# CHAPTER 8

# E-DISCOVERY IN GOVERNMENT INVESTIGATIONS AND CRIMINAL LITIGATION

**Justin P. Murphy**

Dealing with electronically stored information (ESI), for clients, prosecutors and defense attorneys, has steadily grown into a tsunami of cost and complexity – with little guidance provided by 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 and demands in government investigations and criminal matters and the absence of cost-effective methods sanctioned by courts to resolve criminal discovery disputes. The world of criminal e-discovery continues to evolve every day, 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] There is little case law in the criminal arena on this point, but in general the same principle applies: 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 the conduct at Arthur Andersen LLP in 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 do so, 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 the defendant's culpability score.[3]

Importantly, preservation failures can also expose a defendant to an additional investigation for obstruction of justice. If the government encounters efforts to destroy evidence, they may assume bad intent unless good faith can otherwise be demonstrated. Where intent can be shown, 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.

Likewise, the government also has a duty to preserve ESI, and the 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 jury ultimately acquitted the defendant, who argued that the missing text messages were important.

While spoliation sanctions are increasingly common in civil litigation, it is rare for such conduct to be charged as criminal obstruction of justice.[7] But in a recent indictment, the Department of Justice did

just that. 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) & (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 and the significant jail time to which individuals could be exposed.

## II. INVESTIGATIONS: SEARCH AND SEIZURE OF ESI

The unique challenges presented by the very nature of ESI create problems in the context of search warrants as well. Specifically, the modern day phenomenon of immense amounts of intermingled computer 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 many millions of pages of documents, some of which can be hidden or disguised to frustrate the government's 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."

With collection of ESI via a search warrant, it is helpful to think of it as two searches and seizures. First, there is a search of the place specified in the warrant. Over-seizure of ESI is often the result because of the practical realities of on-site searches of large volumes of data, and the fact that files can be readily disguised and intermingled with other personal and/or irrelevant data. Courts have acknowledged and seemingly accepted the need to over-seize in the "first" search and seizure. The second search and seizure usually takes place at law enforcement offices where agents search for and seize data from the "warehouse" of ESI they previously seized.

The debate rises from the second search and seizure – by over-seizing ESI, the government has created a risk that every 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 be involved in controlling the government's conduct of the second search and seizure, whether or not computers deserve special treatment in digital evidence cases, or whether they are analogous to more traditional document containers, such as filing cabinets.

### *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, an *en banc* panel issued new and enhanced guidelines for warrants seeking ESI.[8] 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."[9] 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 . . . ."[10] 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.[11]

In September 2010, an *en banc* panel issued an amended opinion, demoting the above requirements to suggested guidance when dealing with the over-seizure of ESI.[12] In support of the court's change in position, it opined that the five guidelines are hardly revolutionary, and are essentially the Ninth Circuit's solution to the problem of necessary over-seizing of evidence from a prior decision, *United States v. Tamura*.[13] Adhering to its ruling in *Tamura*, the Ninth Circuit applied a two step process. First, where officers come across relevant documents so intermingled with irrelevant documents that they cannot feasibly be sorted at the site, large scale removal of materials can be justified.[14] And second, a Magistrate Judge should then approve the conditions and limitations on a further search of those documents. The "essential safeguard required is that wholesale removal must be monitored by the judgment of a neutral, detached magistrate."[15] 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."[16]

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."[17]

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."[18]

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

Other Circuits have weighed in on the tension between the particularity requirement under the Fourth Amendment and the plain view doctrine. For example, in *United States v. Richards,*[19] the Sixth Circuit acknowledged that: "On 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."[20]

The Sixth Circuit applied "the Fourth Amendment's bedrock principle of reasonableness on a case-by-case basis,"[21] and found that the FBI's warrant was not overbroad, even though there was no distinction made between seizing servers maintained by third parties that contain information belonging

to others, and servers exclusively maintained by the defendant.[22] 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.[23] 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.[24] 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."[25]

