The ESI Tsunami

A Comprehensive Discussion about Electronically Stored Information in Government Investigations and Criminal Cases

BY JUSTIN P. MURPHY & MATTHEW A.S. ESWORTHY

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, social media, Fourth Amendment issues, and postindictment discovery.

Subpoena Compliance

The duty to preserve ESI. In a typical criminal investigation, one of the first e-discovery issues confronted by defense counsel is the need to identify and preserve relevant ESI. Civil litigators also must deal with this issue at the outset of a case, but there is an important distinction: The consequences—both direct and collateral—of failing to preserve relevant evidence can be far more severe in criminal cases. Thus, the problems presented by voluminous, widely dispersed, and constantly changing ESI can be particularly acute.

The first step is determining when a duty to preserve ESI has been triggered. Service of a subpoena or some other government demand is an obvious trigger, but the

Published in *Criminal Justice*, Volume 27, Number 1, Spring 2012.

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." (*The Sedona Conference Commentary on Legal Holds*, Sedona Conf. (Aug. 2007), http://tinyurl.com/8xn7bns; *see also* Zubulake v. UBS Warburg LLC, 229 F.R.D. 422 (S.D.N.Y. 2004).) 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 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. (*See* 18 U.S.C. § 1519 (punishing document destruction in "contemplation" of a federal investigation).)

Once the duty to preserve arises, one must move quickly to understand the ESI that may be implicated and implement a hold order that tracks the government's information request (if it is available) to ensure that employees are on notice of the types of ESI that must be maintained. One should ask these simple questions: What ESI am I losing today if I do not take steps to preserve it? What ESI will be gone tomorrow if I do not, for example, suspend document retention policies or auto-delete functions? It is also becoming a standard in criminal practice to forensically image hard drives—especially for "key" players. In addition, a forensic expert may prove helpful to the assessment and successful preservation of ESI in an enterprise environment.

Unlike in civil litigation, special preservation challenges can arise in government investigations or the criminal context when a matter must be kept confidential. In these situations, there may be limits to the extent to which counsel may communicate with custodians of potentially relevant materials, such as through a widely distributed hold order or other steps to preserve materials. In some situations, counsel may consider conferring with the government to reach an agreement on how to balance the need for secrecy against the need to preserve relevant information.

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. (*See* U.S. Sentencing Guidelines Manual § 8C2.5 (2004).)

Importantly, preservation failures can also expose the client to an 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 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. Most prosecutors are keenly aware of the potential ramifications of failures to preserve evidence and the leverage that can result. (*See, e.g.*, *In re* Grand Jury Investigation, 445 F.3d 266 (3d Cir. 2006) (applying the crime-fraud exception to call defense counsel before the grand jury when it was believed that the target destroyed emails after receipt of the grand jury subpoena).)

There are additional consequences as well. The preservation of ESI, or lack thereof, may impact your client's status in the investigation, particularly if your client finds himself or herself in a middle ground. If for example, upon receipt of a subpoena, you take good-faith steps to preserve data and comply with the subpoena, the prosecution may view your client in a more favorable light. If, on the other hand, ESI has been deleted or destroyed, your client may quickly find himself or herself at the other end of the spectrum.

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*, No. 09-932 (JLL), 2010 WL 4226524 (D.N.J. Oct. 21,

JUSTIN P. MURPHY *is a counsel at Crowell & Moring's Washington, D.C., office, where he practices in the White Collar & Regulatory Enforcement Group and E-Discovery and Information Management Group. His practice focuses on SEC enforcement, white collar criminal matters, e-discovery matters relating to internal and government investigations, and related civil litigation. He is also a member of the* Criminal Justice *magazine editorial board.* **MATTHEW A.S. ESWORTHY** *is a partner in the litigation department of Shapiro Sher Guinot & Sandler in Baltimore, Maryland. He concentrates his practice on general civil and criminal litigation, including white collar criminal defense, complex commercial litigation, securities litigation, partnership disputes, employment law, and appeals. He is also cochair of the ABA Criminal Justice Section's Cyber Crime Committee. The authors are cochairs of the panel discussion "E-Discovery in Government Investigations and Criminal Litigation" at the ABA Criminal Justice Section Spring Conference in Los Angeles in April.*

2010), the government failed to preserve numerous text messages exchanged between a key cooperating witness and FBI agents involved in a public corruption investigation. (*Id.* at *1.) 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, provided an adverse inference instruction to the jury that permitted the jury to infer that the missing text messages were relevant and favorable to the defendants. (*Id.* at *8.) The jury ultimately acquitted the defendant, who argued that the missing text messages were important.

