CHAPTER 7

E-DISCOVERY IN GOVERNMENT INVESTIGATIONS AND CRIMINAL LITIGATION

Justin P. Murphy and **Louisa K. Marion**

Electronically stored information ("ESI"), for clients, prosecutors, and defense attorneys, continues to grow into a tsunami of cost, challenges, and complexity – with little clear guidance from courts and none from the rules. Moreover, the paradigms developed in civil litigation to curb ESI discovery abuses are often not effective 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. 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 some other government demand are obvious triggers, but 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. Sentencing Guidelines § 8C2.5.

Importantly, preservation failures can also expose a defendant to additional investigation for obstruction of justice. 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.

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*,[4] the government failed to preserve numerous text messages exchanged between a key cooperating witness and FBI agents involved in a public corruption investigation.[5] 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.[6] The court declined, however, to suppress other text messages introduced by the Government, absent a showing that the Government deleted the missing text messages in bad faith.[7] The jury nevertheless acquitted the defendant, who argued that the missing text messages were important.[8]

The Ninth Circuit went further in *United States v. Sivilla*,[9] 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."[10] 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."[11] 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.[12] Finding that the prejudice to the defendant 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.[13]

---

[4] United States v. Suarez, No. 09-932 (JLL), 2010 WL 4226524 (D.N.J. Oct. 21, 2010).
[5] *Id.* at *1.
[6] *Id.* at *8.
[7] *Id.* at 7.
[8] *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).
[9] United States v. Sivilla, 714 F.3d 1168 (9th Cir. 2013).
[10] *Id.* at 1173.
[11] *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).
[12] 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. *Sivilla,* 714 F.3d at 1174.
[13] 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

While spoliation sanctions are increasingly common in civil litigation, it is uncommon for such conduct to be charged as criminal obstruction of justice.[14] 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 have been 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 unique challenges presented by the nature of ESI create problems in the context of search warrants. Specifically, the modern day phenomenon of vast amounts of intermingled data has collided with the Fourth Amendment's search and seizure strictures enshrined by the founders hundreds of years ago. On the one hand, computers can store virtually unlimited state, 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 arise 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 have questioned 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 document containers, such as filing cabinets, or personal papers and effects.

---

under Supreme Court precedent in *Arizona v. Youngblood*, 488 U.S. 51 (1988). *See Sivilla,* 714 F.3d at 1172.

[14] 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).

A. The Ninth Circuit's Standards

Two decisions by the Ninth Circuit in the *Comprehensive Drug Testing* matter have 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.[15] 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."[16] 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 . . . ."[17] 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.[18]

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.[19] 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

---

[15] *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).
[16] *Id.* at 998.
[17] *Id.* at 1006.
[18] *Id.*
[19] *See* United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1177-1180, 1183 (9th Cir. 2010).

over-seizing of evidence outlined in its prior decision in *United States v. Tamura*.[20] Adhering to its ruling in *Tamura*, the Ninth Circuit applied a two-step process. First, a 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.[21] 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."[22] 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."[23]

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."[24]

The *Comprehensive Drug Testing* decisions represent 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."[25]

B. 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. 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.[26] In affirming the district court's determination that a warrant application failed to establish probable cause, the panel noted that:

---

[20] 694 F.2d 591 (9th Cir. 1982). *See Comprehensive Drug Testing, Inc.,* 621 F.3d at 1180.
[21] 621 F.3d at 1169, 1171.
[22] *Id.* (quoting *Tamura*, 694 F.2d at 596).
[23] *Id.* at 1177.
[24] *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).
[25] *Id.* at 1176.
[26] United States v. Galpin, No. 11-4808-cr at 16 (2d Cir. June 25, 2013).

> 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 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.[27]

Another example is *United States v. Richards*,[28] 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."[29]

The Sixth Circuit applied "the Fourth Amendment's bedrock principle of reasonableness on a case-by-case basis,"[30] 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.[31] 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.[32] Judge Moore highlighted that the FBI agents 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.[33] 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."[34]

The Third Circuit's opinion in *United States v. Stabile* also addresses the issue of "over-seizure" of evidence under the plain view doctrine.[35] In *Stabile*, agents went to the

---

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

defendant's home to question him regarding allegations that he was involved in counterfeiting and other financial crimes.[36] 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.[37] The agents seized several computer hard-drives from the home, and discovered child pornography on the hard-drives.[38] While the court in *Stabile* declined to follow the Ninth Circuit's suggestion in *Comprehensive Drug Testing*[39] 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."[40] 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.'"[41]

Few federal appeals courts have flatly disagreed with the *Comprehensive Drug Testing* decision. In *United States v. Williams*,[42] 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.[43] 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.[44] 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."[45]

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. For example, a magistrate judge in the District of Columbia who is widely respected for his e-discovery expertise issued a written opinion rebuffing the government's request for authority to seize computer data because it had not made a sufficiently specific showing that the target's computer was related to the alleged crime.[46] The judge expressed his concern that under these circumstances a "forensic search of [the computer's] entire contents . . . appears to me to be the very general search that the 4th Amendment prohibits."[47]

---

[36] *Id.* at 224.
[37] *Id.* at 225.
[38] *Id.*
[39] Comprehensive Drug Testing, 621 F.3d at 1178 (Kozinski, CJ, concurring).
[40] *Id.* at 241.
[41] *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 at 785. 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.*
[42] United States v. Williams, 592 F.3d 511, 515-517 (4th Cir. 2010).
[43] *Id.* at 521-522.
[44] *Id.* at 522.
[45] *Id.*
[46] In re Application for Search Warrant, Mag. No. 09-320 (D.D.C. June 3, 2009) (Facciola, M.J.).
[47] *Id. See also* United States v. Payton, 573 F.3d 859, 864 (9th Cir. 2009) (suppressing evidence

C. Time Limits on the Search of Data Seized Pursuant to a Warrant

Courts have also found that the government must take 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.[48] Although 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. Although the court noted that delays of several months have been found to be reasonable, there was no available guidance as to when a delay becomes presumptively unreasonable. The court found that:

> 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.[49]

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.[50]

The impact of this decision could be significant: The government is on notice that it must do something with lawfully seized evidence in a reasonable amount of time. And at least one court has determined that "reasonable" falls somewhere between a few and 15 months.