*United States v. Stabile* is another decision addressing the issue of "over-seizure" of evidence under the plain view doctrine.[26] In *Stabile*, agents went to the defendant's home to question him regarding allegations that he was involved in counterfeiting and other financial crimes.[27] 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.[28] The agents seized several computer hard-drives from the home, and discovered child pornography on the hard-drives.[29]

While the court in *Stabile* declined to follow the Ninth Circuit's suggestion in *Comprehensive Drug Testing*[30] 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."[31] The court supported the general framework articulated in *Comprehensive Drug Testing* by opining that "we agree 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.'"[32]

Only one federal appeals court has flatly disagreed with the *Comprehensive Drug Testing* decision. In *United States v. Williams*,[33] 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.[34] There, the court reasoned in order to be effective, a search cannot be limited to reviewing only file designations or labeling as these things can easily be manipulated.[35] 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."[36]

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.[37] 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."[38]

### *Time Limits on the Search of Data*

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 the defendant's data pursuant to a valid search warrant but then failed to do anything with the images for over 15 months.[39] While the search warrant itself was proper, the process afterwards was not: the Fourth Amendment requires the government to complete its review within a "reasonable" period of time. While the court noted that delays of several months have been found to be reasonable, there was no guidance as to when a delay become 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.[40]

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

> 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.[41]

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

***Warrantless Searches of Cellular Telephones***

As of December 2011, there were more mobile phones than people in the United States.[42] 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. As with Fourth Amendment search warrants, courts have struggled to apply traditional doctrines to modern day technology – in this case comparing mobile phones to a closed container on an arrestee's person, such as a wallet, purse, address book or cigarette package. However, unlike a closed container, a computer – and a modern mobile phone is a computer – does not store physical objects which are in plain view once the container is opened. Moreover, the storage capability of an electronic device is not limited by the physical size of the container. Today's mobile phones are gateway devices, allowing a user – or potentially a law enforcement officer pursuant to a lawful arrest – to access data stored in the cloud, countless photographs, text messages, location data, chats, or items located on another computer, just to name a few.

Federal courts are divided on the issue of whether a warrant is required to search the data in a cellular telephone following an arrest. Several Circuits have concluded that law enforcement may retrieve text messages and other information from cellular phones seized in a search incident to a lawful arrest.[43] Other courts have invalidated warrantless searches of cellular phones seized incident to arrest.[44]

Some courts have recognized the potential dangers of allowing law enforcement to search mobile phones pursuant to a lawful arrest. For example, a district court in Florida[45] tempered its decision permitting officers to search the contents of a cellular telephone as a "search incident to arrest," by explaining that:

> 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.[46]

Another recent decision expressed similar concerns. In *Hawkins v. State*, the Georgia Supreme court in upholding a search of the defendant's mobile phone incident to a lawful arrest, noted 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 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.[47]

State courts around the county are also divided on the cell phone issue. In *People v. Diaz,*[48] the California Supreme Court recently affirmed the denial of a motion to suppress a text message found on a defendant's cellular telephone. In *Diaz,* a detective witnessed the defendant participate in a controlled drug buy, arrested him, and seized his cell phone from his person.[49] 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.[50] The *Diaz* court found that the cell phone 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 cell phone being seized and being searched.[51] 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.[52]

***Warrantless Use of GPS Tracking Devices***

The United States Supreme Court has addressed whether the warrantless use of a global positioning system (GPS) tracking device on a suspect's vehicle to monitor his movements on public streets violated the Fourth Amendment.[53] The underlying case[54] involved two nightclub owners in the District of Columbia (Antoine Jones and Lawrence Maynard) who were under investigation for narcotics violations.[55] During the investigation, officers attached a GPS device to Jones's vehicle without a warrant.[56] The GPS device tracked Jones's movements 24 hours a day for one month.[57] 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.[58] 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 reveal more about a person than does any individual trip viewed in isolation."[59]

