shown that the encrypted devices contained data and had even known the names of the files, and therefore that the existence and location of the files were a foregone conclusion.[147] However, since the government had only shown that the defendant "may very well be capable of accessing the encrypted portions of the hard drives," his act of production would have been testimonial: successful entry of his password "would be tantamount to telling the government something it [did] not already know with 'reasonable particularity' – namely, that [defendant] has *personal access to and control over* the encrypted storage devices."[148]

In aggregate, these decisions limit government investigators' ability to compel an individual to reveal the contents of devices encrypted with passwords or codes in a criminal investigation, where the government is only speculating as to the data on the devices or the defendant's ownership or control over them. Although a corporation or partnership does not enjoy Fifth Amendment protection, individuals and sole proprietorships do, and this decision could have a significant impact on small businesses and individuals who work in highly regulated industries including health care, government contracting, energy, chemicals, and others that may face government scrutiny.

---

[143] United States v. Fricosu, 841 F.Supp.2d 1232, 1236 (D. Colo. 2012).
[144] *Id.* at 1236.
[145] *Id.* at 1237.
[146] No. 2:13-M-449 (E.D. Wisc., Apr. 19, 2013).
[147] *Id.* at *8.
[148] *Id*. at *9 (emphasis in original); *see also* Commonwealth v. Gelfgatt, No. SJC-11358, 468 Mass. 512 (June 25. 2014) (compelled production of decrypted evidence was nontestimonial where existence and location of incriminating evidence, as well as defendant's control over computer and encryption key, were a foregone conclusion).

V. POST-INDICTMENT DISCOVERY

Joint Federal Criminal E-Discovery Protocol

Unlike e-discovery in civil litigation, which benefits from specific procedural rules and developed case law to guide its practitioners, criminal e-discovery practice continues to face a vacuum of formal guidance. In 2012, the Joint Working Group on Electronic Technology in the Criminal Justice System (comprised of representatives from the DOJ, Federal Defender Organizations, the U.S. Judiciary, and private Criminal Justice Act panel attorneys) formally issued its "Recommendations for ESI Discovery Production in Federal Criminal Cases," designed to aid criminal attorneys, particularly prosecutors, public defenders, and CJA panel attorneys, who have previously wrestled with e-discovery issues.

The Joint E-Discovery Protocol, guidelines only intended to apply to disclosure of ESI under Federal Rules of Criminal Procedure 16 and 26.2, *Brady, Giglio* and the Jencks Act,[149] is comprised of 3 parts: (1) Recommendations; (2) Strategies and Commentary; and (3) an ESI Discovery Checklist. The foundation of the Joint Protocol rests on the following ten principles drawn from core civil practice concepts, including meet and confers, direction about form of production, the use of advanced technology, and conflict resolution:[150]

1. Lawyers have a responsibility to have an adequate understanding of electronic discovery.

2. In the process of planning, producing, and resolving disputes about ESI discovery, the parties should include individuals with sufficient technical knowledge and experience regarding ESI.

3. At the outset of a case, the parties should meet and confer about the nature, volume, and mechanics of producing ESI discovery. Where the ESI is particularly complex or produced on a rolling basis, an ongoing dialogue may be helpful.

4. The parties should discuss what formats of production are possible and appropriate, and what formats can be generated. Any format selected for producing discovery should maintain the ESI's integrity, allow for reasonable usability, reasonably limit costs, and, if possible, conform to industry standards for the format.

5. When producing ESI discovery, a party should not be required to take on substantial additional processing or format conversion costs and burdens beyond what the party has already done or would do for its own case preparation or discovery production.

6. Following the meet and confer, the parties should notify the court of

[149] The Joint Protocol's Recommendations specifically state that they do not "apply to, nor do they create any rights, privileges, or benefits during, the gathering of ESI as part of the parties' criminal or civil investigations." Recommendations for ESI Discovery Production in Federal Criminal Cases at n1, *available at* http://nlsblogdotorg.files.wordpress.com/2012/02/final-esi-protocol.pdf.

[150] *Id.* at Introduction to Recommendations for ESI Discovery in Federal Criminal Cases.

ESI discovery production issues or problems that they reasonably anticipate will significantly affect the handling of the case.

7. The parties should discuss ESI discovery transmission methods and media that promote efficiency, security, and reduced costs. The producing party should provide a general description and maintain a record of what was transmitted.

8. In multi-defendant cases, the defendants should authorize one or more counsel to act as the discovery coordinator(s) or seek appointment of a Coordinating Discovery Attorney.

9. The parties should make good faith efforts to discuss and resolve disputes over ESI discovery, involving those with the requisite technical knowledge when necessary, and they should consult with a supervisor, or obtain supervisory authorization, before seeking judicial resolution of an ESI discovery dispute or alleging misconduct, abuse, or neglect concerning the production of ESI.

10. All parties should limit dissemination of ESI discovery to members of their litigation team who need and are approved for access, and they should also take reasonable and appropriate measures to secure ESI discovery against unauthorized access or disclosure.

The stated purpose of the Joint Protocol also highlights the role of civil principles in their formation:

> These Recommendations are intended to promote the efficient and cost-effective post-indictment production of [ESI] in discovery between the Government and defendants charged in federal criminal cases, and to reduce unnecessary conflict and litigation over predictable framework for ESI discovery, and by establishing methods for resolving ESI discovery disputes without the need for court intervention.[151]

Several important Recommendations of the Joint E-Discovery Protocol warrant discussion. First, the Recommendations are just that; they are not binding on any party and they are not enforceable rules. Thus, the Protocol makes clear that the traditional mechanisms in place to handle discovery disputes will remain the same, and that, if there are disputes, the parties will have to go to court to get them resolved. But prior to seeking court intervention, the Protocol recommends that the parties meet and confer, make good faith efforts to discuss and resolve disputes over ESI discovery, and engage and/or consult with technical experts as needed at the outset of the discovery process. Importantly, if efforts to cooperate and reach agreement about ESI are unsuccessful, the Protocol recommends that each side consult with a supervisor or obtain a supervisor's authorization before going to the court. This remains consistent with an important theme of the Joint E-Discovery Protocol: the promotion of dialogue between the parties and attempts at cooperation, both hallmarks of the civil process.