III. INVESTIGATIONS: WARRANTLESS SEARCHES & SEIZURES OF ESI

A. Warrantless Searches of Cellular Telephones

As of December 2011, there were more mobile phones than people in the United States.[51] The proliferation of smart phones has fed another important and developing issue relating to ESI in government investigations and criminal litigation: the warrantless searches of mobile phones incident to a lawful arrest. Federal courts are divided on the issue of when and whether a warrant is required to search the data in a cellular telephone

---

resulting from search of computer where there was "no . . . evidence pointing to the computer as a repository for the evidence sought in the search.").

[48] *U.S. v. Metter*, No. 10–CR–600 (DLI) (E.D.N.Y May 17, 2012).

[49] *Id.*

[50] *Id.*

[51] Number of cellphones exceeds U.S. population: CTIA trade group, Cecilia Kang, *The Washington Post*, October 11, 2011.

following an arrest, prompting the Supreme Court to grant cert petitions in early 2014.[52]

Several Circuits and state courts have concluded that law enforcement may retrieve text messages and other information from cellular phones seized and searched incident to a lawful arrest.[53] In *People v. Diaz,*[54] the California Supreme Court affirmed the denial of a motion to suppress a text message found on a defendant's cellular telephone. There, a detective witnessed the defendant participate in a controlled drug buy, arrested him, and seized his cellphone from his person.[55] Approximately 90 minutes after the defendant's arrest the detective "looked at the cell phone's text message folder and discovered a message" that was incriminating, at which point the defendant confessed.[56] The *Diaz* court found that the cellphone was personal property immediately associated with the defendant's person, and therefore, the search was valid despite the 90–minute lapse in time between the cellphone being seized and being searched.[57] Relying on *Diaz* in *People v. Riley*,[58] the Fourth District Court of Appeal likewise affirmed a denial of a suppression motion where police searched a cellphone "immediately associated with [the defendant's] person" and incident to his arrest, and seemingly reviewed contacts, video clips, and photographs. *Riley* is one of the two cases in which the Supreme Court granted cert in January 2014.

Other courts have invalidated warrantless searches of cellular phones seized incident to arrest.[59] In the other case in which the Supreme Court granted cert early this year, *United States v. Wurie*,[60] the First Circuit held "that the search-incident-to-arrest

---

[52] United States v. Wurie, 728 F.3d 1 (1st Cir. 2013), *cert granted* Jan. 17, 2014; 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).

[53] *See, e.g.,* United States v. Finley, 477 F.3d 250, 259-60 (5th Cir. 2007) (noting that "[t]he permissible scope of a search incident to a lawful arrest extends to containers found on the arrestee's person," and declining to suppress text messages and call records obtained during a warrantless search of a cell phone incident to a lawful arrest); United States v. Ochoa, No. 10–51238, 2012 WL 104997 (5th Cir. Jan. 13, 2012) (upholding warrantless search of cell phone in impounded vehicle where officers reasonably believed that they had probable cause to arrest defendant and the information found during the search of defendant's cell phone would have been inevitably discovered during the inventory of his car); United States v. Murphy, 552 F.3d 405, 411 (4th Cir. 2009); United States v. Hill, No. CR 10-0026 (JSW) 2011 WL 90130 at *7 (N.D. Cal. Jan. 10, 2011) (affirming the warrantless search of a cell phone because it was contemporaneous to the arrest); *United States v. Deans,* 549 F. Supp. 2d 1085, 1094 (D. Minn. 2008) (agreeing with the Fifth Circuit that "if a cell phone is lawfully seized, officers may also search any data electronically stored in the device."); United States v. Santillan, 571 F. Supp. 2d 1093, 1102-03 (D. Ariz. 2008).

[54] People v. Diaz, 244 P.3d 501 (Cal. 2011).

[55] *Id.* at 502.

[56] *Id.*

[57] *Id*. at 506. Notably, in reaction to *Diaz*, the California state legislature passed a cell-phone privacy bill that would have required officers to obtain a warrant before searching the device, but this bill was vetoed by Governor Jerry Brown. *See* Senate Bill 914.

[58] 2013 WL 475242, at *6.

[59] *See, e.g.,* United States v. Quintana, 594 F. Supp. 2d 1291, 1301 (M.D. Fla. 2009); *United States v. McGhee,* No. 8:09-C-R31, 2009 WL 2424104, at *3-4 (D. Neb. July 21, 2009); *United States v. Wall,* No. 08-60016-CR, 2008 WL 5381412, at *3 (S.D. Fla. Dec. 22, 2008); United States v. Park, No. 05-CR-375-SI, 2007 WL 1521573, at *1 (N.D. Cal. May 23, 2007) (search of a cell phone an hour after the arrest was suppressed).