Finally, it is notable that the mishandling of ESI by private litigants in civil actions can also lead to criminal penalties. In one case, the district court determined that the defendants could be prosecuted under 18 U.S.C. section 1503 for allegedly withholding and then destroying documents sought by plaintiffs' counsel during discovery in a civil discrimination lawsuit between private parties. (*See* United States v. Lundwall, 1 F. Supp. 2d 249 (S.D.N.Y. 1998).) Courts have also referred cases to US 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, 587 F. Supp. 2d 951 (N.D. Ill. 2008) (ordering defendant to show cause why issue of false declaration should not be referred to US Attorney's office, rather than a direct referral); SonoMedica, Inc. v. Mohler, No. 1:08-cv-230 (GBL), 2009 WL 2371507 (E.D. Va. July 28, 2009) (finding third parties in contempt for violation of court's orders, including spoliation of ESI, and referring case to US Attorney's office for criminal investigation).)

Conferring with the government on ESI issues. Federal Rule of Civil Procedure 26(f) requires that parties meet and confer to identify, address, and try to avoid problems with ESI early in the litigation process. There is no criminal meet-and-confer rule similar to Federal Rule of Civil Procedure 26(f), but the need to identify and address ESI issues early on is equally important—if not more important—in a government investigation or criminal matter, given the significant consequences. However, reaching agreement with the government can be more challenging because the symmetry of risks and interests between the two parties that is common in civil litigation generally does not exist in a government investigation. In contrast to civil matters, the government may not be as concerned about the "boomerang" effect of imposing significant burdens on the defense.

Before engaging in such discussions with the government, counsel must first understand their client's ESI, including where it is located, what materials are in the client's possession, custody, and control, and how they may be preserved and ultimately collected in a cost-effective manner. Again, it may prove helpful to have a forensic specialist assist with the identification, preservation, and collection of potentially relevant material, not only to help ensure the job is done correctly, but to assist in communicating clearly and effectively with the government. These experts may also help convince the government that the most relevant ESI can be produced without incurring unnecessary expense, and to serve as an independent expert if questions or issues subsequently arise.

After taking the necessary steps to understand your client's systems and to ensure that ESI is being preserved, counsel should communicate with the government and consider a discussion similar to the Rule 26(f) conference. Such discussions can help avoid problems down the road and allow productions to occur in a more effective, efficient, and timely manner. For example, both counsel and the government should reach a common understanding on the scope of the production, including items such as the date ranges of materials to be reviewed and produced, the specific custodians whose ESI will be examined, the use of search terms, advanced technologies, or other filters to cull the data prior to review and production, and the form of production to the government. If necessary, this dialogue with the government should be ongoing and continuous, in an effort to prioritize and focus the ultimate production of ESI. At the end of the day, there is a potential burden on both the defense and the government, neither of which benefits from backing up the electronic dump truck to the government's door, especially in large volume cases.

There are more subtle benefits to these discussions as well. This dialogue may provide defense counsel with their first opportunity to influence and affect how the government will view the client, especially in situations where a corporate client may potentially be on the hook for the devious conduct of "rogue employees." Moreover, discussions relating to which custodians should be considered "key" and which aspects of the government's request are most important may provide valuable insight into the government's case that the prosecutor would otherwise be reluctant to reveal.

Finally, if counsel uncovers intentional efforts by "rogue employees" to delete or otherwise alter relevant ESI in response to an investigation, such incidents should be addressed immediately. By quickly investigating such matters, taking all reasonable steps to remedy the situation (for example, by restoring deleted materials from backup tapes or through other forensic methods), and, in certain circumstances, reporting the conduct promptly to the government, a company may earn a free pass on obstruction issues while the government pursues the employees involved.

Social Media, the Internet, and Admissibility

The Internet, and social media in particular, represents

the new frontier of information that can be critical in defending a criminal matter. Through a vast array of publicly available sources—government records; property records; licensing and disciplinary records; the media, including blogs, and social media such as LinkedIn, MySpace, and Facebook—one can gather evidence to present an alternative theory of the case, challenge the government's evidence, assist in motion practice, and call into question the credibility and/or motives of cooperating witnesses. However, there are challenges, as well as ethical issues, in using the Internet for fact finding.

