May
2011
Volume 59
Number 3

United States
Department of Justice
Executive Office for
United States Attorneys
Washington, DC
20530

H. Marshall Jarrett
Director

Contributors' opinions and statements should not be considered an endorsement by EOUSA for any policy, program, or service.

The United States Attorneys' Bulletin is published pursuant to 28 CFR § 0.22(b).

The United States Attorneys' Bulletin is published bimonthly by the Executive Office for United States Attorneys, Office of Legal Education, 1620 Pendleton Street, Columbia, South Carolina 29201.

Managing Editor
Jim Donovan

Law Clerk
Carmel Matin

Internet Address
www.usdoj.gov/usao/reading_room/foiamanuals.html

Send article submissions and address changes to Managing Editor,
United States Attorneys' Bulletin,
National Advocacy Center,
Office of Legal Education,
1620 Pendleton Street,
Columbia, SC 29201.

E-Discovery

In This Issue

Introduction to the E-Discovery Issue of the USABulletin

The Hon. Thomas J. Perrelli
Associate Attorney General of the United States

The Administration has pledged, in area after area, to make better use of technology to improve the delivery of services to its citizens. As attorneys for the federal government, we must make sure that the realities of the digital era are not ignored when it comes to representing the Government's interests in court. While the Government has made significant strides in its handling of E-Discovery, much work remains to be done. The Department of Justice is committed not only to handling electronic discovery properly, but also to supporting federal agencies as they lay the groundwork for fulfilling their own responsibilities with regard to E-Discovery. The Department, therefore, has undertaken a major commitment geared toward improving its capabilities and assisting federal agencies as they seek to improve their performance.

First, the Department has formed a new Civil E-Discovery Committee, comprised of legal and technical representatives across all of the civil litigating components (Antitrust Division, Civil Division, Civil Rights Division, Environment and Natural Resources Division, Executive Office for United States Attorneys, Tax Division, and the Civil Divisions within the United States Attorneys' offices). The Committee has been working on a number of initiatives, such as developing new legal and technical E-Discovery training programs for DOJ litigators and agency personnel, as well as creating new Department-wide Civil E-Discovery guidance and best practices in both defensive and affirmative litigation. Second, DOJ components have designated civil attorneys who focus on E-Discovery issues full-time for the component, and each office has designated a civil Electronic Discovery Office Coordinator (EDOC) to serve as an accessible, knowledgeable resource for our litigators. Almost all of the Department's EDOCs completed specialized training at the National Advocacy Center in 2010. This year, we are focused on improving the capabilities of the technical staff critical to supporting the work of the litigators in E-Discovery. All EDOC technical personnel will be offered E-Discovery training at the National Advocacy Center this year.

It is important that everyone involved in civil litigation be prepared to meet and address the challenges faced by E-Discovery. I encourage you to take advantage of the new training programs, guidance, and the EDOC attorneys who are in place to assist you. If you have any questions or concerns, you can contact Sarah Michaels Montgomery, who is serving as DOJ's Senior Litigation Counsel for E-Discovery while on detail to my office. Sarah.M.Montgomery@usdoj.gov. 202-514-9500.

Sincerely,
The Hon. Thomas J. Perrelli
Associate Attorney General of the United States

Trends – Or Lack Thereof – In Criminal E-Discovery: A Pragmatic Survey of Recent Case Law

Andrew D. Goldsmith
National Criminal Discovery Coordinator
Department of Justice

Disclosure of electronically stored information (ESI) has been playing a gradually increasing role in criminal prosecutions. While civil litigators have grappled with discovery of ESI for years–for example, discovery of ESI was explicitly incorporated into the Federal Rules of Civil Procedure in December 2006–criminal law has lagged behind. For ESI, prosecutors have similar disclosure obligations as they have for traditional hard copy documents and records. *See* the Jencks Act, 18 U.S.C. § 3500; FED. R. CRIM. P. 16; *Giglio v. United States*, 405 U.S. 150 (1972); *Brady v. Maryland*, 373 U.S. 83 (1963). Yet, a coherent body of case law on appropriate collection, management, and disclosure of ESI has yet to emerge in the criminal context. This vacuum of case law has led to a recent phenomenon in which practitioners and commentators, in an effort to make sense of the case law–and perhaps help publish articles–have cited unrelated and sometimes unreported cases from across the country, played "connect the dots," and announced trends. This article, by contrast, provides a practical survey of recent criminal E-Discovery and ESI search and seizure case law, and identifies the single trend arising from that case law.

I. Introduction to ESI in the criminal context

For federal prosecutors, ESI arises in two contexts: the first is the prosecutor's affirmative efforts. This includes the prosecutor's efforts to obtain ESI during an investigation, use it at trial, and prosecute obstruction offenses involving its improper manipulation. The second context, disclosure, concerns materials the prosecutor must turn over to the defense before or during trial. With the exception of section eight (which contains some important new case law on search and seizure), this article deals primarily with government disclosure of ESI. For a more complete examination of affirmative use of ESI, *see* Andrew D. Goldsmith & Lori A. Hendrickson, *Investigations and Prosecutions Involving Electronically Stored Information*, Vol. 56, No. 3, United States Attorneys' Bulletin 27 (May 2008).

It bears repeating that the same disclosure requirements and procedures for "traditional" discovery generally apply to ESI. With certain exceptions, the form of the information generally does not affect its discoverability. For example, material exculpatory information must be disclosed under *Brady* whether it exists in a letter, an email, a voice mail, or it was disclosed to the prosecutor during a face-to-face conversation.

The government's constitutional obligations under *Brady* and *Giglio* only apply to evidence that is "material," i.e., where "there is a reasonable probability that, had the evidence been disclosed to the defense, the result of the proceeding would have been different." *United States v. Bagley*, 473 U.S. 667, 668 (1985). As the Supreme Court further explained in *Kyles v. Whitley*, 514 U.S. 419 (1995), undisclosed evidence is material only if it "could reasonably be taken to put the whole case in such a

different light as to undermine confidence in the verdict." *Id.* at 435. The United States Attorneys' Manual (USAM) requires broader disclosure in several ways, however. For example, whereas *Brady* and *Giglio* jurisprudence has tended to focus on evidence, USAM policy applies to information, whether or not it is admissible evidence. USAM 9-5.001(C). The USAM recognizes the materiality element of *Brady* and *Giglio* information, but requires broader disclosure than is required under the Constitution or the law. Under the USAM, and absent countervailing considerations, prosecutors must disclose information that is inconsistent with any element of any crime, or that establishes a recognized affirmative defense, regardless of whether the prosecutor believes such information will make the difference between conviction and acquittal. USAM 9-5.001(C)(1). Similarly, *Giglio* impeachment evidence must be disclosed to the defense even if it may not make the difference between conviction and acquittal. USAM 9-5.001(C)(2).

USAM 9-5.001(C) further states: "a fair trial will often include examination of relevant exculpatory or impeachment information that is significantly probative of the issues before the court but that may not, on its own, result in an acquittal or, as is often colloquially expressed, make the difference between guilt and innocence." Thus, under the USAM, prosecutors must disclose favorable information beyond that which is "material" to guilt. *See Kyles v. Whitley*, 514 U.S. 419 (1995); *Strickler v. Greene*, 527 U.S. 263, 280-81 (1999). Nevertheless, the USAM does not require information that is irrelevant, not significantly probative of the issues before the court, or involves spurious issues or arguments which serve to divert the trial from genuine issues to be disclosed. USAM 9-5.001(C). It is important to note, however, that the USAM does not have the force of law or create or confer any rights. It is merely guidance for prosecutors and is, of course, subject to legal precedent, court orders, and local rules. *See United States v. Caceres*, 440 U.S. 741 (1979); *see also United States v. Montoya*, 45 F.3d 1286, 1295 (9th Cir. 1995) ("[F]ailure to strictly comply with the United States Attorneys' Manual creates no enforceable rights.") (internal citations omitted); *United States v. Lorenzo*, 995 F.2d 1448, 1453 (9th Cir. 1993) ("[T]he U.S. Attorneys' Manual is not intended to, does not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any party in any matter civil or criminal.") (internal citations and quotations omitted).

II. The limited application of civil ESI principles in criminal cases

Given the practical importance and potential constitutional magnitude of ESI-related issues in criminal cases, practitioners and commentators have tried to knit together the existing case law to divine trends in the direction of the law. *See, e.g.*, Justin P. Murphy, *E-discovery in Criminal Matters–Emerging Trends and the Influence of Civil Litigation Principles*, SEDONA CONFERENCE INSTITUTE (2010); Norman C. Simon, et. al, *At The Criminal Defense Bar*, NEW YORK LAW JOURNAL ONLINE, Mar. 21, 2011 (claiming that "recent decisions indicate that, despite the narrower scope of pretrial criminal discovery, the government may well be held to the same high standards of preservation and production of ESI" as faced by civil litigants, and suggesting "[t]his emerging trend has strategic implications for the criminal defense bar when requesting discovery from, and defending against claims brought by, government agencies."); *cf.*, Jared S. Beckerman, *O'Keefe and the Wheel that Begs for Reinvention: An Exceptionalist Approach to Electronic Discovery in Criminal Actions*, 9 NW. J. TECH. & INTELL. PROP. 175 (arguing that the wholesale adoption of the Civil Rules in solving problems of E-Discovery in criminal actions is not the best solution); *see also* Gibson Dunn, 2010 Year-End Electronic Discovery and Information Law Update 23 (2011) http://www.gibsondunn.com/publications/Documents/2010YearEndE-Discovery-InformationLawUpdate.pdf (*e.g., Government and E-Discovery: Clarified Obligations and Limits, Trends in the Criminal Context*); Daniel B. Garrie & Daniel K. Gelb, *E-Discovery in Criminal Cases: A Need for Specific Rules*, 43 SUFFOLK U. L. REV. 393, 399 (2010). With respect to

whether civil ESI principles are being–or should be–applied to criminal cases, *United States v. O'Keefe*, 537 F. Supp. 2d 14 (D. D.C. 2008), provides fodder for such an exercise. The *O'Keefe* court held that as far as the form of document production, the government's discovery obligations to a criminal defendant mirrored the obligations that civil litigants owe each other under the Federal Rules of Civil Procedure. *Id.* at 19. The court cited Rule 34(b), which requires a party to respond to a demand for production by directly turning over the materials in a usable form. Fed. R. Civ. P. 34(b)(2)(E)(I). The court wrote that "it is foolish to disregard [the Federal Rules of Civil Procedure] merely because this is a criminal case, particularly where, as is the case here, 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.*

Unlike civil litigation, which requires broad discovery on the basis of relevance, the prosecution's disclosure obligations are limited in scope, extending only as far as the requirements of *Brady*, *Giglio*, Jencks, and Rule 16; that is, to material exculpatory and impeachment information; witness statements; a defendant's statements and prior record; certain documents, objects, and scientific reports; and expert witness summaries. If the *O'Keefe* holding had been widely cited and adopted, it might have represented a huge change in criminal discovery. Yet, until the *Warshak* decision in late 2010–where the Sixth Circuit explicitly *rejected* the *O'Keefe* court's application of the Federal Rules of Civil Procedure to criminal cases–not a single criminal case appears to have cited *O'Keefe* as support for applying the Federal Rules of Civil Procedure to criminal cases. This strongly suggests that the migration of civil principles is not a trend and *O'Keefe* is an isolated case. Indeed, courts have rejected broad, civil-style discovery of government materials. *See, e.g.*, *United States v. Salyer*, 271 F.R.D.148, 158 (E.D. Cal. 2010) (finding that defendant was only entitled to discovery of government materials relevant to mounting a defense and rejecting defendant's " 'all documents' civil type discovery request.") *aff'd with modifications by United States v. Salyer*, 2010 WL 3036444 (E.D. Cal. Aug. 2, 2010). If criminal discovery is incorporating principles from civil litigation, consistent and persuasive authority has yet to appear.

United States v. Warshak, 631 F.3d 266 (6th Cir. 2010), the case in which the Sixth Circuit rejected the reasoning in *O'Keefe*, concerned a company's scheme to defraud consumers in connection with the sales of "Enzyte," an herbal supplement purported to enhance male sexual performance (made famous by the "smiling Bob" television advertisement campaign). In *Warshak*, the court ruled that the provision of massive amounts of ESI seized from defendant-corporation in an allegedly unsearchable format was proper, in part because the government was giving the defendant back its own information. *Id.* at 296. The court rejected the reasoning in *O'Keefe* that Federal Rule of Civil Procedure 34(b)2(E)(i), which requires documents to be produced in a specific format, is applicable to criminal cases. *Id.* at 296 n.26. The Sixth Circuit noted that federal discovery rules are governed by Federal Rule of Criminal Procedure 16, which contains no such guidance. *Id.* at 296. *Warshak* will be examined in further detail in sections seven and eight of this article.

Dicta in the well-known Cheney energy policy case also provides support for maintaining the distinction between civil and criminal discovery. *Cheney v. U.S. Dist. Court for D.C.*, 542 U.S. 367 (2004). While the court in *Cheney* addressed discovery in a civil case against the former Vice President, the commentary on the difference between prosecutors and civil litigants is directly on point:

> In the criminal justice system, there are various constraints, albeit imperfect, to filter out insubstantial legal claims. The decision to prosecute a criminal case, for example, is made by a publicly accountable prosecutor subject to budgetary considerations and under an ethical obligation, not only to win and to zealously advocate for his client but also to serve the cause of justice. The rigors of the penal system are also mitigated by the

> responsible exercise of prosecutorial discretion. In contrast, there are no analogous checks in the civil discovery process here.

Id. at 386.

Although it has not had a widespread impact on criminal law, *O'Keefe* may have some practical use. For example, when the government searches for and produces government agency business records under Rule 16, it may be useful to model search and production rules on what is required by civil discovery rules. Most criminal production, however, does not involve agency business records. Rather, the government's production is usually records, data, and/or information (often voluminous) that the prosecution team has gathered, e.g., via grand jury subpoena or search warrant, or generated, e.g., via wiretap. In these circumstances, the government's basic obligation under Rule 16 is to make that material available for inspection and copying. Nevertheless, prosecutors may wish to consider producing discovery in a form that is readily usable to both the government and defense.

III. Metadata

"Metadata" refers to data that provides information about one or more aspects of an electronic document, such as the means of a document's creation, the purpose of the data, the time and date of creation, and the creator or author of the data. *See, e.g*, *Latimer v. Roaring Toyz, Inc.*, 574 F. Supp. 2d 1265, 1269 (M.D. Fla. 2008) ("Examples of metadata for electronic documents include . . . file dates (e.g., creation date, date of last data modification, date of last data access, and date of last metadata modification) . . . ."). Metadata may also include details such as the depth, size, and resolution of a photograph, the date it was taken, or a short summary of a document. Metadata arises in several contexts in criminal cases and can provide details about a file's creation, use, and editing history to a prosecutor. For these reasons, prosecutors often attempt to capture metadata when obtaining evidence under a grand jury subpoena or a search warrant.

As with other aspects of E-Discovery, however, discovery of metadata is a sword that cuts both ways: just as prosecutors may demand it from defendants, in certain limited circumstances the government's failure to produce it can weaken the strength of evidence or cause it to be suppressed. In *United States v. Cross*, 2009 WL 3233267 (E.D.N.Y. Oct. 2, 2009), the court granted the defendant's motion to suppress evidence in part based on the government's failure to produce metadata for a photo-array. Observing that the U.S. Attorney's Office had comfortably used metadata in the past, the court found that the government's failure to produce metadata cast fatal doubt on the veracity of the evidence. *Id.* at *8. Although the *Cross* holding appears to stand alone for now, it may apply to metadata within materials discoverable under Jencks, Rule 16, *Giglio*, or *Brady*. In the highly-publicized prosecution of then-Senator Ted Stevens, the defense sought metadata related to the government's forensic photography. The defense characterized the metadata as "an automatic digital stamp that indicates what type of lens was used, aperture settings, etc., all of which is relevant to the reliability and thus admissibility of the government's photographs." Defendant's Reply in Support of Motion to Compel Discovery, *United States v. Stevens*, No. 08-231 (EGS), Doc. No. 50 at 9 (D. D.C. Sept. 6, 2008). Noting that "[c]ourts routinely permit the discovery of metadata in the civil context," the defense relied on *O'Keefe* to argue "there is no principled reason why it ought not be produced in a criminal case." *Stevens*, No. 08-231 (EGS) (citing *O'Keefe*, 537 F. Supp. 2d at 18-19). This motion was eventually resolved without a written opinion by the court.

One of the latest E-Discovery opinions is *Nat'l Day Laborer Org. Network v. U.S. Immigration and Customs Enforcement Agency*, 2011 WL 381625 (S.D.N.Y. Feb. 7, 2011), a civil case in which the National Day Laborer Organization filed a request under the Freedom of Information Act, 5 U.S.C. § 552

(FOIA), for information pertaining to U.S. Immigration and Customs Enforcement's new secure communities program. In this case, the court found that metadata was part of an electronic document under FOIA. The court specifically noted that "[b]y now it is well accepted, if not indisputable, that metadata is generally considered to be an integral part of an electronic record." *Id.* at *4. The court continued: "certain metadata is an integral part of an electronic record" and "[a]s a result, such metadata is 'readily producible' in the FOIA context." *Id.* at *5.