In *United States v. Jones*, the Supreme Court disagreed. In a narrow holding, the Supreme Court found that the installation of a GPS monitoring device is a search. Justice Scalia's opinion for the Court 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."[60] Thus, the installation of the GPS constituted a search because it was a trespass on the defendant's car. However, the opinion continued that "our cases suggest that such visual observation is constitutionally permissible. It 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."[61]

Importantly, the Court declined to address whether the installation of GPS is a search that *requires* a warrant, although at least four members of the Court suggested 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, disagreeing with Justice Scalia's trespass approach. Instead, Justice Alito argued 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."[62] The *Jones* decision raises more questions than it answers and does not even find that a warrant is required to install a GPS device. Rather, the Court's reluctance to "grapple with these 'vexing problems'"[63] highlights the continued challenges we face by applying a document drafted in 1789 – when mail could take months to travel across the Atlantic – to today's technology – when data can span the globe in a matter of seconds.

At least one court has gone further than the *Jones* decision, holding that the Fourth Amendment does in fact require law enforcement agents to obtain search warrant before using a GPS device to monitor a suspect's vehicle. In *State v. Brereton*,[64] the police obtained a warrant to install a GPS tracking device on the car of a suspect believed to be 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:

> 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.'[65]

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."[66]

## III. FIFTH AMENDMENT PRIVILEGE AND DATA ENCRYPTION

Sophisticated encryption software can effectively shield information from what would otherwise be

lawful search and seizure by the government. In an important decision that could have significant implications for government enforcement, the Eleventh Circuit ruled that a suspect could not be required to decrypt his computer hard drives because it would implicate his Fifth Amendment privilege and amount to the suspect's testifying against himself.

In *In re Grand Jury Subpoena Duces Tecum*,[67] 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." 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." 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 against" the suspect.

This decision appears 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.

## IV. POST-INDICTMENT DISCOVERY

### *Joint Federal Criminal E-Discovery Protocol*

Unlike e-discovery in civil litigation, which benefits from specific procedural rules and developed case law to guide its practitioners, criminal e-discovery practice has largely faced a vacuum of formal guidance. However, in February 2012, the Joint Working Group on Electronic Technology in the Criminal Justice System (comprised of representatives from the Department of Justice, 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,[68] 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:[69]

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 mature, volume, and mechanics of producing ESI discovery. Where the ESI is particularly complex or produced on a rolling basis, an on-going dialogue may be helpful.

4. The parties should discuss what formats of production are possible and appropriate, and what formats can be generated. Any format selected for producing discovery should maintain the ESI's integrity, allow for reasonable usability, reasonably limit costs, and, if possible, conform to industry standards for the format.
5. When producing ESI discovery, a party should not be required to take on substantial additional processing or format conversion costs and burdens beyond what the party has already done or would do for its own case preparation or discovery production.
6. Following the meet and confer, the parties should notify the court of 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.[70]

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.

***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*, [71] 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."[72] 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."[73]

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."[74] 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*,[75] 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)."[76] *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.[77] 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."[78]

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."[79] "[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."[80] 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.[81]

***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.[82] 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."[83] 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."[84]

## V. SOCIAL MEDIA AND THE INTERNET

Social media has evolved into a fundamental pillar of communication in today's society, revolutionizing how the world does business, learns about and shares news, and instantly engages with friends and family. Not surprisingly, this exploding medium significantly impacts government investigations and criminal litigation because social media factors into the majority of cases in some respect.