Information contained on social media sites presents a unique challenge for private litigants as well as the government, because information is often maintained by third-party providers, and there is developing law that treats certain information stored on social media websites as "private" and subject to the Stored Communications Act. (18 U.S.C. § § 2701 *et seq*. *See, e.g.*, Hubbard v. MySpace, Inc., 788 F. Supp. 2d 319 (S.D.N.Y. 2011) (holding that the 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 e-mail was sufficient to satisfy the requirements of the Stored Communications Act); *but see* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010) (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).) Under this developing law, a civil subpoena would not be sufficient, or for that matter, appropriate to obtain "private" information such as e-mails or instant message communications stored on a social media website or a private web-based e-mail account. (*See* Theofel v. Farey-Jones, 359 F.3d 1066, 1071–72, 1077 (9th Cir. 2004) (finding that an overbroad civil subpoena to plaintiff's Internet service provider violated the Stored Communications Act).)

It also bears noting that even when Internet postings are removed, they still may be accessible. For example, one effective tool for retrieving past "public" Internet postings is the Internet Archive: Wayback Machine, http://www.archive.org/web/web.php. One of the purposes of websites like Internet Archive is to offer permanent access for researchers, historians, scholars, people with disabilities, and the general public to historical collections that exist in digital format. Being able to look back in time at the changes to a website could prove to be invaluable, particularly in a case where social media is a focal point.

Attorneys can run afoul of ethics rules when they use social media to gather evidence that is not publicly available. For example, both the New York State Committee on Professional Ethics and the Philadelphia Bar Association's Professional Guidance Committee agree that it is unethical for an attorney to obtain information from an opposing party or witness by misrepresenting one's identity on a social media website. (*See* New York Comm. on Prof'l Ethics, Op. 843 (Sept. 10, 2010) (concluding that an attorney may not deceptively "friend" a potential witness in order to thwart privacy settings and gain access to information); *and* Phil. Prof'l Guidance Comm., Op. 2009-02 (March 2009) ("a third-party friend request to an adverse witness for impeachment evidence violates Pennsylvania Professional Conduct Rules 4.1 and 8.4(c)).)

Attorneys may also violate ethical rules by blogging about criminal proceedings. In a recent Virginia State Bar ethics decision, an ethics panel found that a criminal defense attorney violated Virginia lawyer conduct rules by including clients' names in his blog postings without their consent. (*See In re* Hunter, VSB No. 11-032-084907 (Nov. 8, 2011).) In addition, since the attorney's blog was hosted on his firm's website, the ethics panel found that such postings constituted advertising, and therefore the website should have included an appropriate disclaimer required by rules governing lawyer advertising.

ESI is subject to the same rules of evidence as hard copy documents, but the technical nature of ESI—and of social media and Internet sources in particular—create challenges and potential hurdles to admissibility not found with paper documents. As a result, it is critical to consider how you will authenticate and admit the information being gathered, at the time you preserve and collect that information. For example, will you memorialize each step of the collection and production process to enhance reliability? Will you use opportunities during discovery to authenticate potential evidence, or will you provide the court with sufficient evidence to understand technological issues as they relate to the reliability of your evidence? Will you authenticate the information by using witnesses 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 will you attempt to obtain the information in question from the actual website where it appeared?

Notably, when it comes to dynamic and fluid information in digital form, bad actors can manipulate time stamps and content with ease. Establishing authenticity and admissibility poses a challenge that only grows more onerous with the constant evolution of new methods of hacking into and altering files. Any witness providing testimony to authenticate ESI can be cross-examined to reveal potential flaws in digital images or data one takes for granted. In the context of litigation, every electronic document's authenticity can be called into question.

An inexpensive tool available to attorneys to assist with the admissibility of ESI is the digital notary. A digital notary attests to the authenticity of a digital item as it is reflected at a particular date and time. In simple terms, digi-

tal notaries "seal" a digital item with specialized software in order to preserve the integrity of the item and digitally date and timestamp the item. Digital notaries perform a wide variety of services, including the authentication of the data on computer hard drives, e-mails, website ESI, Internet postings, digital photographs, and text messages or instant messages. The uses of digital notaries are only limited by the creativity of the attorney involved.