[60] 728 F.3d 1.

exception does not authorize the warrantless search of data on a cell phone seized from an arrestee's person" under any circumstances[61] (yet noted that other exceptions – such as the exigent circumstances exception – might permit such a search).[62] Although the search of Wurie's phone appears to have been quite limited – with police officers reviewing the phone's wall paper, recent call log, and the phone number associated a caller who had called numerous times while the phone was being held – the courtly expressly eschewed a fact-specific approach in favor of an easily applied, bright-line rule, which it asserted is favored by the Supreme Court's Fourth Amendment jurisprudence.[63]

The First Circuit panel explained that it was "not suggesting a rule that would require arresting officers or reviewing courts to decide, on a case-by-case basis, whether a particular cell phone data search is justified under [existing law]. [Rather, it] believe[d] that warrantless cell phone data searches are *categorically* unlawful under the search-incident-to-arrest exception, given the government's failure to demonstrate that they are ever necessary to promote officer safety or prevent the destruction of evidence[.]"[64] (Although the court conceded there were instances in which a search of a cell phone might be necessary to protect officer safety – e.g., a search to confirm the phone was not a weapon – this rationale would not necessarily permit a more intrusive search into the phone's contents.)[65] The court further noted that "warrantless cell phone data searches str[uck] [the court] as a convenient way for the police to obtain information related to a defendant's crime of arrest—or other, as yet undiscovered crimes—without having to secure a warrant,"[66] and, in the court's opinion, "nothing in the Supreme Court's search-incident-to arrest jurisprudence . . . sanction[ed] such a 'general evidence gathering search.'"[67]

In reaching its conclusion, the court underscored the changed nature of cell phones, the data they contain, and the U.S. population's expectations of privacy in such devices. The court stated that it suspected that the U.S. cell-phone owning population "would have some difficulty with the government's view that [the defendant's] cell phone was indistinguishable from other kinds of personal possessions, like a cigarette package, wallet, pager, or address book" subject to the search-incident-to-arrest exception to the warrant requirement.[68] It further noted that modern cell phones have "immense" storage capacity, contain data of a "highly personal nature," and may provide access to far more than local data (e.g., data in the Cloud or a videostream of a home webcam that could quickly transform a phone search into a house search).[69]

---

[61] *Id.* at 12-13.
[62] *Id.* at 13.
[63] 728 F.3d 1, 6-8 (1st Cir. 2013).
[64] *Id.* at 12. The court was unconvinced by the Government's argument that such searches may be necessary to prevent the destruction of evidence, since there are numerous ways to prevent the "wiping" of devices. The court explained: "Indeed, if there is a genuine threat of remote wiping or overwriting, we find it difficult to understand why the police do not routinely use these evidence preservation methods, rather than risking the loss of the evidence during the time it takes them to search through the phone." *Id.* at 10-11.
[65] *Id.* at 10.
[66] *Id.* at 12-13.
[67] *Id.* at 13.
[68] *Id.* at 8.
[69] *Id.* at 8-9.

The First Circuit's denial of the government's petition for *en banc* review of the *Wurie* decision is especially noteworthy. There, Chief Judge Lynch noted that the case clearly merited *en banc* review, but he voted to deny such a rehearing "because I think the preferable course is to speed this case to the Supreme Court for its consideration. . . . The decision in this case creates a circuit split with respect to the validity of warrantless searches of cell phones incident to arrest. State courts similarly are divided. As the government points out, the differing standards which the courts have developed provide confusing and often contradictory guidance to law enforcement. . . . Only the Supreme Court can finally resolve these issues and I hope it will."[70]

Even other courts have applied a more nuanced approach, finding only limited searches permissible. For example, a district court in Florida[71] tempered its decision permitting officers to search the contents of a cellular telephone as a "search incident to arrest," by explaining:

> To be clear, we do not suggest that the search incident to arrest exception gives agents carte blanche to search indefinitely each and every facet of an arrestee's cell phone. After all, a search incident to arrest must always fall within the reasonableness requirement of the Fourth Amendment and, more narrowly, relate to the evidence of the underlying offense or arrest. Courts applying this exception must also do so in a manner that faithfully enforces the temporal and spatial requirements of the doctrine. By doing so, the scope of a search will be limited as a practical matter. In the case of a cell or smartphone, for instance, a search contemporaneous with an arrest would not possibly allow a law enforcement officer at the scene of an arrest from downloading the entire content of the phone's memory. It would not allow much more than what occurred here—a short, limited perusal of only recent calls to quickly determine if any incriminating evidence relevant to this drug crime can be identified.
>
> It should also be noted that, when a search incident to arrest goes beyond the strict temporal and spatial requirements of the doctrine, a different rule must govern. If officers do not contemporaneously search a cell phone, and instead seize it for later review at the station house the subsequent search could not and should not be deemed incident to arrest.[72]

Similarly, in *Hawkins v. State*, the Georgia Supreme court noted, in upholding a search of the defendant's mobile phone incident to a lawful arrest, that

> the fact a large amount of information may be in a cell phone has substantial import as to the scope of the permitted search; it requires that we must apply the principles set forth in the traditional container cases for searches for electronic data with great care and caution." The court noted this will usually mean that an officer may not conduct a fishing expedition and sift through all of the data stored in the cell phone. Thus, when the object of the search is to

[70] United States v. Wurie, No. 11-1792 (1st Cir, July 29, 2013).
[71] United States v. Gomez, No. 11-20304-CR, 2011 WL 3841071, at *8 -12 (S.D. Fla. 2011).
[72] *Id.* at *12.