The opinion, however, also recognizes that not all metadata is of equal importance. The judge held "the Court will not impose any greater burden on the Defendants than is absolutely necessary to conduct an efficient review," and went on to discuss the minimum fields of metadata that should accompany production of text-based ESI and emails, including file name, last date modified, and the name of the custodian. *Id.* at *6,*7. Notably, the court did not suggest that the proposed protocol should be required in every case, and specifically stated that any production specification which goes beyond the "reasonably usable format" standard of Federal Rule of Civil Procedure 34 is "subject to negotiation by the parties on a case by case basis" and "[i]f no agreement is reached, the court must determine the appropriate form of production, taking into account the principles of proportionality and considering both the needs of the requesting party and the burden imposed on the producing party." *Id*. at *7. While this case captures some of the challenges presented by metadata, it is also important to recognize that it is a civil case, operating under the Federal Rules of Civil Procedure and dealing specifically with a FOIA request. Accordingly, it may have limited application in the criminal context, particularly where metadata for government-generated records could be protected from disclosure, such as under the work product doctrine.

IV. Social networking sites

Evidence found on social networking sites, such as Facebook or Twitter, continues to be used as evidence in both civil and criminal cases around the country. *See United States v. Beckett*, 2010 WL 776049, at *2 (11th Cir. Mar. 9, 2010) (admitting evidence from MySpace in a child pornography case). Interestingly, in *Barnes v. CUS Nashville*, 2010 WL 2265668 (M.D. Tenn. June 3, 2010), a civil case stemming from the plaintiff's slip and fall while dancing on a bar at the "Coyote Ugly Saloon" in Nashville, the Magistrate Judge offered to create his own Facebook account and "friend" the plaintiff for the sole purpose of reviewing, *in camera*, photos she had posted on Facebook of herself dancing on the bar on the night of incident. It is good practice for attorneys, whether in civil or criminal cases, to recognize that social networking sites may contain information that could be used as evidence or otherwise have significance in a court proceeding. While no court thus far appears to have imposed obligations to preserve and search information on social networking sites, such a ruling may not be far off.

Furthermore, another recent civil case suggests that privacy settings on social networking pages make a difference with regard to discovery. *Crispin v. Christian Audigier, Inc*., 717 F. Supp. 2d 965 (C.D. Cal. 2010). The *Crispin* court applied the Stored Communications Act (SCA), 18 U.S.C. §§ 2701-11, to the information contained in the plaintiff's MySpace and Facebook private messaging systems. *Id.* at 980; *see also* Alan Klein et al., *Is 'Private Data' on Social Networks Discoverable?*, NAT'L L.J. (Aug. 25, 2010), http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202471022686&slreturn=1&hbxlogin=1. Although the SCA, which explicitly applies to 1980's technology, may be an awkward fit for social networking sites, the *Crispin* court found that because the plaintiff's social networking messages were private, they were protected from discovery just as if they were private email. *Crispin*, 717 F. Supp. 2d at 991. Prosecutors should learn what is on defendants' social networking pages as this may provide evidence which could prove valuable at trial. Furthermore, it is also important that

prosecutors are aware of the privacy settings of their own social networking pages (should they have them), those of other members of the prosecution team, as well as potential government witnesses.

V. Emails

Just as a defendant's emails can be located and used at trial by prosecutors, government emails may also contain information that must be disclosed to the defense under *Brady/Giglio*, Rule 16, and Jencks. Because emails that contain exculpatory and impeachment materials may be just as discoverable as any other form of information, prosecutors should be aware of their disclosure obligations for such emails. Prosecutors must also remember that emails are permanent in nature and take the appropriate steps to avoid even the appearance of impropriety. *United States v. Welton*, 2009 WL 2390848 (C.D. Cal. Aug.1, 2009), illustrates this point. In *Welton*, a child pornography prosecution, the central issue at the suppression hearing was whether the agent had used psychological coercion to induce a confession from the defendant. The defense contended that when the case agent asked the defendant in an interview about sexual abuse he suffered as a child, this constituted improper "softening up." *See Elliott v. Rocha*, 108 F.3d 337 (9th Cir. 1996) (unpublished table disposition). In preparing to testify at the suppression hearing, the case agent exchanged emails with an AUSA in another district (not the AUSA assigned to the case). These emails surfaced after the suppression hearing. In one of the emails concerning the agent's questioning of the defendant about abuses he suffered as a child, that AUSA advised the agent: "DON'T SAY IT WAS TO SOFTEN HIM UP." *Welton* at *2 (capitalization in original). At an evidentiary hearing concerning the emails, both the agent and the AUSA testified that this particular email was "a joke." *Id.* at *12. Although the court denied the motion to dismiss the indictment, it found neither the agent nor AUSA to be credible on this point, and referred the AUSA for possible disciplinary action. As a postscript, in an order issued one year later, the court clarified that its finding that the AUSA's testimony regarding the emails was not credible was primarily to ensure that a competent agency determined whether an ethical violation had occurred. *Id.* Nonetheless, *Welton* demonstrates the risks attendant to email communications between law enforcement officials: when tone and context are lacking, jocularity may not be viewed as such if evaluated by a court months or years later.

United States v. W.R. Grace, a significant environmental prosecution in the District of Montana, is another important case concerning the hazards of electronic communications. In *Grace*, the government's main cooperating witness exchanged roughly 200 emails with the lead case agent over a 4-year period leading up to the trial. The defense did not learn about these emails until part-way through the cooperating witness's cross examination. The court determined that the emails showed significant bias in the form of the cooperator's extensive relationship with the government and animus towards the defendant, and instructed the jury to that effect. *See United States v. W.R. Grace, et al.*, CR-05-07-M-DWM, doc. no. 1150 (Apr. 28, 2009); *see also* Beth Brennan & Andrew King-Ries, *A Fall From Grace: United States v. W.R. Grace and the Need for Criminal Discovery Reform*, 20 CORNELL J.L. & PUB POL'Y 313 (2010); *Sidebar: Reflections on the W.R. Grace Trial*, http://www.law.com/jsp/tal/PubArticleTAL.jsp?id=1202433359449 (video interview of Caroline Kubota, one of the members of the *Grace* defense team, concerning the trial). The *Grace* case will be further discussed in section seven of this article.

Not all circuits, however, subscribe to "wholesale" discoverability of the prosecution's emails under Rule 16. In *United States v. Malone*, 49 F.3d 393, 396 (8th Cir. 1995), the Eighth Circuit held that emails between prosecutors and agents, as well as the agent's rough notes, were not discoverable under Rule 16 where they included an agent's impressions of a witness interview rather than statements by the witness. *See also Morris v. Ylst*, 447 F.3d 735, 742 (9th Cir. 2006) ("[I]n general, a prosecutor's opinions

and mental impressions . . . are not discoverable under *Brady unless* they contain underlying exculpatory facts.") (emphasis in original).

Interestingly, according to the Seventh Circuit, emails written by government witnesses contemporaneously with the events in question need not be disclosed under the Jencks Act. In *United States v. Kimoto*, 588 F.3d 464 (7th Cir. 2009), the defendant contended that he had been prejudiced by the government's failure to turn over an email referenced in a deposition. The court found that the email at issue was not a "statement" within the meaning of the Jencks Act, because the term "statement" as used in the Jencks Act refers to "a recorded recital of past occurrences made by a prospective prosecution witness[,]" which "[f]rom its very nature, necessarily . . . is made after those events have taken place." *Id.* at 491. In its analysis, the court discussed *United States v. Sopher*, 362 F.2d 523 (7th Cir. 1966), a case in which the Seventh Circuit found that the Jencks Act did not require the government to turn over the transcript of a conversation, recorded by a cooperating witness, during which the defendant accepted a bribe. *Id.* at 525. According to the court, in contrast to a witness's recollection of past events, the transcript at issue in *Sopher*, much like the email in *Kimoto*, involved a "concurrent . . . conversation" which was "obviously of contemporaneous sounds." *Kimoto*, 588 F.3d at 492 (internal quotes and citations omitted). The Seventh Circuit therefore upheld the district court's ruling in favor of the government on the alleged Jencks Act violation. *Id* at 493.

United States v Safavian, 233 F.R.D. 12 (D.D.C. 2005), is another important case concerning the government's obligations to collect and produce emails. In *Safavian*, the court required the Department of Justice "immediately– by formal request, in writing–to demand that the GSA [General Services Administration] conduct a thorough search for and produce to the Justice Department all emails–including archived emails on hard drives–and correspondence sent to or from GSA officials relating to [the subject matter]," and required prosecutors to review the documents for Rule 16 and *Brady* materials. *Id.* at 19. In *United States v. Bhutani*, 175 F.3d 572 (7th Cir. 1999), the Seventh Circuit found that with respect to *Brady* material, "the government does not have the duty to disclose information of which it is unaware, [but] if a government agency is charged with the administration of a statute and has consulted with the prosecution in the case, the agency will be considered part of the prosecution . . . ." *Id.* at 577. These interpretations of the responsibilities of federal prosecutors could impact the scope of discoverable materials. Although emails must be disclosed only if their content falls under *Brady/Giglio*, Rule 16, or the Jencks Act, as a general practice rule, all substantive case-related emails should be preserved to ensure a complete review of emails for discoverable information. *See* Memorandum from David Ogden, Deputy Attorney General, *Guidance for Prosecutors Regarding Criminal Discovery*, 5-6 (Jan. 4, 2010).

VI. Text messages

Prosecutors should be aware that text messages can be subject to the same discovery rules as other materials and preservation of text messages should not be overlooked. This point was made clear in *United States v. Suarez*, 2010 WL 4226524 (D.N.J. Oct. 21, 2010), a case involving a cooperating witness who assisted the government in its investigation of public corruption in New Jersey in 2008-09. From March through July 2009, this witness participated in multiple recorded meetings with the targets, during which the cooperator exchanged numerous text messages with three FBI agents (which could be seen on the video recordings and was visible to the defense when viewed). *Id.* at *1. In response to a defense request for discovery of the text messages, the government attempted to obtain the text messages but was unable to provide all of them because some had been erased pursuant to FBI policy. *Id.* at *3. Absent a litigation hold, FBI policy permitted backup tapes to be overwritten or destroyed after 90 days. *Id.*

Although there was no evidence of bad faith on behalf of the government, the court found a Jencks Act violation. *Id.* at *6. While the court denied the defense motion to suppress the cooperator's testimony and recordings, it gave an adverse inference spoliation instruction from *Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am.*, 685 F. Supp. 2d 456, 470-71 (S.D.N.Y. 2010), that permitted the jury to infer from the government's failure to preserve text messages, or the fact that they were deleted by the agents, that the text messages were relevant and favorable to the defendants. *Id.* at *8. In summation, one defense attorney used the spoliation charge to argue that the FBI had destroyed evidence. The jury acquitted the defendant whose counsel had focused on the missing text messages, but convicted the other defendant. *But cf. United States v Georgiou*, 2011 WL 1081156, *6-7 (E.D. Pa. Mar. 18, 2011) (distinguishing *Suarez* on grounds that the government had preserved the electronic communications in question, defendant's claims concerning alleged missing communications between the cooperator and agents were "pure speculation," and finding that even if such evidence existed, it would have been " 'merely impeaching' and cumulative.").

An instructive civil case dealing with text messages is *Southeastern Mech. Services, Inc. v. Brody*, 657 F. Supp. 2d 1293 (M.D. Fla. 2009). In *Southeastern*, an employer sued its former employees for misappropriation of trade secrets. During the trial it was discovered that the former employees had wiped text messages and other information from their BlackBerries before syncing them to the company's email server. As a result, the court determined that spoliation had occurred and issued an adverse inference jury instruction. *Id.* at 1302. Both *Suarez* and *Southeastern* serve as a reminder to properly preserve case-related communications, because failure to do so may lead to sanctions such as an adverse inference jury instruction.

VII. Discovery of government databases (and other large quantities of ESI)

The government's obligation to disclose information held in voluminous electronic databases is another hot topic in ESI discovery. Fortunately, a body of case law, including circuit court cases, appears to be developing for discovery of government databases. To date, the case law generally appears to be fact-specific and does not offer many clues into emerging trends, with one exception: a growing number of cases support the idea that if prosecutors in good faith provide the defense with a searchable database, they need not search for and then identify any potential *Brady* material within that database, regardless of how voluminous it may be.

Perhaps the most promising case from which to begin to deduce a trend in electronic database discoverability is *United States v. Skilling*, 554 F.3d 529 (5th Cir. 2009) *vacated in part on other grounds*, 130 S.Ct. 2896 (2010). In *Skilling*, the Fifth Circuit applied a standard of reasonableness to find that the government did not violate *Brady* in turning over a voluminous open file because of additional steps it took to make the file easier for the defense to use. *Id.* at 577. Although the government turned over several hundred million pages, the files were electronic and searchable, the government produced a set of "hot documents," and there was no evidence that the government in bad faith hid any exculpatory information in the huge volume of data. *Id.* at 575-77. The court rejected Skilling's argument that the government should have located and turned over exculpatory evidence within the file, finding that "the government was in no better position to locate any potentially exculpatory evidence than was Skilling." *Id.* at 577. The court instead found that "[a]s a general rule, the government is under no duty to direct a defendant to exculpatory evidence within a larger mass of disclosed evidence," rejecting the defense's argument that government concealed favorable information amidst millions pages of information. *Id.* at 576. While the government is not permitted to act in bad faith in performing its obligations under *Brady*, such as purposely hiding *Brady* information in a huge open file, here the affirmative steps the

government took beyond merely providing Skilling with the open file demonstrated the government's good faith efforts to comply with *Brady*. *Id.*

The Sixth Circuit reached a similar result in the aforementioned *Warshak* case. In *Warshak*, relying in part on *Skilling*, the court found that *Brady* did not require the government to aggressively cull massive amounts of data searching for exculpatory material where there was no evidence that the government was concealing *Brady* materials or acting in bad faith by providing the records in bulk (which had been taken from "tera drives" seized from the defendant). *Warshak*, 631 F.3d at 297. The court also held that the trial court's denial of a continuance to enable the defense to look for more exculpatory evidence was not an error because the defense was unable to produce any evidence showing that such materials existed. According to the Sixth Circuit, "it would not be prejudicial if the defendants were denied the chance to excavate a mine that contained no ore." *Id.* at 299.

In *United States v. Ohle*, 2011 WL 651849 (S.D.N.Y. Feb. 7, 2011), the court rejected the defendants' contention that the government failed to fulfill its *Brady* obligations at trial because "the materials were unduly onerous to access." *Id.* at *3. The materials the government produced were comprised of several gigabytes of data–including millions of separate files extending to several million pages in length–in nine separate databases, and any document search had to be conducted on a database-by-database basis. *Id*. Citing *Skilling*, the court ruled that

> the Government, to facilitate review of the documents, provided defense counsel with an electronically searchable Concordance database. Both the Government and defense counsel had equal access to this database. Thus, the defendants were just as likely to uncover the purportedly exculpatory evidence as was the Government. Moreover, as a general rule, the Government is under no duty to direct a defendant to exculpatory evidence within a larger mass of disclosed evidence.

Id. at *4.

The court also rejected the argument that the government had "heightened obligation to uncover exculpatory evidence in light of its allegedly extensive resources and subpoena powers." *Id.* Further, according to the court, *Brady* "does not place any burden upon the Government to conduct a defendant's investigation or assist in the presentation of the defense's case." *Id.* (citing *United States v. Marrero*, 904 F.2d 251, 261 (5th Cir. 1990)).

In the previously discussed case of *United States v. W.R. Grace*, 401 F. Supp. 2d 1069 (D. Mont. 2005), the court found that the government had met its *Brady* obligation by simply turning over to the defense its entire evidentiary database of over 3.3 million documents (much of which came from the corporate defendant). *Id.* at 1080. The court found that the defendants were no less able than the government to locate exculpatory materials in the database, in part, because the documents were easily searchable. *Id.* The court distinguished the *Grace* disclosure from *United States v. Hsai*, 24 F. Supp. 2d 14 (D. D.C. 1998), in which the government provided an "undifferentiated mass of documents" to the defense, partially on the basis of searchability. *Id.* Similarly, in *United States v. Ferguson*, 478 F. Supp. 2d 220 (D. Conn. 2007), the searchability of a 3.5 million page database was a major factor in the court's finding that the government had in good faith met its disclosure obligations.

In *United States v. Dunning*, 2009 WL 3815739 (D. Ariz. Nov. 12, 2009), the court rejected the defense's contention that government had a duty to conduct forensic analysis on the same hard drives that defendant possessed, finding that the government was not suppressing any information, because the defendant had the same access to the information that the government did. The court noted that "Brady does not mean that the government must take the evidence that it has already disclosed to Defendant, sift

through this evidence, and organize it for Defendant's convenience." *Id.* at *1. The court also noted that "Federal Rule of Criminal Procedure 16(a)(1)(E) requires the government merely to permit the inspection and copying of certain items '*if* the item is within the government's possession, custody or control.' " *Id.* (emphasis in original). In *United States v. Serfling*, 504 F.3d 672 (7th Cir. 2007), the court found that the government had not suppressed supposedly exculpatory documents included in 10,000 pages of documents from a civil case where, prior to trial, the government had advised the defendant of the availability of records and the defendant did not review them. And in *United States v. Jordan*, 316 F.3d 1215, 1253-54 (11th Cir. 2003), the Eleventh Circuit rejected the defense's argument that the government hindered its trial preparation by requiring it to search for exculpatory evidence amidst voluminous material, because the defense could have asked for a continuance or advised the government of the defense theory in order for them to help provide the relevant discovery materials.