Given the challenges for authenticating Internet and social media sources of information, at this stage courts seem to be erring on the side of admissibility, and any concerns about the evidence itself—for example, contradictory testimony about whether or not someone authored a Facebook posting—is being left to the jurors to decide what weight that evidence should be given. (*See, e.g.*, People v. Valdez, 201 Cal. App. 4th 1429 (2011) (upholding conviction where the court correctly admitted a trial exhibit consisting of printouts of defendant's MySpace page, which the prosecution's gang expert relied on in forming his opinion that defendant was an active gang member); People v. Lesser, No. H034189, 2011 WL 193460 (Cal. App. Jan. 21, 2011) (concluding that officer's testimony that he cut and pasted portions of Internet chat transcript was sufficient for admissibility); State v. Thompson, 777 N.W.2d 617 (N.D. 2010) (finding victim's knowledge of defendant's cell phone number and defendant's "signature" on text messages sufficient to authenticate threatening text messages). *But see* Commonwealth v. Koch, 2011 WL 4336634 (Pa. Super. Ct. Sept. 16, 2011) (finding text messages inadmissible because authentication requires more than mere confirmation that the cell phone belongs to a specific person).)

Admissibility is just one challenge that the Internet and social media pose at trial. Recently, there has been an increasing trend of jurors using wireless communication devices to look up a defendant's criminal record, conducting their own investigation into a case, posting their opinions about the case on social media websites, or attempting to "friend" parties, lawyers, witnesses, or judges. In some instances, this conduct has resulted in mistrials or overturned convictions. (*See* Dimas-Martinez v. Arkansas, 2011 Ark. 515 (2011) (reversing murder conviction and calling for new trial where juror tweeted during court proceedings; in one tweet, the juror wrote "Choices to be made. Hearts to be broken . . . We each define the great line," and then before the jury announced its verdict, he posted: "It's over").) In response to this trend, California has adopted a new statute that clarifies that jurors may not use social media and the Internet—such as texting, Twitter, Facebook, and Internet searches—to research or disseminate information about cases, and can be held in criminal or civil contempt for violating these restrictions. (*See* 2011 Cal. Laws ch. 181; United States v. Fumo, 655 F.3d 288 (3d Cir. 2011) (providing detailed sample jury instructions relating to the use of electronic technology to research or communicate about a case).)

ESI and the Fourth Amendment

The unique challenges presented by the very nature of ESI create problems in the context of search warrants as well. Specifically, our 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." A landscape of sometimes conflicting case law is developing as courts wrestle with this conundrum.

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. Overseizure of ESI is often the result because of the practical realities of onsite 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 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—filing cabinets that can store unimaginable volumes of data.

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. (*See* United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989 (9th Cir. 2009).) 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 the individuals 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." (*Id.* at 998.) 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." (*Id.* at 1006.) In an attempt to ensure such vigilance, the court established the following explicit requirements:

> 1. Magistrates should insist that the government waive reliance upon the plain view doctrine in digital evidence cases.
>
> 2. Segregation of non-responsive materials [either] must be done by specialized personnel who are walled off from the case agents, or an independent third party.
>
> 3. Warrants must disclose the actual risks of destruction of information, as well as prior efforts to seize that information in other judicial fora.
>
> 4. The government's search protocol must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents.
>
> 5. The government must destroy or return non-responsive data, keeping the issuing magistrate informed about when it has done so and what it has kept.

(*Id.*)

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. (*See* United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1177–80, 1183 (9th Cir. 2010).) 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*, 694 F.2d 591 (9th Cir. 1982). (*Comprehensive Drug Testing*, 621 F.3d at 1180.) 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. (*Id.* at 1169–71.) 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." (United States v. Comprehensive Drug Testing, Inc., 513 F.3d 1085, 1106 (9th Cir. 2008) (quoting *Tamura*, 694 F.2d at 596).) 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." (*Comprehensive Drug Testing*, 621 F.3d at 1177.)

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." He added, "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." (*Id.* at 1178.)

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." (*Id.* at 1176.)

How other circuits treat 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 Sixth Circuit is the most recent court to grapple with this issue, in *United States v. Richards*, 659 F.3d 527 (6th Cir. 2011). In *Richards*, the court 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." (*Id.* at 538.)