> discover certain text messages, there is no need for the officer to sift through photos or audio files or internet browsing history data stored in the phone.[73]

The Supreme Court's review of *Wurie* and *Riley* will hopefully provide some clarity to the muddied questions surrounding the constitutionality of warrantless cell phone searches in its coming term.

B. Warrantless Collection of Real-Time and Historic Geolocational Information

Courts have equally struggled to define the bounds of the Fourth Amendment as applied to technologies that track, trace, and record geolocational information. Although the Supreme Court has provided clear guidance that attaching a global positioning system ("GPS") unit to a criminal suspect's car constitutes a "search,"[74] it has remained silent on many other key questions arising in the context of geolocational information – including whether such a search always requires a warrant, whether the Fourth Amendment protects geolocational information created and stored by common technologies like cell phones and car GPSs, 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.[75]

C. GPS Tracking Devices

As noted, in its only treatment of geolocational privacy, 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.[76] The underlying case[77] involved two nightclub owners in the District of Columbia (Antoine Jones and Lawrence Maynard) who were under investigation for narcotics violations.[78] During the investigation, officers attached a GPS device to Jones's vehicle without a warrant.[79] The GPS device tracked Jones's movements 24 hours a day for one month.[80] The D.C. Circuit found that the use of GPS to track the defendant's movements around the clock for an entire month, without a warrant, violated the Fourth Amendment.[81] The court explained that "[p]rolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each

---

[73] 723 S.E.2d 924 (Ga. 2012). *See also* United States v. Shanklin, No. 2:12-cr-00162-RAJ-DEM (E.D. Va. Nov. 13, 2013) (granting motion to suppress evidence where law enforcement searched photos on defendant's cell phone beyond consent given to investigate text messages).
[74] *See* United States v. Jones, 132 S. Ct. 945 (2012).
[75] 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).
[76] *Id.*
[77] United States v. Maynard, 615 F.3d 544, 559 (D.C. Cir. 2010).
[78] *Id.* at 549.
[79] *Id.* at 558–59.
[80] *Id.*
[81] *Id.* at 559.

reveal more about a person than does any individual trip viewed in isolation."[82]

In *United States v. Jones*, the Supreme Court affirmed, but on narrower grounds. Writing for the Majority, Justice Scalia found the installation of a GPS monitoring device to be a search, but noted that it "is important to be clear about what occurred in this case: The government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted."[83] Thus, the installation of the GPS constituted a search because it was a trespass on the defendant's car. However, the opinion continued, asserting that "our cases suggest that [extensive] visual observation is constitutionally permissible," and that "[i]t may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question."[84]

Importantly, the Court declined to address whether the installation of GPS is a search that *requires* a warrant. At least four members of the Court suggested, however, that long-term monitoring of a GPS device would necessitate a warrant. Justice Alito's concurrence (joined by Justices Ginsburg, Breyer, and Kagan) advocated for a different test than Justice Scalia's trespass approach, arguing that the Court should analyze whether GPS monitoring intrudes on an expectation of privacy that society recognizes as reasonable: "Under this approach, relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. . . . . But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, 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."[85]

Ultimately, the *Jones* decision raises more questions than it answers, failing to find even that a warrant is required to install a GPS device. The Court's reluctance to "grapple with these 'vexing problems'"[86] highlights the continued challenges we face as technologies increasingly narrow our realms of privacy.

At least two courts sought to fill one of voids left by *Jones* decision, holding that the Fourth Amendment indeed requires law enforcement agents to obtain search warrant before using a GPS device to monitor a suspect's vehicle. In *State v. Brereton*,[87] the police obtained a warrant to install a GPS tracking device on the car of a suspect believed to be

---

[82] *Id.* at 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*, described 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 curtillage of the home)).

[83] United States v. Jones, 132 S. Ct. 945 (2012).

[84] *Id.* at 954.

[85] *Id.* at 964.

[86] *Id.* at 954.

[87] State v. Brereton, 2013 WL 440512, No. 2010AP1366–CR (Wis. Feb. 6, 2013).

involved in a number of robberies. The GPS device provided the location of the suspect's vehicle to the officers, and eventually led to the arrest of the suspect with stolen merchandise from a recent robbery.

The defendant moved to suppress the GPS evidence against him. Although the Wisconsin Supreme Court declined to suppress the evidence, it found that the use of a GPS device to collect a suspect's location was a search for Fourth Amendment purposes, on ground broader than those asserted in *Jones*. The court stated:

> 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.' *Id*. at 954–55 (Sotomayor, J., concurring) (quoting *Kyllo v. United States*, 533 U.S. 27, 33 (2001)). 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.'[88]

Therefore, the court concluded "that the decision to install a GPS device on [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."[89]

In 2013, in an opinion now vacated pending rehearing *en banc*,[90] 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, in *United States v. Katzin*.[91] Noting 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," the court considered whether any such exceptions permitted the GPS tracking of a burglary suspect for two days.[92] The court concluded that Katzin's was not a case in which a "special need" other than the need "to uncover evidence of ordinary criminal wrongdoing" permitted a search based merely on the police's reasonable suspicion that he was engaged in criminal activity.[93] Nor was the search authorized by *Terry* and its progeny, where the search involved ongoing surveillance as opposed to a less intrusive stop-and-frisk.[94] Finally, the court considered whether the automobile exception – which permits warrantless searches of any part of a vehicle, where there is probable cause to believe that that part of the vehicle

---

[88] *Id.* at *8.
[89] *Id.* at *10.
[90] *See* United States v. Katzin, No. 12-2548, Order Granting Re-Hearing En Banc, dated Dec. 12, 2013.
[91] 732 F.3d 187 (3d Cir. 2013).
[92] *Id.* at 197.
[93] *Id.* at 198-99.
[94] *Id.* at 200-01.