Some courts have distinguished between discoverability of databases created by the government and the discoverability of the underlying source material used to create those databases. In *United States v. Lewis*, 594 F.3d 1270, 1282 (10th Cir. 2010), citing FRE 1006, the defense sought access to a database created by the government from bank records seized from the defendant. The court found that the defense was not entitled to the database, which constituted government work product, because the underlying source, the bank records, were available to the defense. *Id.* Likewise, in *United States v. Schmidt*, 2007 WL 1232180 (D. Colo. 2007), the court denied the defense access to both computer programs and an electronic database the IRS had used to sort through voluminous files. In *Schmidt*, the defense had access to bank records that were the underlying source material for the database and the court determined that the database and computer programs constituted work product. *Id.* at *1.

In *United States v. Perraud*, 2010 WL 228013 (S.D. Fla. Jan. 14, 2010), the court found that the government met its discovery obligations under Rule 16 by directing defendants to a universe of 5,000 scanned documents gleaned from a huge underlying set of material. Although the court suggested that providing access to the underlying source material alone would not satisfy Rule 16, it found that the government had met its obligations by providing a database created from the complete universe of documents. *Id.* at *12. Notably, the court indicated that should the government become aware of any exculpatory evidence it would be required to identify the evidence to the defense as soon as it was located, rather than refer defendants to the database to find it themselves. *Id.* The *Perraud* court also weighed the searchability of the 5,000 relevant files the government turned over to the defense in finding the government had used a "reasonable and appropriate approach" to disclosure. *Id.*

Prosecutors should, however, keep in mind that defendants may have some success in arguing that the volume of discoverable materials turned over by the government impedes preparation for trial, especially in the face of other aggravating factors. *See United States v. Graham*, 2008 WL 2098044, at *2-3 (S.D. Ohio May 16, 2008). In *Graham*, the court found that the sheer volume of data turned over by the government, combined with the government's erratic and unmanageable method of turning over material, prejudiced the defendants and dismissed the indictment under the Speedy Trial Act, 18 U.S.C. § 3161. *Id* at *8. The *Graham* court compared the government in that case to a "restless volcano [that] periodically spews forth new discovery." *Id.* at *5. *United States v. Qadri*, 2010 WL 933752 (D. Haw. Mar. 9, 2010), is a case in which the court reached the opposite conclusion. In *Qadri*, discovery included documents, electronic communications, audio and video recordings, as well as over 30 computer hard drives and three servers. The court denied the defendant's motion to dismiss the indictment on speedy trial grounds, finding "the delays in this case may be attributed at least in part to the nature of E-Discovery, the complex nature of the alleged crimes, and the necessity of coordinating various branches of government in the investigation." *Id.* at *5.

SEC v. Collins & Aikman Corp., 256 F.R.D. 403 (S.D.N.Y. 2009), a civil security fraud case demonstrates the view that, in certain circumstance, the government must do better than simply turning over a vast open file. In *Collins*, the Securities and Exchange Commission (SEC) provided ten million pages to a defendant without a search protocol, leaving the defendant to find the discoverable materials in the files. *Id.* at 410-11. The *Collins* court found that even if the SEC's compilation of relevant documents was work product, the defendant was entitled to the material because of the hardship and expense associated with searching the unsorted underlying files. *Id.* at 414. The judge also noted that the United States Attorney's Office for the Southern District of New York had produced some of the materials at issue to the defendant (and his three co-defendants) in the parallel criminal prosecutions. The court stated it was "somewhat baffled as to why the SEC continu[ed] to object to the production" in the civil case, and ordered the SEC to turn over to the defense the 175 file folders in which it had segregated the documents for its own use. *Id.* at 413. The *Collins* court also recognized the importance of searchability of databases, ordering the SEC "to negotiate an appropriate search protocol to locate documents." *Id.* at 418.

While case law generally supports the proposition that searchable "open file" disclosures satisfy discovery obligations, prosecutors should be aware of *United States v. Salyer*, 2010 WL 3036444 (E.D. Cal. Aug. 2, 2010), a case in which a magistrate judge ordered the government to identify Rule 16, *Brady*, and *Giglio* materials to the defense as a "matter of case management and fairness." *Id.* at *2. *Salyer* would appear to be limited to its factual circumstances, however. Specifically, the case involved disclosure of a huge amount of discovery materials to "a singular, individual defendant . . . detained in jail pending trial, and . . . represented by a relatively small defense team" without assistance from a corporate defendant. *Id.* at *7. According to the magistrate, after the court asked the prosecution at a hearing why they had sought such a massive amount of materials, "the response pared to its essence was 'because we can.' " *Id.* at *3. As a result, the court found that "[i]f the government argues that it is now 'impossible' to comply with the burden of reviewing evidence for identification purposes, the government more or less made its own bed in this matter by making it impossible." *Id.* at *4. Finding that the government's huge open file disclosure was insufficient, the court observed: "it will not do to state that 'to the extent *Brady/Giglio* material is present, defendant will know it when he sees it.' " *United States v. Salyer*, 271 F.R.D. 148, 154 (E.D. Cal. 2010) *adhered to as modified by* 2010 WL 3036444 (E.D. Cal. Aug. 2, 2010).

The court also rejected the government's argument that it could not undertake *Brady* review as ordered because it could not know the defense theory, remarking that "the prosecution knows, as any litigator would know, what evidence, on its face, significantly detracts from the factual elements which must be proven in a particular case." *Salyer*, 2010 WL 3036444 at *5. According to the *Salyer* court,

> 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. (emphasis in original).

Nonetheless, by its very terms, the opinion has narrow application: "The undersigned emphasizes that the initial order and this reconsideration order is limited to the circumstances of this case. The undersigned does not find, nor would he, that the identification requirements of this case would apply to other cases not similarly situated in factual circumstances." *Id.* at *8. Although the decision may

not have wide-ranging consequences, it demonstrates that prosecutors may not always be able to meet their discovery obligations simply by ensuring that a disclosed database is searchable.

VIII. Search and seizure

While the primary focus of this article is the government's disclosure of ESI, this section will briefly discuss ESI-related search and seizure case law. Recent case law has made the topic of ESI search and seizure worthy of its own article and the brief discussion in this section is not intended to be all-inclusive, but rather to raise awareness of the existence of several recent ESI-related cases and provide a brief summary of their holdings.

In *Warshak*, mentioned earlier, the Sixth Circuit held that to the extent that the SCA (18 U.S.C. § 2703) allowed the government access to stored emails with anything less than a search warrant based on probable cause, the Act was unconstitutional. *Warshak*, 631 F.3d at 288. Although the court found that government agents had violated the defendant's Fourth Amendment rights by compelling email without first obtaining a search warrant based on probable cause, the court held that the exclusionary rule did not apply because the agents relied in good faith on the provisions of the SCA. *Id.* at 282. Given its significance, it is not surprising that *Warshak* has created an immediate buzz among legal commentators. *See, e.g.*, Ben Kershberg, *Can the Government Seize Your Email Without A Warrant? You'll be Surprised*, FORBES BLOGS, LAW &TECHNOLOGY, Feb. 8, 2011, http://blogs.forbes.com/benkerschberg/2011/02/08/can-the-government-seize-your-email-without-a-warrant-youll-be-surprised-2/.

Another significant recent case is *United States v. Stabile*, 2011 WL 294036 (3d Cir. Feb. 1, 2011), a lengthy opinion which contains holdings on a variety of important computer forensic issues. Although the importance of *Stabile* cannot be fully captured in this article, it is important to highlight a few of the holdings. In *Stabile*, the defendant was under investigation for counterfeiting. *Id.* at *1. When agents arrived at his home, his putative wife (the defendant was later found to have not obtained a valid divorce from his previous wife) consented to a search of the home for evidence of financial crimes. *Id.* The police then seized, along with other items, multiple hard drives from the home. During the course of an off-site forensic search of the hard drives, the police discovered child pornography. *Id.* at *3. The defendant sought to have the evidence of child pornography suppressed, arguing, among other things, that the police search was overbroad. *Id.* at *8.

With regard to consent, the *Stabile* court found that because the computers were not password protected, and were located in a common area of the home, the defendant's putative wife's consent to the search was valid. *Id.* Given the complexities of computer forensics, the court concluded that the government's seizure of the entirety of the hard drives for off-site review (as opposed to engaging in on-site review and sorting) was reasonable. *Id.* at *10. The court noted that while consent to the search was based upon the government's request to search for evidence of financial crimes, such crimes are complex and require a thorough review. The court further found that the detective's search of the file containing the pornography under a subsequently obtained state warrant concerning financial crimes was proper because of the likelihood that criminals may seek to obscure evidence on hard drives. *Id.* The court upheld the forensic methods used to accomplish the search and found that even if subjective intent of the examiner was to find child pornography, it was irrelevant in determining whether such a search was proper. *Id.* at *15. In so holding, the Third Circuit joined the Fourth Circuit's view in *United States v. Williams*, 592 F.3d 511, 524 (4th Cir. 2010), that subjective intent of the forensic examiner is irrelevant in determining whether the warrant was executed in a reasonable manner. *Stabile*, 2011 WL 294036 at *15.

Notably, the court also found that the plain view doctrine applies to computer forensic searches and ruled that a list of computer files with "lurid names" were in plain view for purposes of determining whether seizure of such files was lawful under the Fourth Amendment. *Id.* at *16. In its ruling, the court specifically rejected the suggestion by Ninth Circuit in *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1178, 1188 (9th Cir. 2010) (en banc), that the government must "forswear reliance on the plain view doctrine" whenever it seeks a warrant to examine a computer hard drive. Instead, the Third Circuit aligned itself with the Seventh Circuit's decision in *United States v. Mann*, 592 F.3d 779, 785 (7th Cir. 2010), that application of the plain view rule to seized computer hard drives should be decided incrementally, based upon the particular facts of the cases presented to courts. *Stabile*, 2011 WL 294036 at *16. Prosecutors are encouraged to review the *Stabile* decision in its entirety as it contains important holdings on a wide variety of computer forensics and search and seizure issues.

With respect to search and seizure of mobile phones, courts across the country are divided whether and to what extent the "search incident to arrest" doctrine of the Fourth Amendment applies. Most recently, a district court in the Northern District of California denied, in part, a defendant's motion to suppress evidence on the grounds that it was obtained from a warrantless search of his cell phone during and after his arrest. *United States v. Hill*, 2011 WL 90130 (N.D. Cal. Jan. 10, 2011). The court found that the Fourth Amendment does not require officers to have a warrant before searching for text messages stored on cell phones found in possession of arrestees. *Id.* at *7. In *Hill*, the defendant was arrested and his iPhone, which was on his person, was immediately seized and searched by the arresting officer, and was found to contain child pornography. It was then further searched upon their arrival at the station. While the court recognized that modern phones have the capacity to store large amounts of personal information, it held that absent guidance from the Supreme Court and the Ninth Circuit, it was "unwilling to conclude that a cell-phone that is found in a defendant's clothing and on his person . . . should not be considered an element of the person's clothing." *Id.* The court concluded that on the facts of the case, the search was proper and the defendant's cell phone should not have been treated any differently than, for example, a wallet taken from a defendant's person. *Id.*

Notably, the *Hill* court emphasized the contemporaneous nature of the search of the cell phone and the arrest, distinguishing it from a previous holding on those grounds. *Id.* at *7. *See United States v. Park*, 2007 WL 1521573 (N.D. Cal. May 23, 2007) (suppressing evidence obtained through the warrantless searches of cellular phones lawfully seized from defendants at the time of their arrests, where search was conducted approximately an hour and a half after the arrest). Although the Supreme Court has not addressed this issue, numerous federal courts have, with conflicting results. *Compare, e.g.*, *United States v. Quintana*, 594 F. Supp. 2d 1291, 1298-99 (M.D. Fla. 2009) (search of defendant's cell phone was not justified as search incident to valid arrest), *with United States v. Finley*, 477 F.3d 250, 259-60 (5th Cir. 2007) (search of cell phone was justified as search incident to valid arrest), *and United States v. Wurie*, 612 F. Supp. 2d 104, 109-11 (D. Mass. 2009) (same).

Another developing area of ESI is the use of global positioning systems (GPS) by law enforcement to track the movements of suspects. In *United States v. Pineda-Moreno*, 591 F.3d 1212, (9th Cir. 2010), the Ninth Circuit held that the warrantless tracking of the defendant did not violate the Fourth Amendment where officers installed GPS devices on the defendant's vehicle while it was parked in front of his home. *Id.* at 1214. The court rejected the defendant's claim that he had a reasonable expectation of privacy in his driveway, even if the driveway was located "within curtilage of the home," because the defendant had taken no steps to enclose the driveway or obscure the area from public view. *Id.* at 1214-15. On the other hand, in *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), the D.C. Circuit found the warrantless tracking of a defendant to be in violation of the Fourth Amendment. *Id.* at 559. In *Maynard*, the GPS device was used to track the defendant's movements 24 hours-a-day for 28 days. *Id.*

The court reasoned that the duration of the tracking revealed private information through patterns of behavior and found the search unreasonable based on the idea that individuals have a reasonable expectation of privacy in the aggregate total of their movements over the period of 28 days. *Id.* at 561-62. In *United States v. Sparks*, 2010 WL 4595522 (D. Mass. Nov. 10, 2010), however, the court not only rejected the defendant's *Maynard* "aggregate travels" argument, but criticized the holding in *Maynard* as leaving police with "a vague and unworkable standard." *Id.* at *8. The *Sparks* court pointed out, "It is unclear when surveillance becomes so prolonged as to have crossed the threshold and created this allegedly intrusive mosaic," and that, under *Maynard*, "conduct that is initially constitutionally sound could later be deemed impermissible if it becomes part of the aggregate." *Sparks*, at *8; *cf.*, *In the Matter of an Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information*, 2011 WL 679925 (E.D.N.Y. Feb. 16, 2011) (where government sought an order under the SCA for historical cell site information concerning calls and text messages from two mobile telephones, court determined that relatively "short[ ] time period of the surveillance at issue" did not trigger warrant requirement under *Maynard*).

IX. Conclusion

Notwithstanding the efforts of some commentators to piece together case law and claim that there are emerging trends in criminal ESI case law, the existing law appears to be too thin, fact-specific, and inconsistent to draw many conclusions. To the extent that any "trend" has emerged, it is that prosecutors are not required to seek out and then specifically identify for the defense any potential *Brady* material in a large database. Rather, they can meet their disclosure obligations by ensuring that voluminous information is searchable by the defense. Trends concerning disclosure of emails and text messages, metadata, and the migration of civil principles into criminal discovery, however, have yet to appear. *See also Digital Discovery & e-Evidence, Government Operations: ESI Experts Discuss E-Discovery Trends in Criminal Procedure During BNA Webcast*, Bureau of National Affairs, Mar. 17, 2011 (reporting on March 10, 2011 webinar in which author and members of the judiciary and defense bar addressed these issues and others). Rather than rely on purported trends, prosecutors are encouraged to follow best practices concerning use and preservation of ESI developed by their office and by the Department nationwide, adhere to their office's and the Department's discovery policies, and make use of all available resources.❖

ABOUT THE AUTHOR

❑**Andrew D. Goldsmith** is the National Criminal Discovery Coordinator for the United States Department of Justice, having been appointed to this position by the Deputy Attorney General in January 2010. He has also served as the First Assistant Chief of DOJ's Environmental Crimes Section, Chief of the Environmental Crimes Unit of the New York Attorney General's Office, as an Assistant United States Attorney in the District of New Jersey, and as an Assistant District Attorney in the Manhattan District Attorney's Office. Mr. Goldsmith is a three-time Attorney General's Award recipient, having most recently received the award in 2010 for his work on Electronically Stored Information. He frequently serves as an instructor for the Office of Legal Education at the National Advocacy Center on discovery-related topics, including E-Discovery in criminal cases.✠

The author wishes to thank Rebekah E. Weiler (J.D. candidate May 2011, Albany Law School) and Kyle M. Noonan (J.D. candidate May 2012, George Washington University Law School), law interns during 2010-11 with the Executive Office for U.S. Attorneys of the Justice Department, for their invaluable assistance in the preparation of this article.

When Does a Federal Agency "Reasonably Anticipate Litigation"?

Sarah Michaels Montgomery
Senior Litigation Counsel for E-Discovery
Office of the Associate Attorney General of the United States

I. Introduction

When does a federal agency "reasonably anticipate litigation"? The question is an important one because the duty to preserve evidence is triggered once litigation is "reasonably anticipated." *Silvestri v. Gen. Motors Corp.*, 271 F.3d 583, 591 (4th Cir. 2001) ("The duty to preserve material evidence arises not only during litigation but also extends to that period before litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation."). The failure to preserve relevant evidence once the duty to preserve arises can result in sanctions for spoliation. Spoliation is "the destruction or significant alteration of evidence, or failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation." *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2d Cir. 1999).

Applying these established principles in the electronic age is not easy given the enormous amount of electronically stored information (ESI) being created, replicated, and dispersed with a simple click of the mouse. Many large organizations have terabytes, even petabytes, of email stored on their systems. Translated to paper: one terabyte equals 50,000 trees and one petabyte equals 250 billion pages of text. HOW MUCH DATA DO YOU HAVE?, http://e-discoveryteam.com/interviews/questions-about-specialization-and-my-movie-with-jason-baron/. Just searching 20,000,000 email messages can take days, weeks, even years, depending on the search technology. JOHN JESSEN & MARK V. REICHENBACH, DATA PROCESSING AND PRODUCTION FORMATS, GEORGETOWN E-DISCOVERY TRAINING ACADEMY (2009).