[151] *Id.* at Recommendations for ESI Discovery Production in Federal Criminal Cases at 1.

Several courts have addressed the Joint E-Discovery Protocol. In *United States v. Reynolds*, defendants argued that under the protocol, they were entitled to "organizational discovery" from the government, including indices, transcripts, searchable databases and other identifying information from government wiretaps.[152] The court first highlighted that the U.S. Constitution, Federal Rules of Criminal Procedure, the Jencks Act and other federal statutes governed discovery in matter, not the Recommendations themselves.[153] In denying the defendants' request, the court noted that "it appears Defendants failed to actually read the Recommendations upon which they rely in seeking to compel the requested discovery. Based upon the facts made known to the court, and not disputed by defense counsel, defense counsel failed to discuss the matter in good faith with government counsel. Instead, in contravention of the Recommendations, Defendants brought the matter directly to the court undermining the very purpose of the Recommendations and wasting litigation and judicial resources."[154]

Potential* Brady *Issues in ESI Productions

When confronting a massive ESI production from the government, the line between an impermissible "data dump" and permissible "open file" production for defense counsel remains unclear. In *United States v. Skilling*, [155] the defendant argued that the government's production of hundreds of millions of pages violated the government's *Brady* obligations as the "voluminous open file . . . suppressed exculpatory evidence."[156] The defendant added that "no amount of diligence, much less reasonable diligence" would have allowed him to effectively review the government's disclosure. Defendant's counsel estimated "it would have taken scores of attorneys, working around-the-clock for several years to complete the job."[157]

The Fifth Circuit disagreed, noting that the government did not simply dump several hundred million pages on the defendant's doorstep. Rather, the government's open file production was electronic and searchable, the government produced a set of "hot documents" that it thought were important to its case or were potentially relevant to the defense, and the government created indices to these and other documents. The court added that "the government was in no better position to locate any potentially exculpatory evidence than was Skilling."[158] The *Skilling* decision—and other decisions addressing *Brady* in the ESI context—suggests that the more voluminous the data dump, the more organization and indexing will be required from the government.

Similar to the "open file" approach under *Skilling,* the court in *United States v. Salyer*, [159] ordered the government to identify Rule 16, *Brady*, and *Giglio* materials contained in the ESI production to the defense as a "matter of case management (and fairness)."[160] *Salyer* involved the government's large scale "open file" production to a defendant detained in jail awaiting trial, who was represented by a small firm with limited

[152] United States v. Reynolds, No. 1:13-cr-02225-MV (D.N.M. Sept. 19, 2014).
[153] *Id.*
[154] *Id.*
[155] United States v. Skilling, 554 F.3d 529 (5th Cir. 2009).
[156] *Id*. at 576.
[157] *Id*.
[158] *Id*. at 577.
[159] United States v. Salyer, No. S-10-0061, 2010 WL 3036444 (E.D. Cal. Aug. 2, 2010).
[160] *Id.* at *2.

resources.[161] The government stated that if it were required to review the materials it had acquired in the investigation to identify *Brady/Giglio* materials, the burden of doing so would be impossible, and it might have to dismiss the case. The court noted that if

> the government professes this inability to identify the required information after five *years* of pre-indictment investigation, its argument that the defense can 'easily' identify the materials buried within the mass of documents within *months* of post-indictment activity is meritless. Obviously, under the government's reasoning, the defense burden is even more impossible. What the government is actually arguing, in effect and for practical purposes, is that logistics in the 'big documents' case render *Brady/Giglio* a dead letter no matter who has the burden of ascertaining the information. There is no authority to support this evisceration of constitutional rights just because the case has voluminous documentation.[162]

The *Salyer* court explained that "the government cannot meet its *Brady* obligations by providing [the defendant] with access to 600,000 documents and then claiming that she should have been able to find the exculpatory information in the haystack."[163] "[A]t some point (long since passed in this case) a duty to disclose may be unfulfilled by disclosing too much; at some point, "disclosure," in order to be meaningful, requires "identification" as well."[164] Addressing the government's argument that without understanding the defense theory it could not undertake a *Brady* review of the massive ESI database, the court provided this useful guidance:

> When the prosecution, in good faith, determines that a piece of evidence, on its face, significantly tends to controvert what it is attempting to prove, disclosure (and in this case, identification as well) is mandated. Similarly, for *Giglio* information, the prosecution knows, from its vantage point, what information is significantly inconsistent with the testimony it expects *its* potential witnesses to present or with their credibility generally.[165]

Speedy Trial Issues and ESI Production

Failure by the government to properly plan and manage the production of ESI can also result in dismissal of its case. In *United States v. Graham*, the government was slow to produce millions of documents and other media, and the defendants had great difficulty in coping with the large volume.[166] The court dismissed the indictment for Speedy Trial Act violations but acknowledged that discovery was at the heart of the matter: "In this case, the problem . . . is and has been discovery . . . . One, the volume of discovery in this case quite simply has been unmanageable for defense counsel. Two, like a restless volcano, the government periodically spews forth new discovery, which adds to defense counsels' already

---

[161] *Id.* at *7.
[162] *Id.* at *5.
[163] *Id.* at *6.
[164] *Id.*
[165] *Id.* at *5. *But see* United States v. Rubin/Chambers, No. 09 Cr. 1058, 2011 WL 5448066 (S.D.N.Y. Nov. 4, 2011) (distinguishing *Salyer* and finding no *Brady* violation where, in large ESI production, government provided searchable materials, indices, and metadata to defense counsel).
[166] United States v. Graham, No. 1: 05-CR-45, 2008 WL 2098044, at *2-3 (S.D. Ohio May 16, 2008); *see also* State v. Dingman, 202 P.3d 388 (Wash. Ct. App. 2009) (reversing conviction and remanding for new trial after finding that trial court erred by denying defendant meaningful access to hard drives seized from his house).

monumental due diligence responsibilities. Three, the discovery itself has often been tainted or incomplete."[167] In dismissing the case, the court noted that, although the government did not act in bad faith, "discovery could have and should have been handled differently."[168]

VI. SOCIAL MEDIA AND THE INTERNET

Social media is now a fundamental pillar of communication in today's society, revolutionizing how the world does business, learns about and shares news, and instantly engages with friends and family. Not surprisingly, this medium significantly impacts government investigations and criminal litigation.