### *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."[85] Social media use in the United States alone has increased by 356% since 2006.[86] 52% of Americans now have at least one social media profile,[87] more than one billion people use Facebook actively each month,[88] and Twitter has over 140 million active users posting 340 million Tweets a day.[89] And, every minute, social media users create massive amounts of data: Facebook users share 684,478 pieces of content; Tumblr blog owners publish 27,778 new posts; YouTube users upload 48 hours of new video; Foursquare users perform 2,083 check-ins; Flickr users add 3,125 new photos, and Instagram users share 3,600 new photos.[90] In addition, there are hundreds of other social networking websites, each catering to a different demographic.[91] The myriad and continually changing ways to share information via social media has 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.[92]

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.[93] And, with the advent of location-based services offered by social media companies like Facebook, Twitter and FourSquare, precise location information will be increasingly maintained in the ordinary course of business and subject to the same subpoenas and search warrants.[94] Not surprisingly, each social media subpoena can yield admissions or incriminating photos, among other evidence.[95]

### *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.[96] A majority of government agencies are active participants, contributing content and soliciting information through social media.[97] 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.

But, 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 information.[98] In *United States v. Meregildo*,[99] for example, the defendant set the privacy settings on his Facebook account so that only his Facebook "friends" could view his postings. The government obtained the incriminating evidence against the defendant through a cooperating witness who happened to be Facebook "friends" with the defendant. The defendant moved to suppress the evidence seized from his Facebook account, arguing that the government had violated his Fourth Amendment rights. The court found:

> [W]here Facebook privacy settings allow viewership of postings by 'friends,' the Government may access them through a cooperating witness who is a 'friend' without violating the Fourth Amendment. While [defendant] undoubtedly believed that his Facebook profile would not be shared with law enforcement, he had no justifiable expectation that his 'friends' would keep his profile private. And the wider his circle of 'friends', the more likely [defendant's] posts would be viewed by someone he never expected to see them. [Defendant's] legitimate expectation of privacy ended when he disseminated posts to his 'friends' because those 'friends' were free to use the information however they wanted -- including sharing it with the Government.[100]

***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, Twitter received more government requests for user information in the first half of 2012 than in the entirety of 2011.[101] And over 80% of those requests were from authorities in the United States.[102] Google, which is a provider of social networking sites like YouTube and Google+, has also seen an uptick in the frequency with which it receives subpoenas and search warrants in criminal matters. Statistics published by Google, which "primarily cover requests in criminal matters,"[103] show that the number of Google user data requests received from government authorities in the United States increased more than 40% from 2009 to 2011.[104]

Moreover, the prevalence of social media evidence in criminal proceedings will continue to proliferate as government agencies continue to formally train their personnel to search for and collect social media evidence. A recent survey of over 1,200 federal, state and local law enforcement professionals revealed that social media is widely used to assist in investigations, that few have received formal training on how to use social media for investigations, and that "74% of those not currently using it . . . intend to start using it."[105] And the case law is already replete with instances where the government obtained social media evidence through a warrant or subpoena directed at a social media company.[106] Social media evidence is the new frontier of criminal proceedings, and it raises unique legal challenges, including issues of admissibility and a defendant's constitutional rights in material maintained by social media companies.

***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 Stored Communications Act ("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.[107] The SCA, which was passed in 1986, 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.[108] 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.[109]

The SCA provides that non-content records can be compelled via a subpoena or court order.[110] 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."[111] 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).[112]

The constitutionality of the SCA has been called into question by at least one Circuit Court of Appeals. In *U.S. v. Warshak*, the Sixth Circuit held that "the government agents violated the Fourth Amendment when they obtained the contents of [defendant's] emails" without a warrant, and added that "to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional."[113] 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."[114] 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."[115] As social media becomes as pervasive and important to people as email, its treatment under the SCA will require similar clarification by courts.