conceals evidence of a crime – permitted the GPS search.[95] The court found the exception was "inapposite" to ongoing police tracking aimed not at "recover[ing] or ascertain[ing] the presence of evidence already present in [the defendant's] vehicle, but rather "creat[ing] a continuous police presence for the purpose of discovering evidence that may come into existence and/or be placed within the vehicle at some point in the future."[96] Ultimately, the court held that "the police must obtain a warrant prior to a GPS search."[97]

Significantly, the Third Circuit also concluded in *Katzin* that the police's failure to obtain a warrant could not be excused by "good faith," and thus the exclusionary rule barred admission of evidence obtained through the surveillance.[98] Noting that the good faith exception to the exclusionary rule as set forth in *Davis v. United States* requires that "the police rel[y] on binding appellate precedent that '*specifically authorize[s]* [the] particular police practice,"[99] the court concluded that no such precedent did so here: Neither of the cases most closely on point – *United States v. Knotts*[100] and *United States v. Karo*[101] – "involved a physical trespass onto the target vehicle; in both cases the police placed the beeper inside of a container which was then loaded into the target vehicle by the driver (all with the container owner's permission). Additionally, both *Karo* and *Knotts* addressed the use of beepers, which [the court concluded were] markedly different from GPS trackers."[102] Nevertheless, as noted, the Third Circuit has granted *en banc* review of *Katzin*, which is scheduled for May 2014.

At least one state court considering the question of whether the good-faith exception permits admission of GPS evidence obtained pre-*Jones* reached a contrary conclusion to the Third Circuit in *Katzin*. In *Kelly v. State of Maryland*,[103] the Maryland Court of Appeals admitted evidence obtained through 11 days of warrantless GPS surveillance, finding that *Knotts* constituted binding appellate precedent permitting the use of a GPS device to track a vehicle moving on public streets. Unlike the Third Circuit, the Maryland Court of Appeals concluded that the "binding precedent [under *Davis*] does not require that there be a prior appellate case directly on point, *i.e.,* factually the same as the police conduct in question."[104] The court determined that, had it considered the constitutionality of the search in question pre-*Jones*, it would have applied *Knotts* and found the search constitutional – and thus so too could law enforcement reasonably rely on *Knotts* (pre-*Jones*) to conclude the attachment of a GPS to the bottom of a car was constitutional.[105] On this basis, the court found that the good-faith exception applied.

---

[95] *Id.* at 202-04.
[96] *Id.* at 204.
[97] *Id.* at 191.
[98] *Id.*
[99] *Id.* at 207 (emphasis in original).
[100] 460 U.S. 276 (1983).
[101] 468 U.S. 705 (1984).
[102] 732 F.3d at 207.
[103] No. 26, Sept. Term 2013 (Md. Dec. 23, 2013).
[104] *Id.* at *19.
[105] *Id.* at *19-20.

D. Cell-Site Tracking & Other "Business Records" Collection

In 2013, the Fifth Circuit held that a warrant is not required for the government to obtain cell-site information, noting that cell phone users do not have a reasonable expectation of privacy regarding their location when making a cell phone call because they have voluntarily transmitted that information to the cell phone service provider.[106] There, the government 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. The Fifth Circuit, reversing the lower court, ruled that the Fourth Amendment is not violated when the government obtains historical cell-site data for specific phones without probable cause. The court focused on *who* collects the information and for what ends; in this case, the cell phone service providers collect the information for their own business purposes. The court also rejected arguments comparing cell-site data to a "tracking device," finding that the government is not causing the initial collection of the data, nor is it requesting the service providers to collect it or retain it. Rather, the court argued the government is seeking access to existing business records.

The Sixth Circuit likewise upheld cell-site tracking in *United States v. Skinner*,[107] albeit on different grounds. There, the court found that a defendant does not have a reasonable expectation of privacy in location data emitted by a cell phone used voluntarily and on public streets.[108] Relying primarily on *United States v. Knotts*,[109] the court concluded that the cell-site data obtained by pinging the 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."[110] 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.[111] The court explained:

> In all three instances [in which the defendant was tracked using cell-site data,] [his] movements could have been observed by any member of the public . . . . As for not knowing his identity, this is irrelevant because the agents knew the identity of [defendant's] co-conspirators and could have simply monitored their whereabouts to discover Skinner's identity. Using a more efficient means of discovering this information does not amount to a Fourth Amendment violation. In any event, we determine whether a defendant's reasonable expectation of privacy has been violated by looking at what the defendant is disclosing to the public, and not what information is known to the police.[112]

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

---

[106] In Re: Application Of The United States Of America For Historical Cell Site Data, Case No. 11-20884 (5th Cir. July 30, 2013).
[107] United States v. Skinner, 690 F.3d 772, 777 (6th Cir. 2012), *cert. denied*, 133 S. Ct. 2851 (2013).
[108] *Id.* at 781.
[109] 460 U.S. 276 (1983).
[110] 690 F.3d at 778.
[111] *Id.* at 779.
[112] *Id.*

contraband gives off a signal that can be tracked for location, certainly the police can track the signal."[113] Finally, the court distinguished *Jones* on the basis that, here, there was no physical trespass on the defendant's property, since the defendant had "himself obtained the cell phone [with GPS capabilities] for the purpose of communication," nor "extreme comprehensive tracking," where police tracked Skinner for three days (as compared to 28 days of tracking in *Jones*).[114]

E. Electronic Searches at the Border

The Ninth Circuit this year revisited the long-standing rule permitting suspicion-less searches at the U.S. border in *United States v. Cotterman*.[115] In what it called a "watershed case," the Ninth 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.[116]

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.[117] 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."[118] 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."[119] 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). The Supreme Court denied Cotterman's petition for a writ of certiorari in January 2014.