The defendant in *Richards* was the target of an FBI investigation involving the commercial production, advertising, sale, and distribution of child pornography. (*Id.* at 531.) The FBI executed multiple search warrants to retrieve remote servers in Los Angeles and San Francisco that hosted the various websites maintained by the defendant that involved child pornography. (*Id.* at 532.) The FBI also seized items from the defendant's residence in Nashville, Tennessee. (*Id.*) The defendant challenged the seizure of the entire server located in California on the grounds that the warrant only authorized the seizure of the sections of the server hosting the pornographic website. (*Id.* at 535.) The district court denied the defendant's motion to suppress, concluding that the warrant was not impermissibly overbroad. (*Id.* at 536.)

The Sixth Circuit ultimately adopted "the Fourth Amendment's bedrock principle of reasonableness on a case-by-case basis," *id.* at 538, 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. (*Id.* at 541.) Notably, Judge Moore, in her concurring opinion, expressed concern with the majority's rule, 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." (*Id.* at 552 (Moore, J., concurring).) 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. (*Id.* at 558 (Moore, J., concurring).) 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." (*Id.*)

United States v. Stabile, 633 F.3d 219 (3d Cir. 2011) is another recent decision addressing the issue of "overseizure" of evidence under the plain view doctrine. In *Stabile*, agents went to the defendant's home to question him regarding allegations that he was involved in counterfeiting and other financial crimes. (*Id.* at 224.) 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. (*Id.* at 225.) The agents seized several computer hard drives from the home, and discovered child pornography on the hard drives. (*Id.*)

While the court in *Stabile* declined to follow the Ninth Circuit's suggestion in *United States v. Comprehensive Drug Testing*, 621 F.3d 1162, 1178 (9th Cir. 2010) (Kozinski, J., concurring) 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." (*Stabile*, 633 F.3d at 241.) 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.'" (*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*, 592 F.3d 779, 785 (7th Cir. 2010), acknowledged the value of the guidelines articulated in *Comprehensive Drug Testing*. There, 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.*)

Only one federal appeals court has flatly disagreed with the *Comprehensive Drug Testing* decision: the Fourth Circuit in *United States v. Williams*, 592 F.3d 511, 515-17 (4th Cir. 2010), which held that the search warrant impliedly 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. (*Id.* at 521–22.) There, the court reasoned that in order to be effective, a search cannot be limited to reviewing only file designations or labeling as these things can easily be manipulated. (*Id.* at 522.) 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." (*Id.*) Under the Fourth Circuit's interpretation of the plain view doctrine—which permits officers to rummage throughout a seized computer—one is left to wonder what, if anything, is left of the particularity requirements of the Fourth Amendment. The analysis in *Williams* begs the question that if an officer has to "click" around to open each file, is the evidence really in plain view?

Increasing judicial skepticism. 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. (*In re* Application for Search Warrant, Mag. No. 09-320 (D.D.C. June 3, 2009) (Facciola, M.J.).) 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." (*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").)

This skepticism is well-founded. Computers today can store volumes of data that were unimaginable at the time the Fourth Amendment was created, and in investigations and cases dealing with such volumes, digital evidence warrants must be scrutinized carefully. Courts should appropriately test the government's evidence in support of probable cause, and ensure that the place to be searched is described with particularity. And, in the case of computers, that the computer itself, and the places to be searched within the computer, be described virtually.

Warrantless searches of cellular telephones. 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. (See, e.g., 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. 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. Hill, No. CR 10-00261 (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. Wurie, 612 F. Supp. 2d 104, 110 (D. Mass. 2009); United States v. Santillan, 571 F. Supp. 2d 1093, 1102–03 (D. Ariz. 2008); United States v. Deans, 549 F. Supp. 2d 1085, 1094 (D. Minn. 2008) (agreeing with the Fifth Circuit that "if a cellphone is lawfully seized, officers may also search any data electronically stored in the device").)

Other courts have invalidated warrantless searches of cell phones seized incident to arrest. (*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) (supressing search of a cell phone an hour after the arrest).)

Recently, the court in *United States v. Gomez*, 807 F. Supp. 2d. 1134, 1145–50 (S.D. Fla. 2011), 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.

(*Id.* at 1149.)

State courts around the county are also divided on the cell phone issue. The California Supreme Court in *People v. Diaz*, 244 P.3d 501 (Cal. 2011), recently affirmed the denial of a motion to suppress a text message found on the 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 per-

son. (*Id.* at 502.) 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. (*Id.*) The *Diaz* court found that the cell phone was personal property immediately associated with the defendant's person; therefore, the search was valid despite the 90-minute lapse in time between the cell phone being seized and being searched. (*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 (Senate Bill 914), but this bill was vetoed by Governor Jerry Brown.