The Importance of Social Media

Most people use social media in their everyday lives. 91% of today's online adults use social media regularly, and "[s]ocial networking continues to reign as the top online activity."[169] In fact, the number of people actively using social media each month worldwide has now passed the 2 billion mark.[170] More than 1.2 billion people use Facebook actively each month,[171] and Twitter has over 1 billion users posting 500 million Tweets a day.[172] Almost three-quarters of online adults visit Facebook at least once a month. Instagram, with more than 200 million users, already has more than 20 billion uploaded photos.[173] These sources of information have resulted in a digital goldmine of potential evidence: profiles, lists of friends, group memberships, messages, chat logs, Tweets, photos, videos, tags, GPS locations, check-ins, login timetables, and more.[174]

The information available from social media providers is staggering. When a phone company responds to a government subpoena or search warrant, it may provide call or message logs. In contrast, when a social media company such as Facebook responds to a government subpoena it provides the user's profile, wall posts, photos uploaded by the user, photos in which the user was tagged, a comprehensive list of the user's friends with their Facebook IDs, and a long table of login and IP data.[175] And, with the expansion of location-

---

[167] *Graham*, 2008 WL 2098044 at *5.
[168] *Id*. at *8. *But see* United States v. Qadri, 2010 WL 933752 (D. Haw. Mar. 9, 2010) (denying motion to dismiss on speedy trial grounds, despite finding that the delays were due at least in part to the nature of e-discovery, the complex nature of the alleged crimes, and the necessity of several coordinating branches of government in the investigation).
[169] Experian Marketing Services, *The 2012 Digital Marketer: Benchmark and Trend Report*, at 79, http://www.experian.com/simmons-research/register-2012-digital-marketer.html (last visited Oct. 24 2012).
[170] Global Social Media Users Pass 2 Billion, Aug, 8, 2014, http://wearesocial.net/blog/2014/08/global-social-dia-users-pass-2-billion/.
[171] Facebook, Twitter, Instagram, Pinterest, Vine, Snapchat – Social Media Stats 2014, June 9, 2014, http://www.adweek.com/socialtimes/social-media-statistics-2014/499230.
[172] *Id*.
[173] *Id.*
[174] *See* Quagliarello v. Dewees, No. 09-4870, 2011 WL 3438090, at *2 (E.D. Pa. Aug. 4, 2011) ("As the use of social media such as MySpace and Facebook has proliferated, so too has the value of these websites as a source of evidence for litigants.").
[175] For example, the Boston Police Department publicly released the case files of the alleged "Craigslist Killer," Philip Markoff, who committed suicide while awaiting trial. Those case files include the District Attorney's subpoena to Facebook as well as Facebook's response. Carly Carioli, *When The Cops Subpoena Your Facebook Information, Here's What Facebook Sends the Cops* (Apr. 6, 2012), http://blog.thephoenix.com/blogs/phlog/archive/2012/04/06/when-police-subpoena-your-facebook-information-heres-what-facebook-sends-cops.aspx.

based services offered by social media companies like Facebook, Twitter, and FourSquare, precise geolocation information will be increasingly maintained in the ordinary course of business and subject to the same subpoenas and search warrants.[176] Not surprisingly, each social media subpoena can yield admissions or incriminating photos, among other evidence.[177]

Public and Quasi-Public Social Media Evidence

It is no secret that government agencies mine social networking websites for evidence because, even without having to seek a warrant from the court or issue a subpoena, there are troves of social media evidence publicly available.[178] A majority of government agencies are active participants, contributing content and soliciting information through social media. For example, a recent survey on law enforcement use of social media published by the IACP Center for Social Media—a website created in partnership with the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, whose goal is to build the capacity of law enforcement to use social media to prevent and solve crimes, strengthen police-community relations, and enhance services—demonstrates the overwhelming use of social media by law enforcement:

- 95% of agencies surveyed use social media.
- The most common use of social media is for criminal investigations at 82.3%.
- The most frequently used social media platforms are Facebook (95.4%), Twitter (66.4%), and YouTube (38.5%).
- 55.9% of agencies not currently using social media are considering doing so.
- 71.7% of agencies surveyed have a social media policy and an additional 12.2% are in the process of crafting a policy.
- 78.8% of agencies report that social media has helped solve crimes in their jurisdiction.
- 77.5% of agencies state that social media has improved police-community relations in their jurisdiction.[179]

Given the amount of information publicly available, and the avenues that the government has to seek out such information, the government often does not even need a search warrant, subpoena, or court order to obtain social media evidence.