The ground-breaking case that set forth a party's pre-litigation duty to preserve relevant ESI and established the consequences for failing to do so is *Zubulake v. UBS Warburg, LLC* (*Zubulake IV*), 220 F.R.D. 212, 218 (S.D.N.Y. 2003). In a series of five written opinions over a 3-year period, United States District Judge Scheindlin delineated affirmative steps that parties and counsel must take to search for and preserve ESI once litigation is "reasonably anticipated." Once a party reasonably anticipates litigation, "it must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents." *Id.* According to Judge Scheindlin, issuing a written litigation hold notice alone is not sufficient. Instead, parties and their counsel must take affirmative steps to identify, locate, and preserve ESI:

> Once a "litigation hold" is in place, a party and her counsel must ensure that all sources of potentially relevant information are identified and placed "on hold." To carry out this task, counsel must become fully familiar with her client's document retention policies, as well as the client's data retention architecture. Familiarizing herself in this way will invariably involve speaking with information technology personnel who can explain system-wide backup procedures and the actual–as opposed to theoretical–implementation of the firm's recycling policy. It will also involve communicating with the "key players" in the litigation to understand how they store information. In short, it is not sufficient to

> notify all employees of a litigation hold and expect that the party will then retain and produce all relevant information. Counsel must take affirmative steps to monitor compliance so that all sources of relevant information are located.

Zubulake v. UBS Warburg, LLC (*Zubulake V*), 229 F.R.D. 422, 432 (S.D.N.Y. 2004). Judge Scheindlin ultimately concluded that UBS Warburg LLC failed to preserve email messages relevant to Zubulake's claims for gender discrimination and imposed, among other sanctions, an adverse inference instruction. The jury returned a verdict of $29 million in favor of Zubulake and the case settled before the appellate court could review the decision.

The *Zubulake* opinions set forth specific *steps* that must be taken to ensure compliance with ESI preservation obligations and defined the *scope* of the pre-litigation preservation effort.

> While a litigant is under no duty to keep or retain every document in its possession . . . it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request.

Zubulake IV, 220 F.R.D. at 217 (quotation and citation omitted).

According to Judge Scheindlin then, the duty to preserve ESI pre-suit is as broad as the discovery permitted under the Federal Rules of Civil Procedure. United States District Court and Magistrate Judges considered leaders in the E-Discovery field have written E-Discovery orders that cite and adopt the preservation steps and scope of *Zubulake*. *See, e.g.*, *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 269 F.R.D. 497, 522 (D. Md. 2010); *Rimkus Consulting Grp. v. Cammarata*, 688 F. Supp. 2d 598, 611 (S.D. Tex. 2010); *In re Napster, Inc. Copyright Litig.*, 462 F. Supp. 2d 1060, 1070 (N.D. Cal. 2006).

In 2010, Judge Scheindlin reaffirmed the preservation principles set forth in *Zubulake*, making clear that sanctions will be imposed when a party fails to take affirmative reasonable steps to identify and preserve potentially relevant ESI pre-suit. In *Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC*, 685 F. Supp. 2d 456 (S.D.N.Y. 2010), the court held that a spoliation instruction and monetary sanctions were warranted against certain plaintiffs who failed to preserve ESI pre-suit. *Id.* at 496. The *Pension Committee* decision and its ramifications are being debated. *See Orbit One Communications, Inc. v. Numerex Corp.*, 2010 WL 4615547, *10 (S.D.N.Y. Oct. 26, 2010) ("*Pension Committee* . . . appears to [state] that . . . sanctions are warranted [if] information was lost through the failure to follow proper preservation practices, even [without a] showing that [it] had discovery relevance . . . a reading [to which] I respectfully dissent.").

After the *Zubulake* decisions, The Sedona Conference® Commentary on Legal Holds, *The Trigger & the Process* (Aug. 2007), published guidelines to assist organizations in determining when to issue a litigation hold for ESI and how to scope the preservation effort:

- Reasonable anticipation of litigation arises when an organization is on notice of a credible threat that it will become involved in litigation or anticipates taking action to initiate litigation. Guideline 1.
- The determination of whether litigation is reasonably anticipated should be based on good faith, reasonableness, a reasonable investigation, and an evaluation of the relevant facts and circumstances. Guideline 4.

- In determining the scope of information that should be preserved, the nature of the issues raised in the matter, experience in similar circumstances, and the amount in controversy are factors that may be considered. Guideline 7.

While some consensus has emerged as to the appropriate trigger for preserving ESI ("reasonable anticipation of litigation"), what constitutes a reasonable scope such as to avoid sanctions for spoliation is less clear. The 2006 amendments to Federal Rule of Civil Procedure 37 purported to offer a safe harbor against sanctions for parties who lost ESI as a result of "the routine, good-faith operation of an electronic information system." FED. R. CIV. P. 37(e). However, in light of the numerous sanctions decisions issued since 2006, Rule 37(e) has not proved to be much of a safe harbor in E-Discovery. *See* Dan H. Willoughby, Jr. et al., *Sanctions for E-Discovery Violations: By the Numbers*, 60 DUKE L.J. 789 (2010) (a comprehensive survey of written opinions involving motions for sanctions relating to the discovery of ESI).

At the May 2010 Duke Law School's Conference on Civil Litigation, an E-Discovery Panel, comprised of Judge Scheindlin, Magistrate Judge Facciola, and other E-Discovery luminaries, "urge[d] that a rule addressing preservation and spoliation would be a valuable addition to the Federal Rules of Civil Procedure and identifie[d] potential elements of such a rule for the consideration of the Advisory Committee on Civil Rules." Memorandum from Gregory P. Joseph to Hon. John G. Koeltl (May 11, 2010) 1, *available at* http://civilconference.uscourts.gov/LotusQuickr/dcc/Main.nsf/$defaultview/56CEC2792C3A77708525772D00519A7E/$File/E-Discovery%20Panel%2C%20Executive%20Summary.pdf?OpenElement. The proposed Preservation Rule would re-state the common law "reasonable anticipation of litigation" standard and delineate specific events as triggers for preservation. *Id.* at 5-7. Elements of a Preservation Rule, *available at* http://civilconference.uscourts.gov/LotusQuickr/dcc/Main.nsf/h_Library/9E884B4174EE27B6852576E900738E7B/?OpenDocument. One of the proposed triggers for preservation under the Preservation Rule would be the filing of an administrative claim. *Id.* The rule would also establish the "scope" and "duration" of the duty to preserve, as well as the "consequences" for failing to comply. *Id.*

Whether or not the Advisory Committee goes forward with the Duke E-Discovery Panel's recommendation, the United States should grapple with a few questions that could help inform the common law or a new Federal Rule of Civil Procedure regarding the preservation activities of federal agencies: To what extent should agency action with respect to the triggering event and scope of pre-litigation preservation efforts be subject to judicial review? Do the lower courts have the power to sanction a federal agency for pre-litigation spoliation absent a finding of bad faith? Are there pre-existing frameworks apart from *Zubulake* and its progeny that could help guide the judiciary in reviewing a federal agency's pre-litigation preservation decisions? The E-Discovery case law developed thus far has yet to focus on these questions.

Although the law is fairly settled that once the United States arrives in federal court, it must abide by the Federal Rules of Civil Procedure like any other litigant, *Mattingly v. United States*, 939 F.2d 816, 818 (9th Cir. 1991); *Moseller v. United States*, 158 F.2d 380, 382 (2d Cir. 1946), an explicit and clear waiver of sovereign immunity must exist before the United States can be hailed into federal court in the first place. One court has explained the "established [rule] . . . that the United States, as sovereign, is immune from suit save as it consents to be sued . . . and the terms of its consent . . . define [a] court's jurisdiction to entertain the suit." *United States v. Testan*, 424 U.S. 392, 399 (1976) (quoting *United States v. Sherwood*, 312 U.S. 584, 586 (1941)). Under numerous statutory schemes, Congress has conditioned a waiver of sovereign immunity on the mandatory exhaustion of an administrative remedy prior to initiation of a federal court lawsuit. *Bastek v. Fed. Crop Ins. Corp.*, 145 F.3d 90, 94-95 (2d Cir. 1998) (noting that the statute "unambiguously required plaintiffs to exhaust their administrative remedies

before bringing suit, and their failure to do so deprived them of the opportunity to obtain relief in the district court"). Federal agencies have also established additional administrative remedies that govern certain matters. *See Avocados Plus, Inc. v. Veneman*, 370 F.3d 1243, 1248-50 (D.C. Cir. 2004) (discussing jurisdictional and non-jurisdictional exhaustion).

> The exhaustion of administrative remedies requirement fulfills many goals:
>
> First, it carries out the congressional purpose in granting authority to the agency by discouraging the "frequent and deliberate flouting of administrative processes [that] could . . . encourag[e] people to ignore its procedures." Second, it protects agency autonomy by allowing the agency the opportunity in the first instance to apply its expertise, exercise whatever discretion it may have been granted, and correct its own errors. Third, it aids judicial review by allowing the parties and the agency to develop the facts of the case in the administrative proceeding. *Fourth, it promotes judicial economy by avoiding needless repetition of administrative and judicial factfinding, and by perhaps avoiding the necessity of any judicial involvement at all if the parties successfully vindicate their claims before the agency.*

Andrade v. Lauer, 729 F.2d 1475, 1484 (D.C. Cir. 1984) (citing and quoting *McKart v. United States*, 395 U.S. 185, 195 (1969)) (emphasis added).

II. Preservation "trigger"

If a main purpose of the exhaustion requirement is to afford federal agencies an opportunity to resolve disputes without involving the judiciary, then the mere existence of an administrative claim should not *automatically* put a federal agency on notice that *litigation* is "reasonably anticipated." The quandary is that an administrative process may take months, even years, to conclude. Thus, even though a federal agency may not "reasonably anticipate litigation" when an administrative claim is filed, if the agency does not issue a litigation hold for potentially relevant ESI at that time, certain ESI may no longer be available if the case ultimately ends up in federal district court. On the other hand, many more administrative claims are filed than are pursued in federal court. If an agency were to issue a litigation hold for all potentially relevant ESI each time an administrative claim were filed, the agency would needlessly waste precious government resources and time. Moreover, were administrative claims used to trigger broad preservation obligations, the Federal Records Act's requirement that federal agencies maintain and *destroy* federal records pursuant to schedules approved by the National Archives and Records Administration (NARA) would be undermined. *See* Federal Records Act, 44 U.S.C. §§ 3101-3106 (2010).

> The head of each Federal agency shall establish and maintain an active, continuing program for the *economical and efficient management* of the records of the agency. The program, among other things, shall provide for . . . cooperation with the Administrator of General Services and the Archivist in applying standards, procedures, and techniques designed to improve the management of records, promote the maintenance and security of records deemed appropriate for preservation, *and facilitate the segregation and disposal of records of temporary value*.

Id. § 3102(2) (2010) (emphasis added).

According to the State Department's Annual Report of the Foreign Service Grievance Board for the Year 2009, 43 new administrative cases were docketed to the Board in 2009. *Available at* http://www.fsgb.gov/Search/docs/Public/Other/Annual_Report_2009.pdf. Approximately one-third of the

43 cases settled prior to decision by the Board. Fifty-three cases closed in 2009. Of the 53 cases closed in 2009, the Board affirmed the agency's decision in 16 cases, reversed the agency's decision in 14 cases, and partially affirmed/partially reversed the agency's decision in 7 cases. Sixteen cases were settled or withdrawn. Only *three* court decisions involving challenges to actions taken by the Board were issued in 2009, two of which had activity at the agency level for many years prior to arriving in federal court.

In one of the three cases to make it to district court, *Henderson v. Ratner*, 677 F. Supp. 2d 37 (D. D.C. 2009), a former State Department employee brought suit against a Foreign Service Board official (Ratner) and the President of the American Foreign Service Association (Naland). In the Complaint, Henderson asserted claims against Ratner and Naland in their personal and professional capabilities for the denial of his administrative claims for retroactive disability. He sought $12 million in damages trebled to $36 million under a theory of a RICO conspiracy. On December 29, 2009, the district court dismissed all claims for lack of subject matter jurisdiction. This case illustrates the difficulty faced by an agency in determining when and whether to issue a litigation hold for ESI. Henderson was involuntarily separated from the State Department in 1981. Should the agency have engaged in a broad preservation effort for ESI then? Henderson did not apply for retroactive disability benefits (the subject of his later court challenge) until 1994. Should the agency have undertaken a broad preservation effort then? The State Department, however, denied the claim as untimely filed in 1996. Should the agency have undertaken a broad preservation effort then? He did not attempt to appeal the decision to the Board until June 2006, at which time the Board determined that it lacked subject matter jurisdiction. Should the agency have undertaken a preservation effort for ESI then? Henderson did not file his complaint in the federal district court until January 2009 and the district court dismissed all claims in December 2009.

In another case, *Olson v. Clinton*, 602 F. Supp. 2d 93 (D.D.C. 2009), a State Department Foreign Service officer challenged the agency's decision related to his employee evaluation reports. On May 22, 1998, Olson filed a grievance with the State Department. On September 30, 1998, the State Department denied the grievance. On November 25, 1998, Olson appealed to the Board. On April 4, 2002, the Board ruled against Olson. On July 7, 2002, Olson filed a Complaint in federal district court. Both sides filed motions for summary judgment. On February 3, 2005, the district court granted in part and denied in part both motions and remanded the case to the Board. On remand, the Board issued its final decision on November 7, 2005. On June 30, 2006, Olson filed a second Complaint in federal district court. Both sides again filed Motions for Summary Judgment. On March 12, 2009, the district court granted the State Department's Motion for Summary Judgment. *Id.* at 104. At what moment in time during this 11-year period should the agency have undertaken a broad preservation effort for ESI, if at all?

In *Baltimore v. Clinton*, Civil Action No. 09-0458 (Nov. 16, 2009), a case that has not yet come to a conclusion, Ambassador Baltimore was issued a 45-day suspension for three offenses: (1) misuse of his official position, (2) failure to report a gift, and (3) wilful misuse of a government-owned vehicle. The Board upheld the suspension and denied the grievance. Baltimore appealed on the grounds that the Department later published the gift in the *Federal Register* as a gift to the United States. The court remanded the case to the Board for it to consider the *Federal Register* entry. Even for a relatively short time period, should the agency engage in a broad preservation effort for ESI each time one of its employees is suspended?

So, how might the proposed Preservation Rule impact this one agency? If initial grievances were considered to fall within the scope of the "filing of an administrative claim," the agency might be required to take affirmative steps to identify and locate ESI potentially relevant to all claims and defenses for each of the grievances docketed to the Board in a given year. That framework does not appear to be a cost-effective or workable approach.

The cases discussed above illustrate the problem for many federal agencies grappling with E-Discovery. Many federal agencies are looking to formulate their own rules, regulations, or policies to govern when litigation is "reasonably anticipated" such that a litigation hold for ESI will be issued. Some agencies are turning to the Federal Civil Rules for guidance in developing their policies. The Federal Civil Rules recognize that discovery generally will not occur in certain cases and thus exempts the proceedings from the Initial Disclosure requirements of Rule 26(a). These proceedings include:

> (i) an action for review on an administrative record;
>
> (ii) a forfeiture action in rem arising from a federal statute;
>
> (iii) a petition for habeas corpus or any other proceeding to challenge a criminal conviction or sentence;
>
> (iv) an action brought without an attorney by a person in the custody of the United States, a state, or a state subdivision;
>
> (v) an action to enforce or quash an administrative summons or subpoena;
>
> (vi) an action by the United States to recover benefit payments;
>
> (vii) an action by the United States to collect on a student loan guaranteed by the United States;
>
> (viii) a proceeding ancillary to a proceeding in another court; and
>
> (ix) an action to enforce an arbitration award.

Fed. R. Civ. P. 26(a)(1)(B). Federal agencies, therefore, might explore whether they could in good faith determine that discovery is not "reasonably anticipated" in these types of proceedings and reasonably and in good faith decline to issue broad litigation holds for matters that fall within these categories.

The United States and its employees also enjoy some unique defenses. For example, the defense of qualified immunity shields government officials "from liability for civil damages insofar as their conduct does not violate clearly established statutory or constitutional rights." *Harlow v. Fitzgerald*, 457 U.S. 800, 818 (1982). Qualified immunity is an "entitlement not to stand trial or face the other burdens of litigation . . . ." *Mitchell v. Forsyth*, 472 U.S. 511, 526 (1985). The Supreme Court has stated that "[t]he basic thrust of the qualified-immunity doctrine is to free officials from the concerns of litigation, including 'avoidance of disruptive discovery.' " *Ashcroft v. Iqbal*, 129 S. Ct. 1937, 1953 (2009) (citing and quoting *Siegert v. Gilley*, 500 U.S. 226, 236 (1991) (Kennedy, J., concurring)).

> Serious and legitimate reasons validate this notion. If a Government official is to devote time to his or her duties, and to the formulation of sound and responsible policies, it is counterproductive to require the substantial diversion that is attendant to participating in litigation and making informed decisions as to how it should proceed. Litigation, though necessary to ensure that officials comply with the law, exacts heavy costs in terms of efficiency and expenditure of valuable time and resources that might otherwise be directed to the proper execution of the work of the Government.

Id. at 1953.

In light of this recent language from the Supreme Court, federal agencies have additional factors beyond those weighed by the private sector to consider.