Warrantless use of GPS tracking devices. The United States Supreme Court recently 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. (*See* United States v. Jones, 132 S. Ct. 945 (2012).) The underlying case, *United States v. Maynard*, 615 F.3d 544, 559 (D.C. Cir. 2010), involved two nightclub owners in the District of Columbia (Antoine Jones and Lawrence Maynard) who were under investigation for narcotics violations. (*Id.* at 549.) During the investigation, officers attached a GPS device to Jones's vehicle without a warrant. (*Id.* at 558–59.) The GPS device tracked Jones's movements 24 hours a day for one month. (*Id.*) *Maynard* 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. (*Id.* at 559.) The court of appeals 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." (*Id.* at 562. *But see* United States v. Sparks, 750 F. Supp. 2d 384, 392–93 (D. Mass. 2010) (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) (holding that warrantless GPS tracking of the defendant did not violate the Fourth Amendment because the defendant could not claim a reasonable expectation of privacy in his driveway, even if a portion of the driveway was located within the curtilage of the home).)

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." (*Jones*, 132 S. Ct. at 949.) 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." (*Id.* at *7.)

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), 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." (*Id.* at 964) (citation ommitted.) The court's reluctance to "grapple with these 'vexing problems'" 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. (*Id.* at 954.)

Postindictment Discovery

Form of production. Although the Federal Rules of Criminal Procedure do not specifically address e-discovery, the influence of the Federal Rules of Civil Procedure on criminal practice in this area is already apparent. In *United States v. O'Keefe*, 537 F. Supp. 2d 14 (D.D.C. 2008), the court held that a document production by the government must adhere to standards similar to those set forth in Rule 34 of the Federal Rules of Civil Procedure. In *O'Keefe*, the court noted that there was no rule in criminal cases to guide courts in determining whether a production of materials by the government has been in an appropriate form or format. (*Id.* at 18–19.) Recognizing that the "big paper case" would be the exception rather than the rule in criminal cases, the court observed that the "Federal Rules of Civil Procedure in their present form are the product of nearly 70 years of use and have been consistently amended by advisory committees consisting of judges, practitioners, and distinguished academics to meet perceived deficiencies. It is

foolish to disregard them merely because this is a criminal case, particularly where . . . it is far better to use these rules than to reinvent the wheel when the production of documents in criminal and civil cases raises the same problems." (*Id.*) *O'Keefe*'s importation of the civil rules into a criminal case has been advanced by other criminal defendants and has been acknowledged by a US Attorney's bulletin. (*See* Motion to Compel Discovery Pursuant to *Brady v. Maryland* and Fed. R. Crim. P. 16, United States v. Stevens, 2008 WL 8743218 (D.D.C. Dec. 19, 2008) (No. 08-231 (EGS)), 2008 WL 4153746. ("[E]ven civil litigants must either produce documents as they are kept in the course of business or label the documents in response to requested subject areas. Where the government produces documents in 'an undifferentiated mass in a large box without file folders or labels, then these documents have not been produced in the manner in which they were ordinarily maintained as [Fed. R. Civ. P. 34] requires' and thus the government has equally failed to meet its obligations under Fed. R. Crim. P. 16."); Andrew Goldsmith & Lori A. Hendrickson, Investigations and Prosecutions Involving Electronically Stored Information, Address at ALI-ABA Electronic Information: The Investigation, Prosecution and Defense of Crimes Seminar (Dec. 2, 2010) (in citing *O'Keefe*, noting that "[p]rosecutors should be aware that federal judges may hold them to certain standards common to civil litigation").)

In addition to *O'Keefe*, there are several district courts that have adopted local rules that import civil principles, including requiring a discussion amongst the parties about the volume of ESI, the form of production, and the litigation capabilities of counsel. (*See, e.g.*, General Order Regarding Best Practices for Electronic Discovery of Documentary Materials in Criminal Cases, *In re* Best Practices for Electronic Discovery of Documentary Materials in Criminal Cases, No. G.O. 09-05 (W.D. Okla. Aug. 20, 2009), *available at* http://tinyurl.com/yaq2cg7; Northern District of California Suggested Practices Regarding Discovery in Complex Cases and Northern District of California Protocol Regarding Discovery in Complex Cases; U.S. Att'y's Off., W.D. Wash., Best Practices for Electronic Discovery of Documentary Materials in Large Cases (Sept. 2005), *available at* http://tinyurl.com/6snfqwx.)