Moreover, government agents can, and do, go further than defense counsel is allowed in pursuing social media evidence for a criminal proceeding. To bypass the need for a search warrant, government agents may pierce the privacy settings of a person's social media account by creating fake online identities or by securing cooperating witnesses to

[176] Electronic Frontier Foundation, *2012: When the Government Comes Knocking, Who Has Your Back?* (May 31, 2012), https://www.eff.org/sites/default/files/who-has-your-back-2012_0_0.pdf.
[177] *See, e.g.*, United States v. Anderson, 664 F.3d 758, (8th Cir. 2012) (sentencing defendant to 12 years in prison based in part on over 800 private chats with adolescent girls that were obtained through a search warrant for defendant's Facebook account).
[178] *See, e.g.*, U.S. Dep't of Homeland Security, *Publicly Available Social Media Monitoring and Situational Awareness Initiative* (June 22, 2010); *see also* LexisNexis, *Role of Social Media in Law Enforcement Significant and Growing* (July 18, 2012), http://www.lexisnexis.com/media/press-release.aspx?id=1342623085481181 (over 80% of local and federal agencies use social media during investigations).
[179] International Association of Chiefs of Police 2014 Social Media Survey Results, http://www.iacpsocialmedia.org/Resources/Publications/2014SurveyResults.aspx.

grant them access to information.[180] In *United States v. Meregildo*,[181] for example, the defendant set the privacy settings on his Facebook account so that only his Facebook "friends" could view his postings. The government obtained the incriminating evidence against the defendant through a cooperating witness who happened to be Facebook "friends" with the defendant. The defendant moved to suppress the evidence seized from his Facebook account, arguing that the government had violated his Fourth Amendment rights. The court found:

> [W]here Facebook privacy settings allow viewership of postings by 'friends,' the Government may access them through a cooperating witness who is a 'friend' without violating the Fourth Amendment. While [defendant] undoubtedly believed that his Facebook profile would not be shared with law enforcement, he had no justifiable expectation that his 'friends' would keep his profile private. And the wider his circle of 'friends', the more likely [defendant's] posts would be viewed by someone he never expected to see them. [Defendant's] legitimate expectation of privacy ended when he disseminated posts to his 'friends' because those 'friends' were free to use the information however they wanted -- including sharing it with the Government.[182]

Social Media Companies, Subpoenas and Warrants

Given the digital goldmine of potential evidence available from social media companies, it is not surprising that they are increasingly targeted by search warrants and government subpoenas in criminal matters. For example, government information requests from Twitter continue to increase at a substantial rate.[183] And more than 60% of those requests were from authorities in the United States.[184] Google, which is a provider of social

---

[180] *See, e.g.,* United States v. Robison, No. 11CR380 DWF/TNL, 2012 WL 1110086, at *2 (D. Minn. Mar. 16, 2012) (law enforcement created fake online identity and became Facebook friends with defendant, "which permitted [the government] to view [defendant's] name and photo on his Facebook account"); *United States v. Phillips*, No. 3:06–CR–47, 2009 WL 1918931, at *7 (N.D. W.Va. July 1, 2009) (government "created an undercover user profile on www.myspace.com").

Despite a long history of prosecutors and investigators engaging in "ruses" during investigations of a crime, in recent years there has been some confusion over whether state ethics rules—and particularly Rule 8.4(c)—prohibit such conduct. *Compare* ABA Model Rules, Rule 8.4(c) ("It is professional misconduct for a lawyer to: . . . (c) engage in conduct involving dishonesty, fraud, deceit or misrepresentation"), *with* In re the Matter of Pautler, Case No. 01SA129 (Colo. 2002) (after defendant refused to surrender without a lawyer, prosecutor posed as a public defender and negotiated surrender; attorney was found to have violated ethics rules requiring lawyers correct an unrepresented party's misunderstanding of the lawyer's role in the litigation, and prohibiting deception); *Cuyahoga County Prosecutor Fired After Posing as an Accused Killer's Girlfriend on Facebook to Try to Get Alibi Witnesses to Change Their Testimony*, Cleveland.com, June 6, 2013, http://www.cleveland.com/metro/index.ssf/2013/06/cuyahoga_county_prosecutor _fir.html. As a result of such confusion, numerous states have amended their ethics rules to expressly permit prosecutors to supervise lawful covert activity, or to prohibit only dishonesty, fraud, deceit or misrepresentation that reflects adversely on the attorney's fitness to practice law. *See, e.g.,* Missouri Supreme Court, Rule 4-8.4(c); Oregon Rules of Professional Conduct, Rule 8.4; Florida Rules of Professional Conduct, Rule 4-8.4(c); Virginia Rules of Professional Conduct, Rule 8.4(c).

[181] United States v. Meregildo, No. 11 Cr. 576(WHP), 2012 WL 3264501, at *2 (S.D.N.Y. Aug. 10, 2012).

[182] *Id.*

[183] *Twitter Transparency Report* (Jan. 1-June 30, 2014), https://transparency.twitter.com/information-requests/2014/jan-jun

[184] *Id.*

networking sites like YouTube and Google+, continues to see an increase in the frequency with which it receives subpoenas and search warrants in criminal matters.[185]

At least one court has questioned a government request to obtain social media evidence with a search warrant. In *In re the Search of Information Associated with Facebook Account Identified by the Username Aaron.Alexis Stored at Premises Controlled by Facebook, Inc.*, Magistrate Judge John Facciola determined the government's search warrant was overbroad under the Fourth Amendment and significantly narrowed the scope of the information Facebook could give to the government.[186] Specifically, the court permitted the government to seize only information related to its investigation to protect unwarranted invasion into the privacy of third parties; no probable cause had been shown for search and seizure of information related to third parties. Noting that this was the second time this year that the court had rejected an overly broad search and seizure warrant application directed at Facebook, Judge Facciola wrote that the

> government should exercise caution and more narrowly tailor future warrant applications directed at Facebook; individuals may voluntarily share their information with Facebook, but the government, by seeking a search warrant, justly reasons that probably cause for searching within a Facebook account is still a constitutional necessity, particularly when it will have to see third party communication that are innocuous and irrelevant to and sent by persons who could not possibly have anticipated that the government would see what they have posted.[187]