***Defending a Criminal Case with Social Media Evidence***

Defendants face more significant obstacles than the government when seeking exculpatory evidence from social media companies.[116] First, defendants and their counsel do not share the government's freedom to sleuth for publicly-available social media evidence.[117] 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.[118]

Second, Defendants face additional hurdles when seeking to issue a third party subpoena.[119] Defendants may seek to subpoena social media companies for user information regarding the victim, the complaining witness or another witness.[120] In those instances, in federal criminal proceedings, defendants must pursue such non-party discovery pursuant to Federal Rule of Criminal Procedure 17 and seek a court order allowing such a subpoena.[121] 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 and MySpace, from disclosing that information without the consent of the owner of the account.[122] 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.[123]

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*.[124] 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;[125] (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;[126] (3) recommended that an individual "friend" the judge on Facebook in order to facilitate an *in camera* review of Facebook photos and comments;[127] and (4) ordered parties to exchange social media account user names and passwords."[128] Such novel avenues of access to social media evidence may be considered where the defendant subpoenas a social media provider for certain records of a witness or victim and the social media company objects to

the subpoena pursuant to the SCA or is unable to produce the evidence as it previously existed.

***Admissibility of Social Media Evidence***

Social media is subject to the same rules of evidence as paper documents or other electronically stored information, but the unique nature of social media – as well as the ease with which it can be manipulated or falsified[129] – creates hurdles to admissibility not faced with other evidence. The challenges surrounding social media evidence demand that one consider admissibility when social media is preserved, collected, and produced. It is important for counsel to memorialize each step of the collection and production process and to consider how counsel will authenticate a Tweet, Facebook posting, or photograph, for example: by presenting a witness with personal knowledge of the information (they wrote it, they received it, or they copied it), by searching the computer itself to see if it was used to post or create the information, or by attempting to obtain the information in question from the actual social media company that maintained the information the ordinary course of their business.

Notably, these same challenges face the government who must also consider admissibility of social media when they conduct their 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.[130] 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.[131] The logs "had a devastating impact" on the defendant because they contradicted many of his statements made during his testimony, and he was convicted.[132] 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.[133]

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.[134] In *Tienda v. State*,[135] the appellant was convicted of murder based in part on evidence obtained by the prosecutors after subpoenaing MySpace. Specifically, "the State was permitted to admit into evidence the names and account information associated with [the defendant's MySpace.com profiles], photos posted on the profiles, comments and instant messages linked to the accounts, and two music links posted to the profile pages."[136] The Court of Criminal Appeals affirmed the trial judge and concluded that the MySpace profile exhibits used at trial were admissible because they 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."[137]

In another recent case, a defendant was charged with aggravated assault following a domestic dispute with his girlfriend.[138] 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 accounts. Acknowledging that electronic communications are "susceptible to fabrication and manipulation", the court allowed the messages to be authenticated through circumstantial evidence, most notably that they were sent from the defendant's account and that the girlfriend testified that she did not send the messages.[139] 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.[140]

Given the proliferation of social media, the increasing sophistication of technology, and the potential challenges relating to the reliability or authentication of social media, the authentication and admissibility of such evidence will likely be the subject of vigorous disputes between parties that may mean the difference between ultimate guilt and innocence.

---

***Endnotes, Chapter 8***

[1] Sedona Conference Commentary on Legal Holds, August 2007; *Zubulake v. UBS Warburg*, 229 F.R.D. 422 (S.D.N.Y. 2004).

[2] *See* 18 U.S.C. § 1519 (punishing document destruction in "contemplation" of a federal investigation).

[3] *See* U.S.S.G. § 8C2.5.

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

[5] *Id.* at *1.

[6] *Id.* at *8.

[7] 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).

[8] *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).

[9] *Id.* at 998.

[10] *Id.* at 1006.

[11] *Id.*

[12] *See* United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1177-1180, 1183 (9th Cir. 2010).

[13] 694 F.2d 591 (9th Cir. 1982). 621 F.3d at 1180.

[14] 621 F.3d at 1169, 1171.

[15] *Id.* (quoting *Tamura*, 694 F.2d at 596).

[16] *Id.* at 1177.

[17] *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).

[18] *Id.* at 1176.

[19] United States v. Richards, 659 F.3d 527 (6th Cir. 2011).

[20] *Id.* at 538.

[21] *Id.* at 538.