III. Scope of preservation and judicial review

Under numerous statutory schemes, federal agencies compile an administrative record to document the agency's decision-making and dispute resolution processes. Under the Employee Retirement and Income Security Act (ERISA), for example, "[a] court may consider only that evidence presented to the plan administrator at the time he or she determined the employee's eligibility in accordance with the plan's terms. The court's review is thus limited to the administrative record." *Schwalm v. Guardian Life Ins. Co. of Am.*, 626 F.3d 299, 308 (6th Cir. 2010). Under the Comprehensive Environmental Response, Compensation and Liability Act of 1980 (CERCLA), "judicial review normally is limited to the administrative record as it existed at the time of the challenged agency action." *United States v. JG-24, Inc.*, 478 F.3d 28, 33-34 (1st Cir. 2007). Moreover, under the Administrative Procedure Act (APA), "the focal point for judicial review should be the administrative record." *Camp v. Pitts*, 411 U.S. 138, 142 (1973). "[T]he designation of the Administrative Record, like any established administrative procedure, is [generally] entitled to a presumption of administrative regularity." *Bar MK Ranches v. Yuetter*, 994 F.2d 735, 740 (10th Cir. 1993). If the court finds the agency's record inadequate, "the proper course, except in rare circumstances, is to remand to the agency for additional investigation or explanation." *Fla. Power & Light Co. v. Lorion*, 470 U.S. 729, 744 (1985). Importantly, before a reviewing court may permit discovery and evidentiary supplementation of the administrative record, "there must be a strong showing of bad faith or improper behavior." *Citizens to Preserve Overton Park, Inc. v. Volpe*, 401 U.S. 402 (1971); *see also Maxey v. Kadrovach*, 890 F.2d 73, 77 (8th Cir. 1989).

Accordingly, if a federal agency has a formal process in place for identifying and preserving information that it considered in reaching its decisions, should the judiciary interfere with that process by requiring that all ESI potentially relevant to any claim or dispute be preserved pre-litigation in cases that the agency reasonably anticipates will be reviewed on an administrative record?

The federal employment discrimination context is particularly instructive. It has an extensive, multi-layered administrative process that can extend over several years: "In the federal sector, individuals file complaints with their own federal agencies and those agencies are to conduct a full and appropriate investigation of the claims raised in the complaints. Complainants can then request a hearing before an EEOC [Equal Employment Opportunity Commission] administrative judge . . . . [T]he Commission . . . adjudicates appeals of federal agency actions on discrimination complaints, and ensures agency compliance with decisions issued on those appeals." *See* EEOC FY 2009 PERFORMANCE AND ACCOUNTABILITY REPORT, 26, *available at* http://www.eeoc.gov/eeoc/plan/upload/2009par.pdf. In fiscal year 2009, the EEOC resolved 6,779 complaints in the federal sector out of a total of 7,277 requests for hearings. These hearings "secured more than $44.5 million in relief for parties in these complaints." *Id*. The EEOC further resolved 4,287 of the total 4,745 appeals of final agency action. The high percentage of claims resolved and the significant amount of monetary relief obtained during the administrative process may indicate that the information gathered during the administrative process is sufficient to fairly and adequately resolve discrimination claims. If that is the case, should the courts impose an additional burden by requiring that all ESI potentially relevant to any claim or defense be preserved pre-litigation? Naturally, once the parties arrive in federal court, the court may allow additional discovery. But, should federal agencies be required by the courts to undertake a broad preservation effort for ESI during the administrative phase if the agency has a process in place for gathering the information it deems necessary to resolve the dispute?

Applying the Sedona Conference guidelines previously discussed, it might be reasonable for federal agencies to narrow the scope of preservation of ESI in light of the nature and facts of certain types of government cases where the agency already has a process in place for identifying and compiling

much of the information the agency has determined, in its experience, is needed to resolve the matter. *See* Theodore C. Hirt, *Applying "Proportionality" Principles in Electronic Discovery - Lessons for Federal Agencies and Their Litigators* in this issue of the United States Attorneys' Bulletin.

IV. Sanctions for pre-litigation spoliation

The majority view is that the Federal Rules of Civil Procedure do not authorize the trial court to impose sanctions for pre-litigation spoliation. *United Med. Supply Co., Ins. v. United States*, 77 Fed. Cl. 257, 268 (2007). The court, therefore, must rely upon its inherent power to impose such sanctions. In *Chambers v. NASCO, Inc.*, 501 U.S. 32, 50 (1991), the Supreme Court ruled that "when there is bad-faith conduct in the course of litigation that could be adequately sanctioned under the Rules, the court ordinarily should rely on the Rules rather than the inherent power. But if in the informed discretion of the court, neither the statute nor the Rules are up to the task, the court may safely rely on its inherent power." The Court further explained that "[b]ecause of their very potency, [the court's] inherent powers must be exercised with restraint and discretion." *Id.* at 44. Even though the *Chambers* Court described "bad faith" as a pre-condition to the lower court's exercise of its inherent power to sanction, a split exists among the circuits about the level of culpability required before the trial court may exercise its inherent power to impose sanctions for pre-litigation spoliation. United States District Judge Rosenthal examined the split in *Rimkus Consulting Grp, Inc. v. Cammarata*, 688 F. Supp. 2d 598, 614-15 (S.D. Tex. 2010) (stating that the Fifth, Seventh, Eighth, Tenth, Eleventh, and D.C. Circuits require bad faith; the Second Circuit permits an adverse inference sanction for negligent destruction; the First, Fourth, and Ninth Circuits do not require bad faith where prejudice is severe; the Third Circuit balances the degree of fault and prejudice).

Notwithstanding the split in the circuits regarding the culpability required before a court may exercise its inherent power to impose sanctions,

> [i]t is well established that a party seeking the sanction of an adverse inference instruction based on spoliation of evidence must establish that: (1) the party with control over the evidence had an obligation to preserve it at the time it was destroyed; (2) the evidence was destroyed with a culpable state of mind; and (3) the destroyed evidence was "relevant" to the party's claim or defense such that a reasonable trier of fact could find that it would support that claim or defense.

Rimkus, 688 F. Supp. 2d at 615-16 (citing *Zubulake IV*, 220 F.R.D. at 220). Consequently, if the United States were to face facts and circumstances similar to those presented in *Zubulake*, could the United States avoid an adverse inference instruction by showing that it had in good faith adopted and followed a reasonable litigation hold policy or procedure that set forth both the *trigger* and *scope* of preservation of ESI pre-suit? As to the imposition of adverse inference findings or other spoliation sanctions, to what extent would or should the court defer to the agency's determinations as to the proper trigger and scope of pre-litigation preservation?

The courts have long deferred to a federal agency's reasonable interpretation of the statutory scheme it is charged with administering. *Chevron, U.S.A., Inc. v. Natural Res. Def. Council, Inc.*, 467 U.S. 837, 844 (1984) ("[A] court may not substitute its own construction of a statutory provision for a reasonable interpretation made by the administrator of an agency."); *see also Skidmore v. Swift*, 323 U.S. 134, 140 (1944) ("We consider that the rulings, interpretations and opinions of the Administrator under this Act, while not controlling upon the courts by reason of their authority, do constitute a body of experience and informed judgment to which courts and litigants may properly resort for guidance."). Judicial deference has also been extended to an agency's reasonable interpretation of its own regulations.

Auer v. Robbins, 519 U.S. 452 (1997) (holding that agency's opinion letter interpreting regulations entitled to judicial deference); *Mayo Found. for Med. Educ. & Research v. United States*, 131 S. Ct. 704 (2011) (re-affirming *Chevron* deference as the appropriate standard for court's review of agency regulations). Notably, the APA supplies a deferential and narrow scope of judicial review of agency action. 5 U.S.C. § 706(2)(A)-(F) (2011) (delineating the narrow criteria by which a federal court will review federal agency action).

V. Conclusion

In conclusion, settled principles governing judicial review of federal agency action can inform how a court might review a federal agency's preservation decisions pre-litigation. According to the Sedona Conference, even private parties are entitled to some deference when the court reviews preservation decisions. A court's review "of a legal hold decision should be based on the good faith and reasonableness of the decision (including whether a legal hold is necessary and how the legal hold should be executed) at the time it was made." Guideline 5, The Sedona Conference® Commentary on Legal Holds: *The Trigger and the Process* (Aug. 2007). Rather than regulate a federal agency's pre-suit decisions by a Preservation Rule, it can be argued that the court should review with some measure of deference an agency's pre-litigation decisions, especially if the agency weighed the relevant factors and balanced competing interests in good faith. Even in the absence of a formal agency policy, the court might still accord a federal agency the deference generally due agency decisions. Were the agency to adopt a formal litigation hold policy, the policy certainly could inform and assist the court's review of the agency's pre-litigation preservation decisions.❖

ABOUT THE AUTHOR

❑**Sarah Michaels Montgomery** was appointed by the Deputy Attorney General to serve as Senior Litigation Counsel for E-Discovery for the Department of Justice. Among other primary responsibilities, Mrs. Montgomery coordinates the E-Discovery efforts across all of the civil litigating components of the Department, including Antitrust, Civil, Civil Rights, Environment and Natural Resources, Tax, as well as the Civil Divisions in all of the USAOs' 94 districts. She has also been charged with the task of reaching out to federal agencies to help them improve their civil E-Discovery capabilities.✠

Flying Cars and Web Glasses: How the Digital Revolution is Changing Law Enforcement

John Haried
Assistant National Criminal Discovery Coordinator
Department of Justice

I. Introduction

The Jetsons, Star Wars, and The Matrix gave us glimpses of futuristic worlds of high technology, including flying cars, intelligent robots, and instant access to any information. Yes, flying cars may take a few more years. But the digital revolution is already here. The future is now. Digital technology is rapidly reshaping how people violate the law and where key evidence can be found. Today, more than 93 percent of new information begins its life in some digital format. Most electronically stored information (ESI) is never printed to paper and exists only in digital forms: emails and text messages, electronic business records, wiretap data, digital photos, and more. The digital revolution has created marvelous new opportunities for law enforcement to catch more offenders and make better cases provided, of course, that attorneys and investigators embrace new technologies and use them to their advantage.

The importance of ESI as evidence is growing every day. Yet few attorneys use the litigation software tools already on their desktops. Until now, computers and ESI were something that many attorneys and investigators ignored or passed off to someone else to master. That approach will not work anymore because the digital revolution has wrought fundamental changes in the world of information and evidence. Today, gathering ESI or competently laying the foundation for admission of ESI requires acumen and fluency in the digital world. Judges increasingly expect attorneys to understand digital technology and terms well enough to intelligently explain them to the court and to opposing counsel and to help solve any problems that arise in gathering, preserving, and producing ESI in discovery.

This article will explore the digital technology trends affecting law enforcement, where to look for critical evidence, the new skills that attorneys and investigators must acquire to be competent, and what the Department of Justice (the Department) is doing to meet the challenges of the digital revolution.

II. How the digital revolution will help law enforcement

Defendants use digital technologies to plan, communicate, purchase supplies, keep records, conduct transactions, and collect their ill-gotten gains. The more defendants use digital technology, the more their digital trails grow. Consequently, the digital revolution is great news for law enforcement because digital devices and systems are designed to *record* information. They record a cornucopia of information that proves what defendants were doing, whom they did it with, and what they were thinking. A defendant's own emails, texts, internet searches, and browser histories–all *recorded* in digital formats for investigators to find lawfully and analyze–are proof of actions, identity, intent, motive, and conspiracy.

A. Digital world

The Internet will become much faster–eventually up to 10,000 times faster–and it is being integrated into more and more products. Mobile computing will define the future. People will rely primarily on their cell phones and tablet computers such as iPads to maintain a constant connection to the Internet for communicating, socializing, working, collaborating, shopping, paying for purchases, banking, sharing files, and finding information. The world currently has 6.9 billion people and 5 billion cell phones, an increase from the 3 billion cell phones in 2007. Statistics demonstrate that cell phones outnumber personal computers three to one. BBC NEWS, www.bbc.co.uk/news (July 9, 2010). Today, 77 percent of North Americans, 58 percent of Europeans, 11 percent of Africans, and 29 percent of the world's population use the Internet. INTERNET WORLD STATS, www.internetworldstats.com. Internet use will rise dramatically in many countries as Internet-connected cell phones and tablet computers proliferate around the globe.

Digital technology is changing how crimes will be committed. How will con men find and defraud their victims? Facebook. Where will bank robbers–at least the ones who still rob brick and mortar banks–find maps and photos and plan their getaway? Google. How will the defendants who rob virtual banks commit their crimes? They will commit their crimes at home in their bathrobes with no mask or gloves because all they need is the Internet. How will defendants demonstrate their consciousness of guilt? By attempting to delete their digital footprints from their cell phones and Internet browsers or by creating false digital personas. Defendants habitual use of technology to commit crimes will leave an extensive trail of *recorded* data about their actions and motives that investigators may lawfully collect and analyze.

B. Cameras

Employers and governments are deploying cameras in a wide range of public areas–streets, highways, stores, offices, campuses, and malls. These cameras digitally *record* peoples' faces, behaviors, and license plates. Defendants and the public are creating an enormous trove of potential evidence using cell phone cameras, Facebook, Flickr, Picasa, and YouTube. Soon, investigators using facial recognition software, artificial intelligence software, and other tools will mine that data to reconstruct defendants' actions.

C. Tracking and "push marketing"

To enable tracking and "push marketing," GPS chips, radio-frequency identification (RFID) chips, and other sensors are being embedded everywhere, including cell phones, iPads, employee badges, personal and rental cars (electronic toll collection, OnStar), freight containers, passports, and products. Tied to the internet, they track and record the movements of people and things, leaving behind a trail for investigators to reconstruct. Digital marketing and new technologies may inadvertently aid law enforcement. For example, people will sign up for a cell phone application that allows restaurants and retailers to send, or "push," discount coupons to the customer's phone as the customer comes nearby. Investigators can lawfully collect that data to determine whether a suspect was in that area.

D. E-communications

Increasingly, social and commercial relationships will be based upon digital interactions. In 2005, Facebook had five million accounts. Today there are 500 million Facebook accounts. In 5 years, maybe 2 billion accounts or more? Today, cell phone users in the United States send almost 5 billion text messages *per day*. CTIA WIRELESS INDUSTRY SURVEY, www.ctia.org. How will murderers track their

victims? Facebook. Where will defendants conspire? Facebook and text messages. Where will defendants brag? Facebook, text messages, or Twitter, which has grown to 200 million accounts since 2006. Facebook and Twitter are simply examples of today's technology. They may dominate the market for years or new technologies and services may replace them, but the digital evidence will exist somewhere.

E. Delivery

Designers are creating new products to instantly deliver information from the Internet to mobile users. One product being studied is web-connected eyeglasses that use a camera embedded in the wearer's frame to scan places or people within the wearer's sight, send those images through the Internet to a database, and then instantly display names or directions on the wearer's lenses. Someday, when a defendant uses those web glasses–or other new products that come along–his data selections will be able to reveal his location, intent, and motives.

F. Artificial intelligence

How far has artificial intelligence progressed? In February 2011, the game show Jeopardy pitted Watson, an IBM artificial intelligence computer, against two Jeopardy all-time champions, Ken Jennings and Brad Rutter. Watson was designed to demonstrate a computer's ability to answer questions expressed in ordinary human language, learn from experience, and respond with lightning speed. The results were unequivocal. Watson won $77,147, compared to Jennings' $24,000 and Rutter's $21,600. The results do not prove computers are superior to humans in making thoughtful judgments. However, they do demonstrate the tremendous capacity of today's artificial intelligence software to understand natural human language in context, search enormous databases, and quickly provide accurate answers.

Right now litigation software engineers are working to harness the power of artificial intelligence computing to search large volumes of ESI. The transformation from today's simple key word searches to tomorrow's complex thinking searches will be akin to moving from a cupcake recipe to writing a novel. Eventually, artificial intelligence software will do the work of dozens of investigators by reviewing digital evidence much faster and with greater reliability. Artificial intelligence software will comb through thousands or millions of emails, text messages, digital database entries, bank transactions, and phone calls, and it will identify patterns, hot documents, and key transactions along the way, while eliminating duplicate documents. Artificial intelligence software will augment, not replace, attorneys' and investigators' thinking. Someday soon it will be remarkable to think of how cases were ever investigated without digital assistance.

G. Cloud computing

The individual user's computer hard drive will gradually lose its role as the place where people store their software applications and files. Instead, people will use the Internet to access a remote server "in the cloud," where a vendor supplies software applications, Internet services, and data storage. Those servers could be located in Omaha, Beijing, or Azerbaijan. Web-based email services like Hotmail, Yahoo! Mail, and Gmail are examples of cloud computing. Facebook is cloud computing. Companies are contracting with cloud vendors to host their inventory systems, data processing, financial accounting, and personnel files because cloud computing offers several advantages: someone else maintains and upgrades the servers and software; the user can access her data from anywhere with an Internet connection; and the service is state-of-the-art.

The private sector is not alone this transformation. In December 2010, the United States' Chief Information Officer announced a 25-point plan to immediately begin moving federal government

information technology to the cloud. The plan is available at www.cio.gov. That shift will have substantial implications for discovery in criminal and civil cases.

One trend is that the data on a defendant's digital device, say a GPS in a car, will routinely be recorded in the cloud. Thus, law enforcement may not need to seize a suspect's car because the important data can be obtained lawfully from the cloud vendor. Of course, defendants will try to use the cloud to hide their misdeeds by creating accounts using false personas, commingling their data with the data of an innocent third party, or putting their data on a server in a country with strict privacy laws. Perhaps some impoverished country will try to become for data storage what Switzerland was for banking, a place where customers have secret account numbers on cloud servers and the government tries to protect their secrecy.