Accounting for the Stored Communications Act

Federal law provides that, in some circumstances, the government may compel social media companies to produce social media evidence without a warrant. The SCA governs the ability of governmental entities to compel service providers, such as Twitter and Facebook, to produce content (*e.g.*, posts and Tweets) and non-content customer records (*e.g.*, name and address) in certain circumstances.[188] The SCA—and the broader statute of which it a part, the Electronic Communications Protection Act ("ECPA")—was passed in 1986 and has not been amended to reflect society's heavy use of new technologies and electronic services, such as social media, which have evolved since the SCA's original enactment.[189] As a result, courts have been left to determine how and whether the SCA

---

[185] *Google Transparency Report*, http://www.google.com/transparencyreport/.
[186] Case 13-MJ-742 (JMF) (D.D.C. Nov. 26, 2013).
[187] *Id*. at 8. Judge Facciola's opinion also shares a brief glimpse into his "second" opinion, still under seal, rejecting an overly broad warrant application by the government. He notes that the government's application in that matter "casts a remarkable dragnet over communications that surely have nothing to do with this case, including those to and from third parties, who will never know of the government's seeing their communications with John Doe about unrelated matters." *Id.* (citing In the Matter of the Search of Information associated with Facebook Account: http://facebook.com/[John Doe] that is stored at premises controlled by Facebook, Inc.).
[188] *See* United States v. Warshak, 631 F.3d 266, 282 (6th Cir. 2010) (citing 18 U.S.C. §§ 2701 et seq.); Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 977 (C.D. Cal. 2010) (applying the SCA to subpoenas issued to Facebook and MySpace while recognizing that no courts "have addressed whether social networking sites fall within the ambit of the statute").
[189] *See* Rudolph J. Burshnic, Note, *Applying the Stored Communications Act to the Civil Discovery of Social Networking Sites*, 69 Wash. & Lee L. Rev. 1259, 1264 (2012).

applies to the varying features of different social media services, applying precedent from older technologies such as text messaging pager services and electronic bulletin boards.[190]

The SCA provides that non-content records can be compelled via a subpoena or court order.[191] Regarding compelled disclosure of the content of communications, the SCA provides different levels of statutory privacy protection depending on how long the content has been in electronic storage. The government may obtain content that has been in electronic storage for 180 days or less "only pursuant to a warrant."[192] The government has three options for obtaining communications that have been in electronic storage with a service provider for more than 180 days: (1) obtain a warrant; (2) use an administrative subpoena; or (3) obtain a court order under § 2703(d).[193]

The constitutionality of the SCA has been called into question by at least one Circuit Court of Appeals. In *U.S. v. Warshak*, the Sixth Circuit held that "the government agents violated the Fourth Amendment when they obtained the contents of [defendant's] emails" without a warrant, and added that "to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional."[194] The court reasoned that "[o]ver the last decade, email has become 'so pervasive that some persons may consider [it] to be [an] essential means or necessary instrument[] for self-expression, even self-identification'" and that therefore "email requires strong protection under the Fourth Amendment."[195] Noting that e-mail was analogous to a phone call or letter and that the internet service provider was the intermediary that made e-mail communication possible—the functional equivalent of a post office or telephone company—the court concluded that given "the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection."[196]

Recognizing the SCA's deficiencies, both Congress and the White House have sought to downplay the effects of the statute in recent years. In March 2012, the Justice Department, while testifying before the House Judiciary Subcommittee on Crime, Terrorism, Homeland Security, and Investigations, announced it would drop its historic opposition to a warrant requirement before government officials can obtain content stored in the cloud, recognizing that "there is no principled basis to treat email less than 180 days old differently than email more than 180 days old," or to afford different protections to opened and unopened emails. The Justice Department also noted that there is "appeal" and "considerable merit" to proposals that would "require law enforcement to obtain a warrant based on probable cause to compel disclosure of stored email and similar stored content information from a service provider." DOJ nevertheless tempered its support for the search-warrant approach with the caveat that "Congress [must] consider contingencies for certain, limited functions for which this may pose a problem"—such as for civil litigators and

[190] *See, e.g.*, Hubbard v. MySpace, Inc., 788 F. Supp. 2d 319 (S.D.N.Y. 2011) (finding that search warrant served by state authorities on MySpace to produce, among other things, the account IP address, the contents of the account user's inbox, and sent email was sufficient to satisfy the requirements of the Stored Communications Act); Crispin, 717 F. Supp. 2d at 991 (while acknowledging the privacy settings of the user, quashing subpoenas seeking private messages on Facebook and MySpace on the basis that they were protected under the Stored Communications Act).
[191] 18 U.S.C. § 2703(c)(2); *id.* § 2703(d).
[192] Warshak, 631 F.3d at 282-83 (citation omitted).
[193] *Id.*
[194] *Id.* at 288.
[195] *Id.* (citations omitted).
[196] *Id.* at 285-286.

regulators enforcing various laws that do not carry criminal penalties (and therefore for which criminal search warrants are not available).[197]

Over the past several sessions, Congress has struggled to advance bills that would reform ECPA and, in particular, the SCA. Numerous such proposals have been introduced, referred to, or voted out of committee,[198] yet none have been passed as of this writing. Some of these proposals would require law enforcement to obtain a court-issued warrant, supported by probable cause, before compelling commercial ISPs to disclose the contents of email, social media messages, and other digital content stored in the cloud. A sticking point appears to be a desire for a carve-out permitting regulatory agencies to obtain content records without a warrant—which would significantly undermine the protections under the revised statute.

As users increasingly move content into the cloud—in email, social media, video content, cloud-based document storage, etc.—the treatment of this digital content under the SCA (if not under the Constitution) will likely require similar clarification by courts.