---

[113] *Id.* at 777-78.
[114] *Id.* at 780.
[115] 709 F.3d 952 (9th Cir. 2013), *cert. denied* Jan. 13, 2014.
[116] *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.
[117] 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
[118] *Id.* at 965.
[119] *Id.* at 966.

Shortly before, the Southern District of New York, in *Abidor v. Napolitano*,[120] reached a contrary conclusion to *Cotterman* opinion, leaving the state of the law unsettled. There, plaintiffs sought to invalidate Department of Homeland Security regulations permitting Immigration & Customs Enforcement ("ICE") and Customs & Border Patrol ("CBP") 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 ICE or CBP jurisdiction. The court rejected plaintiffs' as-applied and facial challenges to the regulations, which sought declaratory relief finding that the regulations violated the First and Fourth Amendments, on two bases. First, the court found that the plaintiffs lacked standing in an action seeking 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 on the merits 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, including that travelers have advance notice of border crossings and can choose to leave sensitive information behind. It noted, however, that "if suspicionless forensic computer searches at the border threaten to become the norm, then some threshold showing of reasonable suspicion should be required."[121] Like *Cotterman*, the court ultimately concluded that the agents had had reasonable suspicion for both the "quick look" and forensic searches of the individual plaintiff's laptop, where the plaintiff was returning from Lebanon, had two separate passports, had stored electronic pictures of Hamas and Hezbollah rallies (both categorized as terrorist organizations), and was unable to sufficiently explain the presence of pictures of Hamas rallies on his laptop, which were unrelated to his academic research focusing on Shiites in Lebanon.

IV. FIFTH AMENDMENT PRIVILEGE AND DATA ENCRYPTION

Encryption software can effectively shield information from what would otherwise be lawful search and seizure by the government. The only federal appeals court decision that squarely addresses this issue is a 2012 child pornography case from the Eleventh Circuit. In the case of *In re Grand Jury Subpoena Duces Tecum*,[122] the government seized hard drives that it believed contained child pornography. Some of the hard drives were encrypted, and the suspect refused to decrypt the devices, invoking his Fifth Amendment right against self-incrimination. The Eleventh Circuit held that compelling the suspect to decrypt and produce the drives' contents "would be tantamount to testimony by Doe 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."[123] Moreover, the government could not force a suspect to decrypt and produce the information where it could not identify with "reasonable particularity" the existence of certain files, noting that an "act of production can be testimonial when that act conveys some explicit or implicit statement of fact that certain materials exist, are in the subpoenaed individual's possession or control, or are authentic."[124] The court also rejected the government's attempt to immunize production of the drives' contents because the government acknowledged that "it would use the contents of the unencrypted drives

[120] No. 1:10-cv-04059-ERK (S.D.N.Y. Dec. 31, 2013).
[121] *Id.* at 30.
[122] 670 F.3d 1337 (11th Cir. 2012).
[123] *Id.* at 1346.
[124] *Id.* at 1345.

against" the suspect.[125]

The critical aspect is the government's knowledge about the encrypted data. If the government does not know what type of data is in the computer, an individual's act of decrypting and producing it constitutes "testimony" under Fifth Amendment case law. This is clear in another recent decision.[126] In *United States v. Fricosu*, Ms. Fricosu was under investigation for her alleged involvement in a mortgage scam. Federal agents obtained a search warrant, searched her home, and seized three laptop computers. One of the computers was encrypted and two were not. Ms. Fricosu went to visit her husband, who was in jail at the time. In a recorded jailhouse conversation, they discussed whether there was "anything on [the] computer to protect it," and Ms. Fricosu said there was. She said, "I don't know if they can get to it," and "my lawyer said I'm not obligated by law to give them any passwords or anything they need to figure things out for themselves."[127] Based on that conversation, the government sought a writ requiring Ms. Fricosu to decrypt and produce the laptop's contents. She refused, asserting her Fifth Amendment rights. The judge granted the writ, noting that because the government knew about the existence of the files on the computer, and knew their location, the act of decrypting and producing the files was not "testimonial."

The distinction is apparent between *Doe* and *Fricosu*. In *Doe*, where government agents did not know what was on the computer, the court could not compel Doe to use "the contents of his own mind" to decrypt the data. However, in *Fricosu*, her act of decryption would provide the government with the data on the computer, but it would not provide the information that the files existed in the first place. The government already knew they existed.[128]

These decisions appear to limit government investigators' ability to compel an individual to reveal the contents of devices encrypted with passwords or codes in a criminal investigation based only on government speculation as to what data may be contained in certain files. 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.

---

[125] *Id.* at 1349.

[126] United States v. Fricosu, 841 F. Supp. 2d 1232, 1236 (D. Colo. 2012).

[127] *Id.* at 1236.

[128] A more recent decision on this issue continues to follow the same foregone-conclusion analysis. In the case of *In re Decryption of a Seized Data Storage System*, No. 2:13-MG-449-WEC (E.D. Wis. Apr. 19, 2013), 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. *Id.* at *8. However, the court noted that the government had only shown that the defendant "may very well be capable of accessing the encrypted portions of the hard drives." *Id.* Therefore, the Fifth Amendment protection was available to defendant, since his act of production "which would necessarily require his using a password of some type to decrypt the storage device, would be tantamount to telling the government something it does not already know with 'reasonable particularity' – namely, that [defendant] has *personal access to and control over* the encrypted storage devices." *Id.* at *9 (emphasis in original).