[22] *Richards*, at 541.

[23] *Id.* at 552 (Moore, C.J., concurring).

[24] *Id.* at 558 (Moore, C.J., concurring).

[25] *Id.*

[26] United States v. Stabile, 633 F.3d 219 (3d Cir. 2011).

[27] *Id.* at 224.

[28] *Id.* at 225.

[29] *Id.*

[30] Comprehensive Drug Testing, 621 F.3d at 1178 (Kozinski, CJ, concurring).

[31] *Id.* at 241.

[32] *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.*

[33] United States v. Williams, 592 F.3d 511, 515-517 (4th Cir. 2010).

[34] *Id.* at 521-522.

[35] *Id.* at 522.

[36] *Id.*

[37] In re Application for Search Warrant, Mag. No. 09-320 (D.D.C. June 3, 2009) (Facciola, M.J.).

[38] *Id. See also* United States v. Payton, 573 F.3d 859, 864 (9th Cir. 2009) (suppressing evidence resulting from search of computer where there was "no . . . evidence pointing to the computer as a repository for the evidence sought in the search.").

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

[40] *Id.*

[41] *Id.*

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

[43] *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. Wurie, 612 F. Supp. 2d 104, 110 (D. Mass. 2009); United States v. Santillan, 571 F. Supp. 2d 1093, 1102-03 (D. Ariz. 2008).

[44] *See, e.g.*, United States v. Quintana, 594 F. Supp. 2d 1291, 1301 (M.D. Fla. 2009); *United States v. McGhee*, No. 8:09CR31, 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. CR 05-375 SI, 2007 WL 1521573, at *1 (N.D. Cal. May 23, 2007) (search of a cell phone an hour after the arrest was suppressed).

[45] United States v. Gomez, No. 11-20304-CR, 2011 WL 3841071, at *8 -12 (S.D. Fla. 2011).

[46] *Gomez* at *12.

[47] 723 S.E.2d 924 (Ga. 2012)

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

[49] *Id.* at 502.

[50] *Id.*

[51] *Id.* at 506.

[52] Senate Bill 914.

[53] *See* United States v. Jones, 2012 WL 171117 (Jan. 23, 2012).

[54] United States v. Maynard, 615 F.3d 544, 559 (D.C. Cir. 2010).

[55] *Id.* at 549.

[56] *Id.* at 558–59.

[57] *Id.*

[58] *Id.* at 559.

[59] *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 cartilage of the home)).

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

[61] *Id.* at 954.

[62] *Id.* at 964.

[63] *Id.* at 954.

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

[65] *Id.* at *8.

[66] *Id*. at *10.

[67] 670 F.3d 1337 (11th Cir. 2012).

[68] 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.

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

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

[71] United States v. Skilling, 554 F.3d 529 (5th Cir. 2009).

[72] *Id*. at 576.

[73] *Id*.

[74] *Id*. at 577.

[75] United States v. Salyer, No. S-10-0061, 2010 WL 3036444 (E.D. Cal. Aug. 2, 2010).

[76] *Id.* at *2.

[77] *Id.* at *7.

[78] *Id.* at *5.

[79] *Id.* at *6.

[80] *Id.*

[81] *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).

[82] 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).

[83] *Graham* at *5.

[84] *Id*. at *8. *But see* United States v. Qadri, 2010 WL 933752 (D. Haw. Mar. 9, 2010) (court denied 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).

[85] 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).

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

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

[88] Mark Zuckerberg, *One Billion People on Facebook* (Oct. 4, 2012), http://newsroom.fb.com/News/One-Billion-People-on-Facebook-1c9.aspx.

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

[90] Josh James, *How Much Data is Created Every Minute?* (June 8, 2012), http://www.domo.com/blog/2012/06/how-much-data-is-created-every-minute/.

[91] Pingdom, *Report: Social Network Demographics in 2012* (Aug. 21, 2012), http://royal.pingdom.com/2012/08/21/report-social-network-demographics-in-2012/.