Defending a Criminal Case with Social Media Evidence

Defendants face more significant obstacles than the government when seeking exculpatory evidence from social media companies.[199] First, defendants and their counsel do not share the government's freedom to sleuth for social media evidence.[200] Although defense counsel may freely obtain truly *public* social media evidence (public-facing profiles, comments and the like), various state and local bar ethics opinions have established that defense counsel are limited in when and whether they may communicate with a third-party or witness in litigation in order to search for impeachment material or exculpatory evidence.[201] When contacting unrepresented parties and witnesses, for example, some opinions require an attorney to fully disclose not only that she is an attorney but also her

---

[197] Attorney General Eric Holder cemented this support for a warrant requirement for email at a May 15, 2013 hearing before the House Judiciary Committee. He stated that DOJ supported "the more general notion of having a warrant to obtain the content of communication from a service provider," but added the caveat that there may be "certain very limited circumstances" such as "civil cases" in which the government may not support a warrant requirement for electronic content. *See* Hearing Tr., House Judiciary Comm., May 15, 2013, at 87.

[198] *See, e.g.*, S. 607 (Electronic Communications Privacy Act Amendments Act of 2013); H.R. 6529 (ECPA 2.0 Act of 2012); H.R. 983 (Online Communications and Geolocation Protection Act); H.R. 1847 (Electronic Communications Privacy Act Amendments Act of 2013); H.R.1852 (Email Privacy Act); H.R. 3557 (REAP Act of 2013). In early 2015, a bipartisan and bicameral proposal was launched to once again attempt to reform the law. *See* Press Release, *Leahy Joined By Bipartisan, Bicameral Group To Introduce Bill Protecting Online Privacy*, Feb. 4, 2014, http://www.leahy.senate.gov/press/leahy-joined-by-bipartisan-bicameral-group-to-introduce-bill-protecting-online-privacy.

[199] Daniel K. Gelb, *Defending a Criminal Case from the Ground to the Cloud*, 27-SUM CRIM. JUST. 28 (2012).

[200] *See* Zach Winnick, *Social Media an Ethical Minefield for Attorneys*, Law360, Apr. 13, 2012, http://www.law360.com/articles/329795/social-media-an-ethical-minefield-for-attorneys (describing ethical concerns regarding private counsel's use of social networking sites in connection with litigation that are generally not shared by government authorities in investigations).

[201] *See, e.g.*, Philadelphia Bar Ass'n , Prof. Guidance Comm., *Opinion 2009-02* (March 2009) (concluding that a social media friend request to a witness in the litigation for the purpose of gathering social media evidence is "deceptive" and in violation of ethical rules); N.Y. State Bar Ass'n, Committee on Prof'l Ethics, *Opinion 843 (9/10/10)* (Sept. 10, 2010) (accessing publicly available social media evidence is permissible but "friending" another party to do so may not be); San Diego County Bar Legal Ethics Committee, *SDCBA Legal Ethics Opinion 2011-02* (May 24, 2011) (ethics rules bar attorneys from making ex-parte friend request of a represented party or "deceptive" friend requests of unrepresented witnesses); NH Bar Ass'n, Ethics Committee Advisory Opinion #2012-13/05, *Social Media Contact with Witnesses in the Course of Litigation* (ethics rules permit an attorney to access public-facing portions of social media); Massachusetts Bar Ass'n, Comm. On Prof'l Ethics, Op. 2014-5.

role in the instant litigation.[202] Others require not only full disclosure of these facts, but also require the attorney to send the witness or party a message; it is not sufficient, for example, to simply state in one's profile that one is an attorney.[203] And, of course, ethics rules limit when defense counsel may contact a represented witness or opposing party.[204] Despite these strict limitations, attorneys also have duties of competence and diligence that may require them to scour social media to the limits that the ethical rules allow.[205] Moreover, failure to appropriately use social media evidence can result in a finding of ineffective assistance of counsel.[206]

Second, defendants face additional hurdles when seeking to issue third-party subpoenas.[207] Defendants may seek to subpoena social media companies for user information regarding the victim, the complaining witness, or another witness.[208] In those instances, in federal criminal proceedings, defendants must pursue such non-party discovery pursuant to Federal Rule of Criminal Procedure 17 and seek a court order allowing such a subpoena.[209] Among other hurdles in seeking such an order, the court may find that the evidence maintained by a social media website is "private," in which case the SCA prohibits a non-governmental entity, such as Facebook or MySpace, from disclosing

---

[202] *See* Massachusetts Bar Ass'n, Comm. On Prof'l Ethics, Op. 2014-5 (attorney may friend an unrepresented adversaries only if she identifies herself as an attorney and states her role the litigation at issue; attorney must obtain consent to "friend" or otherwise communicate with a represented individual); New Hampshire Bar Ass'n, Ethics Committee Advisory Opinion #2012-13/05, Social Media Contact with Witnesses in the Course of Litigation; Philadelphia Bar Ass'n, Professional Guidance Committee Op. 2009-02, *Ethics & Social Media*. *But see* Oregon Bar Ass'n, Formal Op. No. 2013-189, *Accessing Information About Third Parties Through a Social Networking Site* (2013) (lawyer contacting unrepresented person need not identify herself as an attorney so long as she provides her true name, unless lawyer has reason to believe that the unrepresented person misunderstands lawyer's role); NY City Bar, Formal Op. 2010-02, *Obtaining Evidence from Social Networking Websites* (NY policy encourages "informal discovery" yet ethics rules bar deception: "consistent with the policy, we conclude that an attorney or her agent may use her real name and profile to send a 'friend request' to obtain information from an unrepresented person's social networking website without also disclosing the reasons for making the request" but may not engage in "trickery").

[203] *See* Massachusetts Bar Ass'n, Comm. on Prof'l Ethics, Op. 2014-5 ("We also do not agree with the suggestion in Formal Opinion 2010-2 of the New York City Bar Association's Committee that the lawyer's identification message may be contained in a 'profile' created on the lawyer's personal social media page.").