H. Security and privacy

In February 2011, national security experts warned that cyberattacks are the greatest future threat to the United States' security. Because any Internet connection will suffice for criminal purposes, more defendants will reside and operate from outside the United States. As people increasingly rely on the Internet as a place to work, shop, and store valuable information, more emphasis will be placed on protecting computer systems from hackers, protecting on-line personal information, and defining electronic privacy. Law enforcement will depend on international collaboration to investigate and collect evidence overseas. Courts, legislators, and regulators in the United States, the European Union, and elsewhere are already grappling with questions concerning government investigators' access to individuals' digital communications and data to investigate law violations. The Wikileaks investigation is a recent example. Cross-border discovery of ESI is a hot issue before the European Commission's Data Protection Working Party. *See* http://ec.europa.eu/justice/policies/privacy/working group/index_en.htm for more information.

I. Digital sophistication

Smart defendants will become much more savvy about covering their tracks with encryption, steganography (the use of concealed messages in documents understood only by the sender and receiver), concealment, and destruction. When uncovered by investigators, the digital trail will be compelling evidence of consciousness of guilt. However, not all defendants are smart. Many criminals will not realize that they are creating a digital trail every time they use their cell phone or browser.

J. Increasing Digital Crimes

Identity theft will continue to increase dramatically. Fraud schemes will depend less on face-to-face conversations and more on digital interactions. Thefts of services, trade secrets, and intellectual property will also increase. Computer hacking to collect sensitive information or destroy computer services will rise. The success of the Stuxnet software worm in sabotaging Iranian nuclear centrifuges in 2010 illustrates what is at stake in national defense. There will be a sharp increase in the number of sophisticated cyberattacks aimed at commerce, research, banking, securities, technology, and the military.

III. Law enforcement adaptations to a digital world

A. How will investigators and attorneys know how much ESI to gather?

One of the biggest challenges facing law enforcement will be determining how much ESI to gather. The volume of available ESI is staggering and too much data will quickly overwhelm an investigation. One gigabyte of information contains 894,000 pages of plain text, an amount equal to a semitrailer stuffed full of paper. One terabyte is 916,000,000 pages of plain text, or a 1,000 truckloads of paper. Using human eyes to examine every piece of ESI is impossible. Consequently, law enforcement will use artificial intelligence software, coupled with manual review and judgment, to find evidence.

Thus, accurately framing the scope of a demand for ESI in a search warrant, grand jury subpoena, administrative subpoena, civil discovery request, or civil investigative demand will be a critically valuable skill. Investigators and attorneys will need substantial knowledge about how digital systems generally work as well as the particular system containing the information they seek. Surreptitious investigation, detailed planning, and intelligent communication with system managers will remain essential tools of the trade.

B. What will law enforcement need to collect and analyze?

Forensic collection, analysis, and support will be critical for getting the most out of the digital evidence available. Specific training is also an important component. The Department's Computer Forensics Working Group is coordinating the development of forensic resources, protocols, and field guidance. The National Advocacy Center provides training for attorneys, agents, paralegals, and legal assistants on litigation software, ESI management, and criminal and civil discovery. Increasingly, training and support will be delivered to investigators, attorneys, and support staff on the Department's Intranet through live webinars, Intranet Web sites, and instructional videos. On the civil side in particular, the Department is designating attorneys and support staff to be Electronic Discovery Office Coordinators.

Investigative agencies are also creating new tools for agents. The Drug Enforcement Administration has just rolled out its IMPACT system for managing case information and the FBI is working to get simple forensic tools in the hands of agents for forensically sound, but quicker assessment of cell phones, CDs, thumb drives, and hard drives.

C. What tools can attorneys use to manage all of the case information?

Paper systems of 3-ring notebooks filled with hot documents, trial binders, paper folders, and file drawers will disappear. They are being replaced with litigation software for electronic management of case information that enables investigators and attorneys to electronically manage, analyze, and organize their evidence. The best and brightest young attorneys and investigators will expect digital systems because that is what they know. The Department has already provided its attorneys with excellent software tools and resources:

- **CaseMap** is software for the prosecution team to organize their key information and analytical thinking about facts, evidence, witnesses, events, issues, witness questions, and legal research. The software has easy-to-use spreadsheets that link all of this information together; for example, it links a fact to the digital image of the evidence, why the fact is important, and the testifying witness. CaseMap is an excellent tool for creating a simple fact chronology, keeping a list of witnesses with their contacts, maintaining an inventory of the evidence, tracking subpoenas and discovery productions,

keeping a list of hot documents, scribbling witness questions, and linking legal issues to pertinent cases, statutes, and regulations. As a result, attorneys, investigators, and paralegals are able to effectively use this system to organize their analysis with large amounts of information. Thus, CaseMap promotes teamwork in identifying critical case information, preserves the team's institutional knowledge about the case, and helps the team organize and plan for charging, motions, trial, and appeal.

- **TextMap** is software used for managing testimonial evidence, including witness interviews, grand jury transcripts, and depositions. TextMap links to CaseMap, so testimony relevant to a fact or legal issue can be opened with a mouse click.
- **TimeMap** is software for creating timelines to show the relationships between key events in a case.
- **IPRO** is software for scanning paper documents to an electronic image and converting native files, such as word processing, PowerPoint presentations, and emails, to digital images along with searchable text. IPRO will Bates number discovery productions, providing a simple index of discovery. IPRO allows attorneys to manage discovery production right from their desks, leaving the originals intact and stored securely. The information that IPRO produces can be linked with the CaseMap file.
- **Concordance and Summation** are software database systems designed for managing large collections of evidence, for example, records, correspondence, interviews, transcripts, photos, video, and spreadsheets. These systems track case evidence at a document level, allowing staff to search the contents of documents, code documents for relevance to the investigation, and ultimately produce documents in discovery. Both Concordance and Summation are excellent tools for full-text searches and coding documents and both allow the user to create his own tags to identify particular files, such as hot doc, relevant, privileged, etc., and then select documents for additional review according to their tags.
- **Sanction** is a trial presentation software designed to electronically display evidence at trial. Sanction can display images, photos, audio, and video files. Exhibits can be endorsed with exhibit number stickers and have annotations such as highlights, arrows, and redactions, as well as side-by-side comparisons of signatures, fingerprints, and more.
- **The Litigation Technology Service Center (LTSC)** is a resource for U.S. Attorneys that provides scanning of paper documents, optical character recognition (OCR), Bates-stamping, and de-duplication of emails and other digital files for cases that are too large to handle in-house, but not big enough for Mega-3 contracts. The LTSC also provides Electronic Data Discovery processing and hosting.
- **Mega-3 Contracts** provide litigation support for cases with very large amounts of discovery, including scanning, OCR, document organization, coding, and discovery databases. They also provide document coders, document analysts, statisticians, translators, paralegals, and support personnel, like project managers. The Mega-3 vendors are Labat-Anderson, Inc., Lockheed-Martin, Inc., and CACI, Inc.

D. How will investigators and attorneys collaborate?

Investigators and attorneys will work together online over secure intranet connections, in the same way that LEO or Law Enforcement On-Line enables agents to collaborate today. They will access the same set of case materials–interviews, transcripts, records, photos, data compilations–and collaborate on building an electronic case file where they keep critical case information. Key to electronic sharing between investigators and attorneys is standardization of electronic file formats to enable the efficient flow of case information. For that reason, the Department has undertaken a Pilot Project for Case Information Management to create templates, protocols, file standards, and best practices for investigators and attorneys to manage their information using the tools they already have.

E. How will discovery change?

All discovery will be provided electronically and paper discovery will be confined to historical or legacy collections, although most organizations have already imaged their paper collections to make access easier and to save on storage costs.

Parties in both criminal and civil cases, particularly multi-party cases, will want to put all discovery on Internet sites for easy access, to have a central repository, and to cut costs. This strategy will, of course, provoke concerns about the security of discovery materials because criminal case discovery often contains protected grand jury, victim, or informant information. Even with paper discovery productions, courts often restrict criminal defendants' access to and dissemination of discovery materials. Both criminal and civil discovery may contain trade secrets or other confidential business information or privileged materials. Posting criminal discovery on the Internet increases the risk of unauthorized access to the government's discovery by the defendant's associates and its widespread dissemination. The advent of the Web site, Who's a Rat? (self-described as "The largest on-line database of informants and agents!"), and other underworld efforts to retaliate against ordinary citizen witnesses illustrate the risks of unauthorized dissemination of the government's discovery. Therefore, courts, litigants, and vendors will develop new standards for the access to and security and dissemination of discovery materials posted on-line.

F. How will investigative teams manage their own potentially discoverable e-communications?

Text messages between investigators and informants, voice mails from witnesses to attorneys, and emails between investigators are all examples of e-communications that may contain potentially discoverable information. The technical and logistical difficulties involved in collecting, preserving, and reviewing text messages and other e-communications are cropping up in enforcement cases. For example, in *United States v. Suarez*, 2010 WL 4226524 (D.N.J. Oct. 21, 2010), the government was sanctioned with a spoliation of evidence instruction when it was unable to produce a portion of the text message traffic between the agent and informant during a long investigation. *Id.* at *1. In a drug deal or mortgage fraud sting, an undercover investigator might have to use text messaging to maintain his cover and communicate with a target, so simply banning text messages is not a viable option. Similarly, law enforcement agencies operating in different time zones with far-flung offices rely on email to coordinate investigations. No simple solutions are available today.

On March 30, 2011, Deputy Attorney General James M. Cole issued guidance for investigators and attorneys concerning their own e-communications with prosecution team members, victims, and witnesses to ensure the preservation and review of potentially discoverable e-communications. The guidance recommends common sense "dos and "don'ts" for using e-communications and it addresses

recurring legal issues. Moreover, all Department components are reviewing their information technology structures to develop systems that can preserve their own potentially discoverable e-communications.

G. How will the digital revolution change job functions?

The backbone of litigation teams will be electronic information management, that is, collecting digital information according to forensically sound protocols, producing discovery electronically, and electronically organizing and analyzing case information, including interviews, investigative reports, forensic examinations, databases, and more. Every team member–attorneys, investigators, analysts, paralegals, and legal assistants–will need to be proficient in using software to help manage the flood of digital information. Knowing the software tools and using them will not be someone else's job; it will be every team member's responsibility.

In particular, investigators and legal assistants will be on the front lines of managing case information. They will use litigation software to log evidence, identify significant testimony, organize key evidence, and support the team's work. From the beginning of an investigation, the team will create their work product–namely, witness interviews, deposition summaries, evidence and subpoena logs–in electronic formats so it may readily be transmitted to other team members, searched, and linked to other files in CaseMap. The team will inventory all the evidence and information they collect so that, when it comes time to provide discovery, they can review what they have, make disclosure determinations, and track what was produced or withheld.

H. Where will the Department's attorneys turn for help?

The Department is creating a new Intranet Web site to provide support regarding the use of litigation software, criminal and civil discovery, E-Discovery, and ESI collection, preservation, analysis, and production. From their desktops, attorneys will have access to policy, guidance, best practices, templates, go-bys, FAQs, case law, sample briefs, and Intranet-based training for criminal and civil cases. Users will also be able to have discussion threads on particular problems or ideas and find expertise within the Department.

III. Conclusion

The digital revolution is creating terrific opportunities for law enforcement to catch and successfully prosecute those who violate the law. The advent of DNA testing gave law enforcement a powerful new tool for identifying defendants. The fruits of the digital revolution are equally valuable to law enforcement, and perhaps more so, because they provide the defendant's self-created trail of evidence, revealing his actions, movements, thoughts, decisions, and fellow collaborators. It is impossible, of course, to forecast all the ways that technology might evolve or how new products or systems might assist law enforcement. There may never be web glasses or flying cars but it is certain that fantastic inventions, unimaginable today, will create a trail of digital evidence in the future.❖

ABOUT THE AUTHOR

❑**John Haried** is the Assistant National Criminal Discovery Coordinator for the United States Department of Justice. He has been an Assistant United States Attorney in Colorado for 21 years and was a state prosecutor in Boulder, Colorado for 8 years. Mr. Haried received the Directors Award from the Department of Justice in 2009. He frequently serves as an instructor for the Office of Legal Education at the National Advocacy Center on electronic management of case information and discovery-related topics.✠

The author wishes to thank Christine Riddell, Litigation Support Specialist, Antitrust Division, U.S. Department of Justice, for her invaluable assistance in the preparation of this article.

What We See in the Clouds: A Practical Overview of Litigating Against and on Behalf of Organizations Using Cloud Computing

Allison C. Stanton
Director of E-Discovery
Civil Division
U.S. Department of Justice

Andrew J. Victor
Trial Attorney
Torts Branch, Civil Division
U.S. Department of Justice

I. Introduction

Where is the evidence? This question, while always a challenging one, elicited a simpler answer before the dawn of the twenty-first century. Today much of the complexity arises from the tremendous effort to locate, collect, and use electronically stored information in both civil and criminal cases. These processes have compelled companies, local governments, and federal agencies alike to embrace "cloud computing," the next step in the evolution of electronic data storage, and to outsource their data, services, and Information Technology (IT) infrastructure. As a result, litigators are challenged to adapt old strategies to new technology when litigating against or on behalf of organizations using cloud computing.

This article will provide a basic overview of cloud computing, explain the current movement of federal agencies and the private sector into the cloud, discuss the opportunities and challenges for litigators when confronted with this technology, and provide practical suggestions for litigators when seeking evidence in the cloud.

II. What is this "cloud" you speak of?

United States Chief Information Officer, Vivek Kundra, stated that "[j]ust as the Internet has led to the creation of new business models [that were] unfathomable 20 years ago, cloud computing will disrupt and reshape entire industries in unforeseen ways." VIVEK KUNDRA, FEDERAL CLOUD COMPUTING STRATEGY 33 (2011). Cloud computing appears in many forms but the common underlying feature is that a person accesses software programs or creates, saves, and retrieves data from a group of computers usually owned by a third-party, the cloud service provider. The user accesses the data via the Internet. Cloud computing extends to a wide range of services from payroll systems to research and development databases. One of its most common services, however, is Web email, where a user composes, receives, and saves email by logging into a Web site. Traditionally, email would be located on a computer owned and located in the organization. With cloud computing, the user can still access their account via a company or personal computer but the email messages are located on a server owned by a third-party.

The National Institute of Standards and Technology (NIST) defines cloud computing as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources . . . that can be rapidly provisioned and released with minimal management effort or service provider interaction." NIST Definition of Cloud Computing, version 15 (2009). Cloud computing has five basic characteristics: (1) shared resources, (2) scalability, (3) elasticity, (4) pay-as-you-go, and (5) self-provisioning of resources. TIM MATHER ET AL., CLOUD SECURITY AND PRIVACY: AN ENTERPRISE PERSPECTIVE ON RISKS AND COMPLIANCE (2009).

The shared resources characteristic involves multiple users employing the same resources, similar to multiple organizations using the same warehouse to store boxes of files. Scalability is the ability to scale up to massive numbers of systems, bandwidth, and storage space. Elasticity is how users can rapidly increase and decrease resources as needed, analogous to increasing the shelf space used in a warehouse and then decreasing it when the storage is no longer needed. Pay-as-you-go refers to paying only for resources used for the time needed, such as renting storage space only for as long as necessary. Self-provisioning of resources occurs when users decide what additional systems, software, and/or network resources are needed.

There are also different types of clouds. Each type of cloud is named after the type of groups who share the space in the cloud. A "private cloud," for example, is operated solely for an organization so that individuals outside of the organization are unable to access the cloud. A "public cloud" is made available to the general public or a large industry group and is owned by an organization selling cloud services. *See infra* Figure 1. A "community cloud" is shared by several organizations and supports a specific community that has shared concerns.

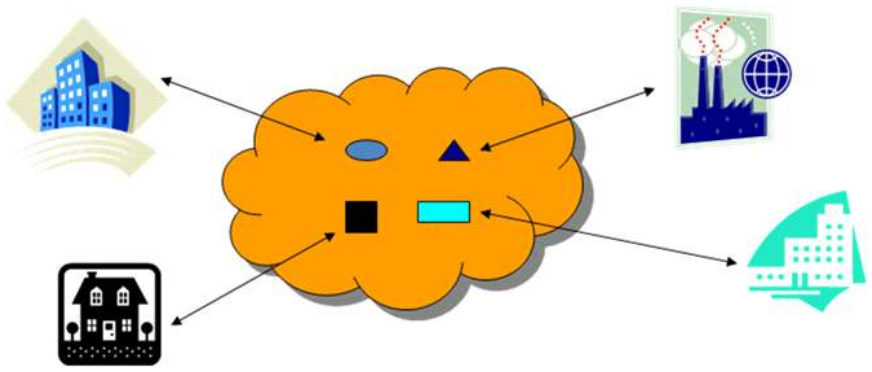

FIGURE 1: example of a public cloud.

Three common cloud computing services have been developed for each of these three types of clouds: (1) software-as-a-service (SaaS), (2) platform-as-a-service (PaaS), and (3) infrastructure-as-a-service (IaaS). As these names denote, cloud computing offers services to users, transforming the traditional computing operations into something closer to a common utility, such as electricity or water, a resource that can be used on demand. SaaS, for example, can be an email service or something more complex like payroll software used by an organization. Instead of accessing the software on its own computers, the organization accesses and runs an application hosted on a cloud provider's servers. TIM MATHER, ET AL., CLOUD SECURITY AND PRIVACY: AN ENTERPRISE PERSPECTIVE ON RISKS AND COMPLIANCE (2009).

Cloud computing also offers economic efficiencies and benefits for an organization. SaaS, IaaS, and PaaS allow an organization to reduce its reliance on internal IT infrastructure by requiring only a

connection to the Internet. An organization, for example, no longer has to buy expensive computer equipment or software licenses to run email systems in-house. A cloud provides one central location for data or applications, eliminating the need to establish multiple systems or IT centers that may spread across a large geographic space. An organization also does not have to worry about repairing or trouble-shooting the systems it uses because the cloud provider performs that responsibility. These cost savings benefits are some of the main characteristics that have attracted organizations, and now federal agencies, to this new technology.