V. POST-INDICTMENT DISCOVERY

A. 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 has largely faced a vacuum of formal guidance. However, 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," representing an important development that should significantly aid criminal attorneys, particularly prosecutors, public defenders, and CJA panel attorneys, who have previously wrestled with e-discovery issues.

The Joint E-Discovery Protocol, which is only intended to apply to disclosure of ESI under Federal Rules of Criminal Procedure 16 and 26.2, *Brady, Giglio* and the Jencks Act,[129] 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:[130]

> 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.

---

[129] 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.

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

> 6. Following the meet and confer, the parties should notify the court of 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.[131]

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.

---

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

B. 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*, [132] 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."[133] 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."[134]

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."[135] 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*,[136] 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)."[137] *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 resources.[138] 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.[139]

---

[132] United States v. Skilling, 554 F.3d 529 (5th Cir. 2009).
[133] *Id*. at 576.
[134] *Id*.
[135] *Id*. at 577.
[136] United States v. Salyer, No. S-10-0061, 2010 WL 3036444 (E.D. Cal. Aug. 2, 2010).
[137] *Id.* at *2.
[138] *Id.* at *7.
[139] *Id.* at *5.

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."[140] "[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."[141] 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.[142]

C. 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.[143] 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 monumental due diligence responsibilities. Three, the discovery itself has often been tainted or incomplete."[144] 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."[145]

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

---

[140] *Id.* at *6.
[141] *Id.*
[142] *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).
[143] 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) (court reversed conviction and remanded for new trial after finding that trial court erred by denying defendant meaningful access to hard drives seized from his house).
[144] *Graham*, 2008 WL 2098044 at *5.
[145] *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).

engages with friends and family. Not surprisingly, this medium significantly impacts government investigations and criminal litigation.

A. 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."[146] Social media use in the United States alone has increased by 356% since 2006.[147] An estimated 52% of Americans now have at least one social media profile,[148] more than 1.1 billion people use Facebook actively each month,[149] and Twitter has over 500 million users posting 400 million Tweets a day.[150] Almost one-quarter of Facebook users check their account more than 5 times per day, and 350 million photos are uploaded each day.[151] Instagram, with more than 130 million users, already has more than 16 billion uploaded photos, with more than 5 million photos uploaded each day.[152] 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.[153]

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.[154] And, with the advent of location-based services offered by social media companies like Facebook, Twitter, and FourSquare,

---

[146] 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).

[147] Netpop Research, *Connect: Social Media Madness U.S. 2012* (April 2012), http://www.netpopresearch.com/social-media-madness.

[148] Tom Webster, *The Social Habit 2011* (May 29, 2011), http://www.edisonresearch.com/home/archives/2011/05/the_social_habit_2011.php.

[149] Social Media Stats 2013 (Nov. 14, 2013), http://www.digitalbuzzblog.com/infographic-social-media-stats-2013/; Mark Zuckerberg, *One Billion People on Facebook* (Oct. 4, 2012), http://newsroom.fb.com/News/One-Billion-People-on-Facebook-1c9.aspx; 21 Awesome Social Media Facts, Figures and Statistics for 2013, http://www.jeffbullas.com/2013/05/06/21-awesome-social-media-facts-figures-and-statistics-for-2013/

[150] *Twitter Turns Six* (Mar. 21, 2012), http://blog.twitter.com/2012/03/twitter-turns-six.html.

[151] Social Media Stats 2013 (Nov. 14, 2013), http://www.digitalbuzzblog.com/infographic-social-media-stats-2013/.

[152] *Id.*

[153] *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.").

[154] 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.

precise geolocation information will be increasingly maintained in the ordinary course of business and subject to the same subpoenas and search warrants.[155] Not surprisingly, each social media subpoena can yield admissions or incriminating photos, among other evidence.[156]

B. Accessing Publicly Available 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.[157] 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:

- 95.9% of agencies surveyed use social media.
- The most common use of social media is for criminal investigations at 86.1%.
- The most frequently used social media platforms are Facebook (92.1%), Twitter (64.8%), and YouTube (42.9%).
- 57.1% of agencies not currently using social media are considering doing so.
- 69.4% of agencies surveyed have a social media policy and an additional 14.3% are in the process of crafting a policy.
- 80.4% of agencies report that social media has helped solve crimes in their jurisdiction.
- 73.1% of agencies state that social media has improved police-community relations in their jurisdiction.[158]

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 grant them access to

---

[155] 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.

[156] *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).

[157] *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).

[158] International Association of Chiefs of Police 2013 Social Media Survey Results, http://www.iacpsocialmedia.org/Portals/1/documents/2013SurveyResults.pdf.

information.[159] In *United States v. Meregildo*,[160] 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 that

> where 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.[161]

C. *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.[162] And almost 80% of those requests were from authorities in the United States.[163] Google, which is a provider of social 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. Statistics published by Google demonstrate a 68% increase from January to June 2013 over the second half of 2012.[164]

At least one court has questioned a government request to obtain social media evidence with a search warrant. In the case of *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.[165] Specifically, the

---

[159] *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*, Criminal 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").

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

[161] *Id.*

[162] *Twitter Transparency Report* (Jan. 1 – June 30, 2013), https://transparency.twitter.com/information-requests/2013/jan-jun.