[204] *See, e.g.*, New Hampshire Bar Ass'n, Ethics Committee Advisory Opinion #2012-13/05, *Social Media Contact with Witnesses in the Course of Litigation*; Oregon Bar Ass'n, Formal Op. No. 2013-189, *Accessing Information About Third Parties Through a Social Networking Site* (2013) ("If Lawyer has actual knowledge that the holder of the account is represented by counsel on the subject of the matter, Oregon RPC 4.2 prohibits Lawyer from making the request except through the person's counsel or with the counsel's prior consent."); *see also* Massachusetts Bar Ass'n, Comm. On Prof'l Ethics, Op. 2014-5 (noting that ethics obligations rules may change if the individual being contacted obtains counsel following the initial contact).

[205] *See August 2012 Amendments to ABA Model Rules, Rule 1.1* (providing in commentary that an attorney's duty of competence requires an attorney "[t]o maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology . . . [.]") (emphasis in original); New Hampshire Bar Ass'n, Ethics Committee Advisory Opinion #2012-13/05, *Social Media Contact with Witnesses in the Course of Litigation* (recognizing attorneys' conflicting duties of competence and diligence, and truthfulness and fairness in dealing with others, in the context of social media use).

[206] See *Cannedy v. Adams*, 706 F.3d 1148 (9th Cir. 2013) (lawyer provided ineffective assistance of counsel when he failed to interview witness who notified him that alleged sex abuse victim had recanted on a social media platform, and failed to seek to admit evidence of victim's motive to lie in a case based on witness testimony and no forensic evidence).

[207] In criminal litigation, the majority of evidence, electronic or otherwise, is collected by the government prior to indictment and Federal Rule of Criminal Procedure 16 does not require the government to produce such evidence unless it is being used in their case-in-chief.

[208] *Id.*

[209] Fed. R. Crim. P. 17(e)(1).

that information without the consent of the owner of the account.[210] In one high profile example of the hurdles faced by defendants, on October 19, 2012, the court presiding over the Trayvon Martin murder trial granted the defendant's motion seeking permission to subpoena Facebook and Twitter for the records of Trayvon Martin's social media accounts, as well as Mr. Martin's girlfriend's Twitter account.[211]

Still, criminal defendants may attempt to use novel methods of obtaining exculpatory social media evidence. For example, a law enforcement officer's social media account records may be obtained under *Brady v. Maryland* or *Giglio v. United States*.[212] Moreover, courts may order jurors, witnesses, or third parties to produce or manipulate their social media information in unique and unprecedented ways. Courts have, for example: (1) ordered a juror to "execute a consent form sufficient to satisfy the exception" in the SCA to allow Facebook to produce the juror's wall posts to defense counsel;[213] (2) ordered a party to briefly change his Facebook profile to include a prior photograph so that his Facebook pages could be printed as they existed at a prior time;[214] (3) recommended that an individual "friend" the judge on Facebook in order to facilitate an *in camera* review of Facebook photos and comments;[215] and (4) ordered parties to exchange social media account user names and passwords."[216] Such novel avenues of access to social media evidence may be considered where the defendant subpoenas a social media provider for certain records of a witness or victim and the social media company objects to the subpoena pursuant to the SCA or is unable to produce the evidence as it previously existed.

Admissibility of Social Media Evidence

Social media is subject to the same rules of evidence as paper documents or other electronically stored information, but the unique nature of social media—as well as the ease with which it can be manipulated or falsified[217]—creates hurdles to admissibility not faced with other evidence. The challenges surrounding social media evidence demand that one consider admissibility when social media is preserved, collected, and produced. It is important for counsel to memorialize each step of the collection and production process and to consider how counsel will authenticate a Tweet, Facebook posting, or photograph—for example, by presenting a witness with personal knowledge of the information (they wrote it, they received it, or they copied it), by searching the computer to see if the computer was used to post or create the information, or by attempting to obtain the information in question from the social media company that maintained the information in the ordinary course of their business.

---

[210] 18 U.S.C. § 2703.

[211] Erin Fuchs, *A Jury Will Likely Scrutinize Trayvon Martin's Deleted Facebook and Twitter Accounts* (Oct.19, 2012), http://www.businessinsider.com/zimmerman-can-subpoena-social-media-2012-10.

[212] *See* Brady v. Maryland, 373 U.S. 83 (1963); Giglio v. United States, 405 U.S. 150 (1972).

[213] Juror Number One v. California, No. CIV. 2:11-397 WBS JFM, 2011 WL 567356, at *1 (E.D. Cal. Feb. 14, 2011).

[214] Katiroll Co. v. Kati Roll and Platters, Inc., 2011 WL 3583408, at *4 (D.N.J. Aug. 3, 2011).

[215] Barnes v. CUS Nashville, LLC, No. 3:09-CV-00764, 2010 WL 2265668, at *1 (M.D. Tenn. June 3, 2010).

[216] *See, e.g.*, Gallion v. Gallion, No. FA114116955S, 2011 WL 4953451, at *1 (Conn. Super. Ct. Sept. 30, 2011) (ordering parties to exchange passwords to Facebook and a dating website); McMillen v. Hummingbird Speedway, Inc., No. 113-2010 CD, 2010 WL 4403285 (Pa. Com. Pl. Sept. 9, 2010) (ordering plaintiff to produce Facebook and MySpace login credentials to opposing counsel for "read-only access").

[217] *See, e.g.*, Griffin v. State, 19 A.3d 415, 424 (Md. 2011) (collecting cases similarly recognizing "[t]he potential for abuse and manipulation of a social networking site by someone other than its purported creator").