III. Movement of federal agencies and the private sector to the cloud

The government's responsibility is "to achieve the significant cost, agility and innovation benefits of cloud computing as quickly as possible." VIVEK KUNDRA, FEDERAL CLOUD COMPUTING STRATEGY 33 (2011). On December 9, 2010 the White House announced that "[e]ach [federal] agency will identify three 'must move' [IT] services within three months, and move one of those services to the cloud within 12 month[s] and the remaining two within 18 months." VIVEK KUNDRA, 25 POINT IMPLEMENTATION PLAN TO REFORM FEDERAL IT (2010), *available at* http://cio.gov/documents/25-Point-Implementation-Plan-to-Reform-Federal%20IT.pdf.

Transforming the federal government's IT infrastructure at such an accelerated pace holds promise for the future. The main concern, however, rests in ensuring that government attorneys and agencies integrate these changes into their litigation planning. The challenges for litigators confronted with either a client agency or organization using cloud computing for data storage are best addressed by developing E-Discovery strategies at the earliest stages of the case. Agencies should also plan ahead by proactively incorporating litigation and discovery needs into their agreements with cloud providers. By embracing and adjusting to these changes, agencies will have the proper tools and procedures in place and thus be better prepared to aid litigators when litigation arises.

As part of the effort to "jump start" agency adoption of cloud computing, the Office of Management and Budget (OMB) will continue to exercise an important role in this transformation. When OMB evaluates funding and options for new IT deployments, it "will require that agencies default to cloud-based solutions, whenever a secure, reliable, cost-effective option exists." *OMB Announces "cloud first" policy for agencies*, FEDERAL CLOUD BLOG (Nov. 23, 2010), http://fedcloud.wordpress.com/tag/omb/. In November, OMB promulgated a policy that is triggering the movement of additional government entities into the cloud. The policy stated that starting with the 2012 budget process, agencies would be required to consider using cloud computing options first when formulating their budgets. *See* Office of Management and Budget, www.whitehouse.gov/blog/2010/11/19/driving-it-reform-update. Consequently, both agency data and documents needed by Department of Justice attorneys for litigation and discovery are moving to the cloud.

Several agencies have already started this migration. For example, the United States Department of Agriculture (USDA) announced that it would move to a Microsoft cloud for email, web conferencing, document collaboration, and instant messaging. Press Release, USDA, USDA Moves to Microsoft Cloud (Dec. 8, 2010). USDA stated that in implementing the plan it would consolidate 120,000 users who were spread across 21 email systems. *Id.* Other agencies that embrace the cloud are the GSA, the Department of Treasury, the Securities and Exchange Commission, and the Department of Veterans Affairs. *See generally* FEDERAL CLOUD COMPUTING CASE STUDIES, http://info.apps.gov/content/federal-cloud-computing-case-studies (profiling several projects from agencies as varied as the U.S. Forest Service to the Federal Labor Relations Authority).

The movement to the cloud, however, is not unique to the government. Cloud migrations are also expanding at private companies, many of which the government investigates and litigates against. Among the largest group of early adopters for cloud services are financial services and manufacturing industries. *See* Gartner Says Worldwide Cloud Services Market to Surpass $68 Billion in 2010, http://www.gartner.com/it/page.jsp?id=1389313. Companies such as Genentech and Virgin Atlantic have publically disclosed their utilization of cloud computing for certain business functions. Moreover, an extensive survey of company CIOs revealed that cloud computing was their top priority. *See* Gartner Executive Programs Worldwide Survey of More Than 2,000 CIOs Identifies Cloud Computing as Top Technology Priority for CIOs in 2011, http://www.gartner.com/it/page.jsp?id=1526414. As a result, the data and potential evidence needed from these companies may now be in the cloud.

By its very nature, the information found in the cloud is electronic. Consequently, discovery in the cloud will require litigators and courts to rely on E-Discovery law, strategies, and processes. E-Discovery entails the identification, preservation, collection, review, production, and presentation of documents and data originally found in electronic form, and/or documents originally found in hard copy but converted to electronic form for review and production. While E-Discovery has evolved with changes in both the law and technology, the cloud still presents new complications.

IV. E-Discovery challenges and opportunities in the cloud

One challenge presented by cloud computing rests in the discovery issues that have yet to be addressed by the courts. The courts have not resolved how the very nature of cloud computing may complicate the preservation, collection, or production of data stored in the cloud.

Another challenge involves cloud providers. Providers constantly move the data in the cloud to different geographic locations to take advantage of savings found, for example, when data is moved to a different server location because the new location has less network traffic during certain times of day. The ability to preserve data may be complicated by the constant movement of information in the cloud. Further, the data to be preserved and collected is physically with a third-party and may not easily be in the agency's or the company's reach. Collecting data and its associated metadata from the cloud may be challenging because many cloud providers may not provide access to the original metadata.

In the civil context, at the very start of a case or when litigation is reasonably anticipated, a litigation hold must be issued to prevent the spoliation of potential evidence. *See, e.g.*, *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212 (S.D.N.Y. 2003). In the criminal context, the triggers for preservation may be different but organizations will have certain preservation obligations. These obligations may be statutory. The Sarbanes-Oxley Act of 2002, 18 U.S.C. § 1519 (2002) provides, for example, that

> [w]hoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction . . . of the United States . . . or in relation to or contemplation of any such matter . . . shall be fined . . . [or] imprisoned not more than 20 years, or both.

Id. It remains unclear how courts will interpret and litigators will implement these preservation requirements given how cloud providers store and move data. It is also unclear how the collection and production of data from the cloud will affect the development of law regarding the production of metadata in response to discovery requests in litigation. *See, e.g.*, *Aguilar v. Immigration and Customs Enforcement Div. of the U.S. Dep't of Homeland Security*, 255 F.R.D. 350 (S.D.N.Y. 2008) (observing the relationship between a document and its metadata for production); *Williams v. Sprint/United Mgmt.*

Co., 230 F.R.D. 640, 652 (D. Kan. 2005) (explaining that metadata is an inherent part of an electronic document). Depending on the system configuration and cloud services, the original metadata for data stored in the cloud may no longer technically exist. A further discussion of the practical effect that cloud computing has on a litigator's practice continues below.

V. Potential opportunities for litigators in the cloud

In the search for evidence, several potential benefits are available for litigators if a client agency or investigation target uses cloud computing to store their information. First, email and data in the cloud will be centrally located as opposed to dispersed across different systems, programs, organizational divisions, and physical locations. As a result, subpoenas, civil investigative demands, or document requests seeking information from these centralized systems should yield faster responses. Collecting email, for example, will start at a centralized entry point instead of beginning with an exhaustive search through multiple, isolated systems.

Second, but not wholly unrelated to the first, data stored in the cloud should lend itself to faster and easier electronic searches. Instead of an agency searching each sub-agency email system separately, it will be able to perform one top level search over all agency email. The email software would also be consistent organization-wide, rather than one department using Microsoft Outlook, one using GroupWise, and another potentially using Lotus Notes. Further, if the cloud systems are originally configured with E-Discovery in mind, the cloud technology may have built-in search capabilities. Consequently, the amount of time and effort saved searching for evidence could be substantial. The litigator may want to inquire about the search functionality of the system in advance of issuing discovery or an inquiry so that search requests can be more effective.

A third potential advantage for litigators is that the data will be held by a third-party, the cloud provider. In some circumstances the investigator or requestor may be able to obtain that data without notice to the data owner. *See* Stored Communication Act, 18 USC §§ 2701-2708 (2010). *But see United States v. Warshak*, No. 08-3997, 2010 WL 5071766, at *14 (6th Cir. Dec. 14, 2010) (holding that "a subscriber enjoys a reasonable expectation of privacy in the contents of his emails 'that are stored with, or sent or received through, a commercial ISP.'").

Fourth, a user may have less ability to actually destroy or alter evidence because the data now sits with a third-party. Cloud providers may establish processes that control what and how a person may, for example, delete a document. The cloud provider's disaster recovery and back up procedures may prevent a culpably-minded person from permanently destroying electronic evidence in the cloud. The cloud provider's procedures may aid a litigator in capturing and locating potential evidence that might have otherwise been lost if the data solely resided with the user or an interested party.

Finally, more data, and therefore more evidence, may be accessible to litigators. In addition to the move towards information remaining actively and more easily accessible online, as opposed to being removed and placed on a disaster recovery system such as back up tapes, cloud computing may feed into users natural tendencies to store more than necessary. The cost to store data in the cloud will continue to decrease; therefore, the motivation to only create and store what is absolutely needed will also decrease. Consequently, more information may be generated and retained, depending on the existence and compliance with an organization's records management policies.

VI. Potential disadvantages of cloud data storage for litigators

The many benefits of cloud data storage are nonetheless accompanied by potential disadvantages for litigators. First, an organization using cloud computing for storage may not have the knowledge or ability to implement a hold on data that may be potential evidence. If document retention needs were not addressed by an organization when developing their terms and requirements with the cloud provider, their attempts to preserve information may be undermined by the cloud provider's normal data recycling processes and procedures, despite potential good faith efforts by the users. The cloud providers may not be able to suspend their own procedures because such suspension may affect other unrelated users. The evidence may be gone before the litigator even knows it existed unless the user takes proactive preservation steps to avoid loss of important data or evidence.

Second, debate over what information the agency or organization has custody or control over may substantially increase. This debate may be both factual and legal. In the past, an organization's email, for example, was found on the organization's computers, network, and servers because the organization owned and controlled the physical location of the information. With the rise of cloud computing and with the data being stored by a third-party's system, more debate as to whether the data is within the control of the company may naturally arise.

Case law suggests, however, that courts may find the data in the control of the company even if it is found with a third-party. In *Flagg v. City of Detroit*, 252 F.R.D. 346 (E.D. Mich. 2008), the court held that the Stored Communications Act did not preclude discovery of a city's relevant, non-privileged electronically stored communications that were maintained by a non-party service provider but remained within the city's control. The court evaluated whether control existed under FED. R. CIV. P. 34(a), which states that a party may request disclosure by another party of information that the responding party has within its "control." *Id.* at 358-66. The court concluded that control under FED. R. CIV. P. 34(a) existed because the city had a contract with the service provider. It based its reasoning in large part on the fact that the city could permit disclosure by granting consent because it could "block" disclosure by withholding consent. *Id.* at 355.

The extent of control under FED. R. CIV. P. 34 by a person or entity may depend on other statutes. For example, in *Tomlinson v. El Paso Corp.*, 245 F.R.D. 474 (D. Colo. 2007), pension plan participants sued their employer under the Employee Retirement Income Security Act (ERISA) and moved to compel the production of electronically stored information (ESI). *Id.* at 476. The ESI was stored with a third-party that refused to produce part of the ESI, arguing that part of it was proprietary. *Id.* at 475. The court examined the concept of control under FRCP 26(a)(1)(B) and compelled production under FRCP 34(a), stating that "Rule 34(a) enables a party seeking discovery to require production of documents beyond the actual possession of the opposing party if such party has retained any right or ability to influence the person in whose possession the documents lie." *Id.* at 476-77. The court reasoned that because a duty arose under ERISA to maintain records, the employer was in possession of the documents and may not "delegate [its] duties to a third-party under ERISA." *Id.* at 477.

Even without a statute, courts will likely construe the concept of control broadly. In *Goodman v. Praxair Services, Inc.*, 632 F. Supp. 2d 494 (D. Md. 2009), the court stated that "Rule 34 'control' would not require a party to have legal ownership or actual physical possession of any documents at issue." *Id.* at 515. Instead, documents are considered to be under a party's control when that party has "the right, authority, or practical ability to obtain the documents from a non-party to the action." *Id.* (quoting *In re NTL, Inc. Sec. Litig.*, 244 F.R.D. 179, 195 (S.D.N.Y. 2007) (a securities litigation case where the district court found that successor entities still had "control" over ESI arising from a cooperative file-sharing system)).

While some may argue that the data remains within the organization's control when the data is in the cloud, legitimate factual arguments may exist suggesting that the evidence sought is not actually in the organization's control. The outcome may depend on how the services are arranged with the third-party. For example, Twitter allows users to retrieve only up to 3,200 of their last tweets. Twitter retains all tweets sent by a user in its archived system but the user only has access to the last 3,200 messages. *See* TWITTER HELP CENTER, http://support.twitter.com/entries/13920-frequently-asked-questions. Therefore, organizations may not be physically able to reach the evidence even if it exists in the possession of a third-party.

Third, if the data in the cloud is difficult to manage or retrieve for litigation purposes, courts may be disinclined to sympathize with discovery difficulties. Courts may view cloud computing as a normal business function where the data cannot be made inaccessible when the organization should have known of potential E-Discovery needs when incorporating cloud computing into their systems. In *Radian Asset Assurance, Inc. v. Coll. of the Christian Bros. of N.M.*, No. CIV 09-0885 JB/DJS, 2010 WL 4928866 (D.N.M. 2010), Plaintiff, Radian Asset, sought production of ESI from the Defendant College. The college had sold its assets, including ESI on backup tapes, to a third-party. College subpoenaed the third-party to produce the ESI. The third-party proceeded to produce, but Radian Asset argued that the format of the ESI was not the same format as the "usual course of business" under FRCP 34(b)(2)(E). *Id.* at *1-2. The district court disagreed and found that it was common for businesses to transfer ESI to backup tapes. The district court stated that:

> Businesses commonly store data in increasingly less accessible formats as the data loses currency, and the data is retained primarily for archival purposes. It is common to move data from on-line storage, where it is quickly accessible through networks, to near-line storage robotic storage devices - where data can be retrieved after a short delay, and eventually to offline or archival storage, such as tape backups.

Id. Courts may not be receptive to hearing from organizations whose data has, in the normal course of business, been sent to the cloud but is not easily accessible.

Finally, although access to a large amount of information may be beneficial, the volume of data may actually be a hindrance depending on which side of the request the litigator is on. When defending an agency that has moved its data to the cloud, the potentially voluminous data must still be reviewed and produced in some way in response to a discovery request. The more data a cloud stores, the more work to determine relevancy and privilege. One terabyte of data can cost less than $100 to store but more than $1 million in litigation costs to collect, processes, review, and produce. A caveat to this concern is that with advances in technology, smarter automated tools will be able to help alleviate this problem by increasing efficiency when reviewing large volumes of information in the cloud. The potential help these tools provide becomes available if one has access to these resources. The investment in and access to litigation technology in handling the data in discovery may, however, very well lag behind the rise in storing data in the cloud.

The challenges that litigators face with either a client agency or organization using cloud computing for data storage are best addressed by taking a proactive position on this new movement and developing E-Discovery strategies at the earliest stages of the case.

VII. Suggestions for the twenty-first century litigator facing the cloud

In this changing world, litigators must learn how to adapt. Given these cloud computing challenges and opportunities, several practical steps are available for litigators to take in adjusting to these changes. First, attorneys need to work closely with IT and technical staff to understand what is stored in the cloud, what the terms of that storage agreement are, and the options for retrieving that data. To learn about where the evidence is, the litigator may have to issue a document request or subpoena for the cloud terms and data policies or, in the civil context, seek a Fed. R. Civ. P. 30(b)(6) deposition of the relevant IT personnel.

Second, attorneys may want to notify the organization to preserve the potentially relevant information in the cloud at the very outset of the case. Litigation holds should not be overly broad, but rather should be accurate in scope and related to the inquiry. As discussed, the challenge with data in the control of a third-party is that it may not be retained or easily retained after time has elapsed. By notifying the client agency, for example, of the need to preserve the relevant data in the cloud, the agency will activate the preservation steps they hopefully negotiated with the cloud provider in the contract, before normal data management procedures delete the information. In contrast, in investigations and affirmative litigation, if a litigator notifies the target organization up front that any relevant data in the cloud must be preserved–depending on the strategy for providing notice of the ongoing investigation–then the organization risks potentially serious ramifications, such as an obstruction of justice charge, if the data is destroyed.

Third, the best way to deal with many of the challenges caused by cloud computing is to reach an early understanding with opposing counsel. Litigators should negotiate the scope of discovery to reflect what is needed because the volume of potential data in the cloud may be large. Consequently, the need to process and review that data may threaten to slow the investigation or litigation. In the defensive context, the attorney will want up front and early limitations on discovery, potentially limiting the searches by custodian, time frame, location, or topic, so that preservation, search, and collection can be done by the agency in a more streamlined and cost-efficient manner. In the civil context, the concept of discovery effort being proportional to the case is becoming a more acceptable argument used to limit the scope of discovery. *See e.g.*, Sedona Conference®, Commentary on Proportionality in Electronic Discovery, October 6, 2010. *But see Orbit One Communications, Inc. v. Numerex Corp.*, No. 08 Civ. 0905 (LAK) (JCF), 2010 WL 4615547 (S.D.N.Y. Oct. 26, 2010). In the affirmative context, the litigator needs to understand the proper scope for their request so that they are not buried in irrelevant or unusable data.

Fourth, litigators should be prepared for arguments regarding the burden and cost of discovering data from the cloud and be prepared to educate the court and opposing counsel. Litigators, both requesters and responders to discovery, must educate themselves on the technology employed at their client agency or target or the litigator risks missing valuable opportunities and evidence. A partnership between the litigator and their litigation technology or IT resources is essential for litigators to make persuasive and accurate arguments.

Finally, a litigator may consider being more involved in the early stages of discovery by engaging in reviews of sample sets of data or search results. This will help to determine early on if the discovery strategy is accurately capturing and producing the evidence requested from the cloud.