One court has declined to follow *O'Keefe*'s rationale (requiring the production of documents in a specific format under Federal Rule of Civil Procedure 34 in criminal cases), *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). In *Warshak*, the Sixth Circuit noted that Federal Rule of Criminal Procedure 16 is "entirely silent on the issue of the form that discovery must take; it contains no indication that documents must be organized or indexed." (*Id.* at 296.) However, the dispute in *Warshak* was notably about the government's production of ESI that was seized from the defendants themselves, who had equal and ready access to the information being produced by the government. The Sixth Circuit highlighted that any difficultly the defendants experienced in accessing the government's production could be attributed to the defendants' poor organization of the ESI it maintained. (*Id.*)

While some have lauded *Warshak* as the end of *O'Keefe* and the importation of civil rules into criminal practice, recently *United States v. Briggs*, No. 10CR184S, 2011 WL 4017886, (W.D.N.Y. Sept. 8, 2011), breathed new life into the approach taken by the *O'Keefe* court. (*See* Andrew D. Goldsmith, *Trends—or Lack Thereof—in Criminal E-Discovery: A Pragmatic Survey of Recent Case Law*, 59 U.S. Att'y Bull. 3 (2011).) In *Briggs*, the court, applying Rule 34(b)(2)(E)(ii), ordered the government to re-produce ESI "in a reasonably usable form or forms," following the government's data dump. (*Briggs*, 2011 WL 4017886, at *8.) The court found that in the absence of an express criminal procedure rule addressing the manner of production, and under the court's inherent authority under Federal Rule of Criminal Procedure 16(d), the government was the party "better able to bear the burden of organizing these records for over twenty defendants in a manner useful to all." (*Id.*) In support of the decision to order the government to reproduce the discovery, the court noted:

> Use of the conveniences of electronic storage avoids the problems of the warehouses full of documents and "docu-dump" discovery prevalent in civil practice almost a generation ago. But these techniques are also being used in criminal practice. While the rules for such ESI have been developed (and are being fleshed out) on the civil side of litigation, this case gives the example of the need for a more uniform regime on the criminal side. It is hoped that the Advisory Committee on Criminal Rules will take note of the omission and address it at the earliest opportunity. Until then, and to decide the motions before this Court, **the Government is to bear the burden of reproducing these ESI materials in a fashion that defendants can retrieve and manipulate** as discussed in this Order.

(*Id.* at *9.)

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*, 554 F.3d 529 (5th Cir. 2009), 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." (*Id.* at 576.) 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." (*Id.*)

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." (*Id.* at 577.) 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*, No. S-10-0061, 2010 WL 3036444 (E.D. Cal. Aug. 2, 2010), 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)." (*Id.* at *2.) *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. (*Id.* at *7.) 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.

(*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." (*Id.* at *6.) "[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." (*Id.*) 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.

(*Id.* at *5; *but see* United States v. Rubin/Chambers, Dunhill Ins. Serv., 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).)

For those representing indigent clients, or clients of limited financial means, *Salyer* is a step in the right direction, but not a complete solution. Consider the difficulties associated with tackling a government production of 10,000 electronic documents when there are no resources, no technical support, and limited access to your client who is likely incarcerated. In situations such as this, dealing with 10,000 documents is just as daunting as reviewing productions of millions of documents, each which may contain exculpatory evidence.

Speedy trial issues in 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. (United States v. Graham, No. 1:05-CR-45, 2008 WL 2098044, at *2–3 (S.D. Ohio May 16, 2008). *See also* State v. Dingman, 202 P.3d 388 (Wash. Ct. App. 2009) (reversing conviction and remanding for new trial after finding that trial court erred by denying defendant meaningful access to hard drives seized from his house).) 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." (*Graham*, 2008 WL 2098044, at *5.) 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." (*Id*. at *8. *But see* United States v. Qadri, No. 06-00469, 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).)

Conclusion

E-discovery issues cut across various phases of government investigations and criminal cases, and the law in this area continues to evolve rapidly and increase in complexity. Both defense counsel and the government are faced with skyrocketing volumes of data, the costs and resources associated with handling those extraordinary volumes, and the continuing developments in ESI jurisprudence. Those failing to appreciate and understand their e-discovery obligations do so at the risk of committing critical mistakes that affect the outcome of the case. ■