Notably, the government faces these same challenges, and must consider admissibility of social media when it conducts an investigation. In *United States v. Stirling*, the government seized the defendant's computer pursuant to a search warrant and provided the defendant with a forensic copy of the hard drive.[218] The government also performed a forensic examination of the hard drive and extracted 214 pages of Skype chats downloaded from the defendant's computer—chats that were not "readily available by opening the folders appearing on the hard drive"—but did not provide this information to the defense until the morning of its expert's testimony near the end of trial.[219] The logs "had a devastating impact" on the defendant because they contradicted many of his statements made during his testimony, and he was convicted.[220] In a short but stinging opinion ordering a new trial, the court found:

> [If a defendant] needs to hire a computer forensics expert and obtain a program to retrieve information not apparent by reading what appears in a disk or hard drive, then such a defendant should so be informed by the Government, which knows of the existence of the non-apparent information. In such instance, and without the information or advice to search metadata or apply additional programs to the disk or hard drive, production has not been made in a reasonably usable form. Rather, it has been made in a manner that disguises what is available, and what the Government knows it has in its arsenal of evidence that it intends to use at trial.[221]

While both government and defense attorneys grapple with addressing and authenticating social media sources of evidence, state courts addressing the issue have largely erred on the side of admissibility, leaving jurors to resolve concerns about the evidence itself (such as who authored the evidence or whether the evidence is legitimate) when deciding the *weight* that the evidence should be given. Social media evidence has repeatedly been ruled admissible where the content of the evidence is found to contain sufficient indicia that it is the authentic creation of the purported user.[222] In *Tienda v. State*,[223] for example, the appellant was convicted of murder based in part on evidence obtained by the prosecutors after subpoenaing MySpace. Specifically, "the State was permitted to admit into evidence the names and account information associated with [the defendant's MySpace.com profiles], photos posted on the profiles, comments and instant messages linked to the accounts, and two music links posted to the profile pages."[224] The Court of Criminal Appeals affirmed the trial judge and concluded that the MySpace profile exhibits used at trial were admissible because there were "sufficient indicia of authenticity" that "the exhibits were what they purported to be – MySpace pages the contents of which

---

[218] Order on Defendant's Motion for New Trial, United States v. Stirling, No. 1:11-cr-20792-CMA, slip op. at 2 (S.D. Fla. June 5, 2012).
[219] *Id.* at *2.
[220] *Id.*
[221] *Id.* at *4-5.
[222] See, e.g., People v. Lesser, No. H034189, 2011 WL 193460, at *4 (Cal. Ct. App. Jan. 21, 2011) (finding that officer's testimony that he cut and pasted portions of internet chat transcript was sufficient for admissibility); People v. Valdez, No. G041904, 135 Cal. Rptr. 3d 628, 633 (Cal. Ct. App. 2011) (upholding conviction where the court correctly admitted a trial exhibit consisting of printouts of defendant's MySpace page, which the prosecution's gang expert relied on in forming his opinion that defendant was an active gang member); People v. Fielding, No. C06022, 2010 WL 2473344, at *4-5 (Cal. Ct. App. June 18, 2010) (incriminating MySpace messages sent by defendant authenticated by victim who testified that he believed defendant had sent them; inconsistencies and conflicting inferences regarding authenticity goes to weight of evidence, not its authenticity).
[223] Tienda v. State, 358 S.W.3d 633, 634-35 (Tex. Crim. App. 2012).
[224] *Id.* at 635.

the appellant was responsible for."[225] In *Campbell v. Texas*,[226] prosecutors introduced Facebook messages prosecuting an aggravated assault. The messages, which were sent from the defendant's account, stated that he regretted striking his girlfriend and asked for her forgiveness. Although the defendant denied sending the messages and argued that both he and his girlfriend had access to each other's Facebook accounts, and although the court acknowledged that electronic communications are "susceptible to fabrication and manipulation," the court nevertheless allowed the messages to be authenticated through circumstantial evidence, including most notably evidence that the messages were sent from the defendant's account and the girlfriend's testimony that she had not sent the messages.[227]

The first federal circuit court to address the admissibility of social media evidence took a harder line this year, however, in *United States v. Vayner*.[228] The court vacated a conviction for unlawful transfer of a false identity, finding that the conviction was based on improperly authenticated social media evidence. There, the government had sought to admit a printout of a Russian social media profile page containing information that linked the defendant to the email address that was allegedly used to transfer the false identity. The court found that the social evidence media evidence was insufficiently authenticated where the government offered no evidence that any identify verification was necessary to create a profile, that the defendant had or used a profile on the site, or that the profile contained information known only by the defendant (or more importantly not known to others who might have an incentive to create a false profile for defendant). The court concluded that "Rule 901 required that there be *some* basis beyond [a co-conspirator's] testimony on which a reasonable juror could conclude that the page in question was not just any Internet page, but in fact *[defendant's]* profile. No such showing was made and the evidence should therefore have been excluded."[229] Moreover, the error was not harmless since the evidence was central to the prosecution's case.

The Second Circuit's closer look at admissibility of social media evidence is significant in light of the widespread use of such evidence in criminal litigation. Indeed, looking forward, given the proliferation of social media, the increasing sophistication of technology, and the potential challenges relating to the reliability or authentication of social media data, the authentication and admissibility of such evidence will likely be the subject of vigorous disputes between parties that may mean the difference between conviction or acquittal.

---

[225] *Id.* at 647.

[226] Campbell v. Texas, No. 03-11-00834-CR, 2012 WL 3793431, at *1 (Tex. App. Aug. 31, 2012).

[227] *Id.* at *4. In yet another instance, a federal court held that photographs of a defendant from his MySpace page, which depicted him holding cash, were relevant in his criminal trial for possession of firearms and drugs but withheld ruling on the admissibility of the photos and whether they presented a risk of unfair prejudice. United States v. Drummond, No. 1:09-cr-00159, 2010 WL 1329059 at *2-3 (M.D. Pa. March 29, 2010). The defendant ultimately entered a guilty plea and there was no final ruling by the court on the admissibility of the photographs.

[228] United States v. Vayner, 769 F.3d 125 (2d Cir. Oct. 3, 2014). The Ninth Circuit also provides helpful guidance on the types of circumstantial evidence that may be used to authenticate social media evidence in *Cannedy*, 706 F.3d at 1164.

[229] *Id.* at *133.