[163] *Id.*

[164] *Google Transparency Report*, (January to June, 2013) http://www.google.com/transparencyreport/.

[165] Case 13-MJ-742 (JMF) (D.D.C. Nov. 26, 2013).

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.[166]

D. 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.[167] 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.[168] As a result, courts have been left to determine how and whether the SCA 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.[169]

---

[166] *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.).

[167] *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").

[168] *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).

[169] *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).

The SCA provides that non-content records can be compelled via a subpoena or court order.[170] 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."[171] 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).[172]

The constitutionality of the SCA has been called into question by at least one Circuit Court of Appeals. In *United States 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."[173] 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."[174] 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."[175]

Recognizing the SCA's deficiencies, both Congress and the White House have sought to downplay the effects of the statute in 2012 and 2013. On March 19, 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 regulators enforcing various laws that do not carry criminal penalties (and therefore for which criminal search warrants are not available).[176]

---

[170] 18 U.S.C. § 2703(c)(2); *id.* § 2703(d).
[171] Warshak, 631 F.3d at 282-83 (citation omitted).
[172] *Id.*
[173] *Id.* at 288.
[174] *Id.* (citations omitted).
[175] *Id.* at 285-286.
[176] 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

Over the past two sessions, Congress has struggled to advance bills that would reform ECPA and, in particular, the SCA. Numerous such proposals have been introduced, referred to, and/or voted out of committee,[177] 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 will likely require similar clarification by courts.

E. Defending a Criminal Case with Social Media Evidence

Defendants face more significant obstacles than the government when seeking exculpatory evidence from social media companies.[178] First, defendants and their counsel do not share the government's freedom to sleuth for publicly-available social media evidence.[179] Ethics opinions issued to lawyers in various states have established that a defendant's lawyer may not "friend" or direct a third person to "friend" another party or witness in litigation in order to search for impeachment material or exculpatory evidence.[180]

Second, Defendants face additional hurdles when seeking to issue a third-party subpoena.[181] Defendants may seek to subpoena social media companies for user information regarding the victim, the complaining witness, or another witness.[182] In those instances, in

---

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.

[177] *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).

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

[179] *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).

[180] *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 is not); 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).

[181] 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.

[182] *Id.*

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.[183] 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 that information without the consent of the owner of the account.[184] 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.[185]

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*.[186] Moreover, courts may order jurors, witnesses, or third parties to produce or manipulate their social media information in unique and unprecedented ways. For example, courts have done the following: (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;[187] (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;[188] (3) recommended that an individual "friend" the judge on Facebook in order to facilitate an *in camera* review of Facebook photos and comments;[189] and (4) ordered parties to exchange social media account user names and passwords."[190] 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.

F. 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[191] – creates hurdles to admissibility not

---

[183] Fed. R. Crim. P. 17(e)(1).
[184] 18 U.S.C. § 2703.
[185] 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.
[186] *See* Brady v. Maryland, 373 U.S. 83 (1963); Giglio v. United States, 405 U.S. 150 (1972).
[187] Juror Number One v. California, No. CIV. 2:11-397 WBS JFM, 2011 WL 567356, at *1 (E.D. Cal. Feb. 14, 2011).
[188] Katiroll Co. v. Kati Roll and Platters, Inc., 2011 WL 3583408, at *4 (D.N.J. Aug. 3, 2011).
[189] Barnes v. CUS Nashville, LLC, No. 3:09-CV-00764, 2010 WL 2265668, at *1 (M.D. Tenn. June 3, 2010).
[190] *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").
[191] *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

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.

Notably, these same challenges face the government, which must also 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.[192] 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.[193] The logs "had a devastating impact" on the defendant because they contradicted many of his statements made during his testimony, and he was convicted.[194] 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.[195]

While both government and defense attorneys grapple with addressing and authenticating social media sources of evidence, courts largely seem to be erring on the side of admissibility and leaving any concerns about the evidence itself – such as who authored the evidence or whether the evidence is legitimate – to jurors to decide what weight that evidence should be given. For example, social media evidence has been ruled admissible where the content of the evidence contains sufficient indicia that it is the authentic creation of the purported user.[196] In *Tienda v. State*,[197] the appellant was convicted of murder based

---

creator").

[192] 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).

[193] *Id.* at 2.

[194] *Id.*

[195] *Id.* at 4-5.

[196] *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

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."[198] 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 the appellant was responsible for."[199]

In another case, a defendant was charged with aggravated assault following a domestic dispute with his girlfriend.[200] At trial, the prosecution introduced Facebook messages sent from the defendant's account, in which he regretted striking his girlfriend and asked for her forgiveness. The defendant denied sending the Facebook messages, and argued that both he and his girlfriend had access to each other's Facebook account. Acknowledging that electronic communications are "susceptible to fabrication and manipulation," the court allowed the messages to be authenticated through circumstantial evidence, most notably evidence that they were sent from the defendant's account and the girlfriend's testimony that she did not send the messages.[201] In 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.[202]

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.

---

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 he believed defendant had sent them; inconsistencies and conflicting inferences regarding authenticity goes to weight of evidence, not its authenticity).

[197] Tienda v. State, 358 S.W.3d 633, 634-35 (Tex. Crim. App. 2012).

[198] *Id.* at 635.

[199] *Id.* at 647.

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

[201] *Id.* at *4.

[202] United States v. Drummond, No. 1:09-cr-00159, 2010 WL 1329059 at **2-3 (M.D. Pa. Mar. 29, 2010). The defendant ultimately entered a guilty plea and there was no final ruling by the court on the admissibility of the photographs.