[92] *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.").

[93] Earlier this year, 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.

[94] 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.

[95] *See e.g.*, United States v. Anderson, 664 F.3d 758, (8th Cir. 2012) (defendant sentenced 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).

[96] *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).

[97] Saba, *New Study Shows 66% of Government Organizations Have Adopted Social Networking, Collaboration Tools* (Jan. 14, 2010), http://www.saba.com/company/press-releases/2010/saba-and-hci-publish-study-of-social-networking-in-government/.

[98] *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").

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

[100] *Id.*

[101] *Twitter Transparency Report* (July 2, 2012), http://blog.twitter.com/2012/07/twitter-transparency-report.html.

[102] *Id.*

[103] *FAQ – Google Transparency Report*, http://www.google.com/transparencyreport/userdatarequests/faq/ (last visited Oct. 24, 2012).

[104] *Visible Changes – Google Transparency Report*, http://www.google.com/transparencyreport/userdatarequests/data/ ( last visited Oct. 24, 2012).

[105] LexisNexis, *supra* note 13.

[106] *See, e.g.*, Anderson, 664 F.3d at 762 (hundreds of Facebook private chats obtained through a search warrant); *Meregildo*, 2012 WL 3264501, at *2 (evidence obtained through warrant issued to Facebook); *People v. Harris*, 949 N.Y.S.2d 590, 597 (N.Y. Crim. Ct. 2012) (state sent Twitter a subpoena seeking to obtain defendant's user information and Tweets); United States v. Sayer, 2:11-CR-113-DBH, 2012 WL 2180577, at *3 (D. Me. June 13, 2012) (subpoenas used to obtain evidence from Facebook and MySpace); In re Grand Jury Subpoena No. 11116275, 846 F. Supp. 2d 1, 2 (D.D.C. 2012) (denying anonymous intervenor's motion to quash a subpoena issued to Twitter by a federal grand jury for records pertaining to the intervenor's identity); United States v. Kearney, 672 F.3d 81, 84-85 (1st Cir. 2012) (law enforcement used account and IP address information obtained from MySpace via an administrative subpoena to subpoena defendant's internet provider for his name and address).

[107] *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").

[108] *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).

[109] *See, e.g.*, Hubbard v. MySpace, Inc., 788 F. Supp. 2d 319 (S.D.N.Y. 2011) (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 (acknowledging the privacy settings of the user, the court quashed subpoenas seeking private messages on Facebook and MySpace as they were protected under the Stored Communications Act).

[110] 18 U.S.C. § 2703(c)(2); *id.* § 2703(d).

[111] Warshak, 631 F.3d at 282-83 (citation omitted).

[112] *Id.*

[113] *Id.* at 288.

[114] *Id.* (citations omitted).

[115] *Id.* at 285-286.

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

[117] *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).

[118] *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).

[119] 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.

[120] *Id.*

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

[122] 18 U.S.C. § 2703.

[123] 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.

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

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

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

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

[128] *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").

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

[130] 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).

[131] *Id.* at 2.

[132] *Id.*

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

[134] *See, e.g.,* People v. Lesser, No. H034189, 2011 WL 193460, at *4 (Cal. Ct. App. Jan. 21, 2011) (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) (conviction upheld where the court correctly admitted a trial exhibit consisting of printouts of defendant's MySpace page, which the prosecution's gang expert relied on in forming his opinion that defendant was an active gang member); People v. Fielding, No. C06022 , 2010 WL 2473344, at *4-5 (Cal. Ct. App. June 18, 2010) (incriminating MySpace messages sent by defendant authenticated by victim who testified he believed defendant had sent them; inconsistencies and conflicting inferences regarding authenticity goes to weight of evidence, not its authenticity).

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

[136] *Id.* at 635.

[137] *Id.* at 647.

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

[139] *Id.* at *4.

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