VIII. Conclusion

In the twenty-first century, electronic evidence is rapidly moving to the cloud as companies, local governments, and federal agencies embrace cloud computing. As a result, potential evidence is being stored with third-parties in virtual warehouses. Those who litigate against or on behalf of organizations using cloud computing should adapt their discovery strategies and leverage the technological advances to their advantage when confronted with this new technology. In the final analysis, the question remains the same: Where is the evidence?❖

ABOUT THE AUTHORS

❑**Allison C. Stanton** is the Director of E-Discovery for the Civil Division of the U.S. Department of Justice. Among her responsibilities, Ms. Stanton develops E-Discovery policies, practices, and training for the Civil Division, works with the other Department Divisions on E-Discovery initiatives, advises federal agencies on E-Discovery matters, and provides guidance on proposed changes to procedural rules, regulations, and legislation affecting E-Discovery. Ms. Stanton is also the Chair of the D.C. Bar E-Discovery Committee. She is an established author and has spoken at national and international E-Discovery conferences.

❑**Andrew J. Victor** joined the Department of Justice in 2010 through the Honors Program as a Trial Attorney with the FTCA Staff of the Torts Branch. He handles a range of FTCA litigation matters and is an E-Discovery Coordinator for his office.✠

Applying "Proportionality" Principles in Electronic Discovery – Lessons for Federal Agencies and Their Litigators

Theodore C. Hirt
Attorney
Office of Immigration Litigation
Civil Division

I. Introduction

One of the challenges of E-Discovery is how to balance a party's need for information that will assist it in establishing its claims or defenses in its case with the burden and expense of obtaining and using that information. For Department of Justice attorneys who litigate on behalf of the federal government and its agencies, this challenge takes on additional significance. Department attorneys often litigate significant, "high stakes" cases. Agencies also face increasing demands on their resources and, in some cases, the agencies may confront reductions in their program and operating budgets. Litigation costs, including the substantial costs that can be required to identify, preserve, collect, review, and produce electronically stored information (ESI), also can result in a substantial diversion of agency resources away from the agency's programs or its mission.

The Federal Rules of Civil Procedure recognize that discovery must be "proportional" to the needs of the case, which may include the amount in controversy and the legal rights or obligations to be adjudicated. Rule 1 expressly states that the Rules are to be "construed and administered to secure the just, speedy, and inexpensive determination of every action and proceeding." FED. R. CIV. P. 1. When, however, parties request ESI in civil discovery, it may become particularly difficult to balance and achieve the three goals of Rule 1. Applying "proportionality" principles in discovery may help litigants, including the federal government and its agencies, achieve that balance.

This article first describes the principal rules that apply to ESI issues and how they incorporate proportionality principles. Next, the article reviews a recent commentary by The Sedona Conference® that advocates the application of proportionality to the discovery of ESI and discusses several cases in which district courts have applied proportionality principles to E-Discovery disputes. Finally, some recommendations on how Department attorneys can incorporate proportionality principles in their cases are provided. As this article notes, proportionality principles may also be applied, in some situations, even before the litigation is filed.

II. Proportionality in the Civil Rules, including Civil Rule 26(b)(2)(B)

The Civil Rules have been interpreted and applied to permit broad-ranging discovery. Rule 26(b)(1) provides that "[r]elevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence." FED. R. CIV. P. 26(b)(1). Over

time, however, the Rules have been amended to restrict discovery. For example, until 2000, Rule 26(b)(1) provided, in pertinent part, that unless otherwise limited by a court order, the parties could obtain discovery relevant to the "subject matter" of the case. *See* FED. R. CIV. P. 26 advisory committee's note (2000). In 2000, the rule was amended to state that the parties "may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense, and that, for 'good cause,' the court also may order discovery of any matter relevant to the subject matter of the action." *See* FED. R. CIV. P. 26(b)(1). This rule, therefore, now embodies a distinction between party-initiated discovery that is limited to a party's "claim or defense" and court-ordered discovery that can extend more broadly to "any matter" relevant to the subject matter involved in the case. *See* FED. R. CIV. P. 26 advisory committee's note (2000). In addition, the Rules have been amended to impose quantitative limits on the number and length of depositions and the number of interrogatories that can be propounded in a case. *See* FED. R. CIV. P. 30(a)(2)(A)(i), (d)(1); 31(a)(2)(A)(i); 33(a)(1).

Rule 26(b)(1) provides that "[a]ll discovery is subject to the limitations" of Rule 26(b)(2)(C). FED. R. CIV. P. 26(b)(1). That provision authorizes the court, either on motion or *sua sponte*, to limit the frequency or extent of discovery if it makes certain determinations:

> (i) the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive; (ii) the party seeking discovery has had ample opportunity to obtain the information by discovery in the action; or (iii) the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues.

FED. R. CIV. P. 26(b)(2)(C)(i)-(iii).

The December 2006 Rules amendments specifically incorporated discovery of ESI into the discovery rules. One of the most prominent amendments is the creation of the so-called "two tier" system for the discovery of ESI under Rule 26(b)(2)(B). This rule provides that "[a] party need not provide discovery" of ESI "from sources that the party identifies as not reasonably accessible because of undue burden or cost." *See* FED. R. CIV. P. 26(b)(2)(B). The rule next states that if the requesting party can establish "good cause" for the production of that ESI, a court may order its production and impose conditions on that production. *Id.* The Civil Rules Advisory Committee that crafted this rule explained that "some sources of electronically stored information can be accessed only with substantial burden and cost [and that] these burdens and costs may make the information on such sources not reasonably accessible." *See* FED. R. CIV. P. 26 advisory committee's note (2006). The rule thus differentiates between first-tier and second-tier sources of ESI. The specifics of this rule were reviewed more comprehensively in a previous issue of the United States Attorneys' Bulletin. *See* Theodore C. Hirt, *The "Two Tier" Discovery Provision of New Rule 26(b)(2)(B) - How Can Federal Agencies Benefit By Using this Rule?*, 56 UNITED STATES ATTORNEYS' BULLETIN 45 (2008) (discussing the benefit of Federal Rule of Civil Procedure 26(b)(2)(B)).

Rule 26(b)(2)(B) recognizes that proportionality should apply to the discovery of ESI because it expressly differentiates between ESI sources that are "reasonably accessible" from ESI sources that are not "reasonably accessible." FED. R. CIV. P. 26(b)(2)(B). For example, if a federal agency can establish that one or more of its ESI sources only can be accessed by the agency's expenditure of substantial costs, the requesting party may not be entitled to that discovery unless it can establish "good cause" for the agency to make that expenditure. When the court evaluates the party's request, it takes into account the

limitations of Rule 26(b)(2)(C) that include an assessment of whether "the burden or expense of the proposed discovery outweighs its likely benefit." *See* FED. R. CIV. P. 26(b)(2)(C)(iii).

Accordingly, when ESI sources are at issue in discovery, a key inquiry is whether those sources are reasonably accessible. If the sources are not reasonably accessible, proportionality principles must be applied. As the Committee Note explains, Rule 26(b)(2)(C) balances the costs and potential benefits of discovery, and whether a court will require a responding party to search and produce information that is not reasonably accessible "depends not only on the burdens and costs of doing so, but also on whether those burdens and costs can be justified in the circumstances of the case." *See* FED. R. CIV. P. 26 advisory committee's note (2006). The Committee Note also identifies the following as appropriate factors to consider:

> (1) the specificity of the discovery request; (2) the quantity of information available from other and more easily accessed sources; (3) the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources; (4) the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources; (5) predictions as to the importance and usefulness of the further information; (6) the importance of the issues at stake in the litigation; and (7) the parties' resources.

Id. Department attorneys will want to keep these considerations in mind when they approach discovery issues.

The Civil Rules also incorporate "proportionality" principles in the context of the parties' Rule 26(f) duty to "meet and confer" concerning their discovery plans. *See* FED. R. CIV. P. 26(f). The court's scheduling order may incorporate the parties' agreements on those issues. *See* FED. R. CIV. P. 16(b). Rule 26(f) provides that the parties must discuss "any issues about disclosure or discovery of electronically stored information." *See* FED. R. CIV. P. 26(f)(3)(c). The Committee Note explains that the parties may identify "the various sources of information within a party's control that should be searched for electronically stored information." *See* FED. R. CIV. P. 26 advisory committee's note (2006). With specific reference to Rule 26(b)(2)(B), the note explains that the parties should discuss "whether the information is reasonably accessible to the party that has it, including the burden or cost of retrieving and reviewing the information." *Id.*

III. The Sedona Conference® Commentary on Proportionality in Electronic Discovery and recent court decisions applying proportionality principles

In October, 2010, The Sedona Conference®, a well-respected, nonprofit legal research and policy organization, issued *The Sedona Conference® Commentary on Proportionality in Electronic Discovery*. *See The Sedona Conference® Commentary on Proportionality in Electronic Discovery*, 11 SEDONA CONF. J. 289 (2010). The *Commentary* addresses proportionality issues in considerable detail. *Id.* The centerpiece of the *Commentary* is *The Sedona Conference® Principles of Proportionality* (the *Principles*), an articulation of six principles to guide courts and practitioners in applying proportionality to civil litigation. These principles provide that: (1) The burdens and costs of preservation of potentially relevant information should be weighed against the potential value and uniqueness of the information when determining the appropriate scope of preservation, (2) Discovery should generally be obtained from the most convenient, least burdensome, and least expensive sources, (3) Undue burden, expense, or delay resulting from a party's action or inaction should be weighed against that party, (4) Extrinsic information and sampling may assist in the analysis of whether requested discovery is sufficiently important to warrant the potential burden or expense of its production, (5) Nonmonetary factors should be considered

when evaluating the burdens and benefits of discovery, and (6) Technologies to reduce cost and burden should be considered in the proportionality analysis. *See* 11 SEDONA CONF. J. at 291.

The *Principles* are intended to provide "a framework for the application of proportionality to all aspects of electronic discovery." *See id.* at 292. The *Principles* acknowledge that the 2006 Rules amendments were intended to give the courts a greater ability to address the "tremendous increase" in the amount of potentially relevant ESI by applying proportionality principles to discovery, but recognize that the courts have not always applied those principles in appropriate cases. *Id.* at 293. The *Principles* emphasize that "[i]n the electronic age, it has become increasingly important for courts *and* parties to apply the proportionality doctrine to manage the large volume of ESI and associated expenses now typical in litigation." *Id.*

A number of courts have endorsed the applicability of proportionality principles to E-Discovery, and it can be expected that some judges will cite the *Principles* in their resolution of future E-Discovery disputes. One magistrate judge recently cited the *Principles* in addressing the defendants' motion to stay discovery pending the resolution of their motion to dismiss the plaintiffs' complaint. *Tamburo v. Dworkin*, 2010 WL 4867346 (N.D. Ill. Nov. 17, 2010). In granting that motion in part, the court emphasized that the Rule 26 "proportionality test" authorized the court to limit discovery if it determined that the burden of the discovery outweighed its benefit. The court also cited the *Principles*, interpreting Rule 26(b)(2)(C)(iii) as providing the court with flexibility and discretion to limit discovery "to ensure that the scope and duration of discovery is reasonably proportional to the value of the requested information, the needs of the case, and the parties' resources." *Id.* at *3. The court ordered a phased discovery schedule, under which the parties were limited to written discovery, and also ordered the parties to conduct an "in person meet and confer" to prepare a phased discovery schedule, and to "actively engage in cooperative discussions to facilitate a logical discovery flow." *Id.* The court also directed the parties to "focus their efforts" on completing their Rule 26(a)(1) initial disclosure requirements before proceeding with other discovery. *Id.* Finally, the court stated that the parties "should prioritize their efforts on discovery that is less expensive and burdensome." *Id.*

Proportionality principles also have been applied in cases involving government agencies. For example, one magistrate judge applied the seven considerations (or factors) described in the 2006 Committee Note to Rule 26(b) in the context of the plaintiffs' request that a state agency search approximately 2,500 computer backup tapes for emails. *Major Tours, Inc. v. Colorel*, 2009 WL 3446761 (D.N.J. Oct. 20, 2009), *objections overruled*, 720 F. Supp. 2d 587, 620 (D.N.J. 2010). After determining that defendants established that the requested discovery was not reasonably accessible, the court concluded that a "substantial amount" of the relevant information was available to plaintiffs from a number of more easily accessed sources and that the information was "likely cumulative" of other relevant evidence already produced. *Major Tours*, 2009 WL 3446761, at *3-4. The court acknowledged that the sixth factor – the importance of the issues at stake in the litigation – favored plaintiffs, but it also concluded that the final factor – the parties' resources – favored the defendants. *Id.* at *4. The court remarked that the defendants already have spent "hundreds of thousands of dollars in time and money" on the defense of the case and that "[n]o party, including the State, has an unlimited litigation budget to pay for document production efforts that in all likelihood are of marginal benefit." *Id.* The court did order that, if plaintiffs and defendants could agree on the search of a much smaller number of backup tapes, the search would be conducted under a cost-sharing agreement. *Id.* at *6.

Finally, in a recent case against a local school district, the district court applied Rule 26(b)(2) in denying the plaintiffs' demand for the restoration and production of the school district's backup tapes for its email system. *Young v. Pleasant Valley Sch. Dist.*, 2008 WL 2857912 (M.D. Pa. July 21, 2008). The

court explained that the school district had demonstrated that it would be costly to rebuild a discontinued server. The court observed that, although it was skeptical of the district's cost estimate, it recognized that the $5,000 expenditure would be a significant one. *Id.* at *2. It also noted that the "resources of the parties involved and the amount in controversy in this case are relatively small," noting that the dispute did not involve a large corporation "that could produce the material in question using a minuscule fraction of its budget." *Id.* The court concluded that the information sought from the emails, while relevant, likely could be obtained from more accessible sources. *Id.*

These cases show that district courts have applied Rule 26(b)(2) and proportionality principles to reduce the costs and burdens of E-Discovery. The decisions reflect the individual judges' careful efforts to review the parties' contentions and, more importantly, the parties' documentation concerning both the relevance of the information requested and the costs and burdens of retrieving the information for possible production. The cases also show that a court's ability to apply proportionality to discovery demands is dependent on the clarity of the parties' submissions and the court's ability to weigh the alleged importance of the discovery against the other relevant factors of Rule 26(b). Whether a proportionality argument will be as successful in the context of a federal agency, as opposed to a state or local agency, is an open question. That uncertainty, however, should not deter a Department attorney from raising this issue in an appropriate case. *See McPeek v. Ashcroft*, 202 F.R.D. 31, 34 (D.D.C. 2001).

As discussed in the next section, Department attorneys can also apply proportionality principles in their resolution of E-Discovery disputes. If they are able to do so, their efforts could result in lower discovery costs as well as the saving of time and effort in their cases. Moreover, to the extent the attorneys can allocate proportionate efforts to discovery, their time can be devoted more intensively, and more effectively, to addressing the merits of the dispute and obtaining a favorable outcome for the government and the broader public interest.

IV. How proportionality can be applied in civil litigation involving the federal government

Whether the Department attorney is bringing an affirmative case on behalf of the United States or one of its agencies, or is defending government agencies or officials in a suit brought by another party, the effective management of discovery will be critical to a just and successful resolution of the case. During the discovery phase of the litigation, the Department attorney has the opportunity, as well as the responsibility, to conduct discovery in a reasonable, cost-effective manner and to expect that opposing counsel will do the same.

The challenge is determining what discovery is appropriate and then to ensure that both parties conduct discovery that is proportionate to the case. Optimally, both sides will recognize their shared interest in resolving discovery issues without the involvement of the court or motions practice. Realistically, however, this mutual understanding does not always occur. If the parties reach an impasse as to the scope of discovery, the Department attorney will need to develop a strategy that will protect the agency against disproportionate discovery. In addition, to the extent that the Department attorney needs discovery from the other party to support the government's claims or defenses, the Department attorney will want to ensure that the party will be responsive to the government's information needs.

The Department attorney must first determine if any discovery is even appropriate in the case. For example, in actions where an agency decision is based on an administrative record, extrinsic evidence, including evidence obtained from discovery is – subject to some narrow exceptions – not appropriate. *See, e.g.*, *Little Co. of Mary Hosp. v. Sebelius*, 587 F.3d 849, 856 (7th Cir. 2009); *Rempfer v. Sharfstein*, 583 F.3d 860, 865 (D.C. Cir. 2009); *Nat'l Audubon Soc'y v. U.S. Forest Serv.*, 46 F.3d 1437,

1447 (9th Cir. 1993). Other types of litigation may exist where discovery should not proceed at all. For example, Rule 26(a)(1)(B) exempts from the duty of "initial disclosure," *inter alia*, actions by the United States to recover benefit payments and actions by the United States to collect on a student loan guaranteed by the United States. *See* FED. R. CIV. P. 26(a)(1)(B). Actions in which purely legal issues are raised may also be resolved without the need for any discovery. Moreover, in defensive litigation the Department attorney should also consider whether a jurisdictional defense is appropriate as a response to the complaint and, therefore, whether a motion to dismiss can be filed in lieu of an answer. The Department attorney can seek to stay discovery if that becomes an issue.

If, however, discovery may be appropriate in the case, the Department attorney must determine how he can develop a discovery plan that will yield information relevant to the claim or defense, but that will not result in a disproportionate expenditure of time or resources. The Department attorney also will want to ensure, to the extent possible, that the opposing party's discovery requests are proportional and that the government agency (or agencies) who will respond to that discovery are not burdened with excessive discovery requests.

As explained below, there are many opportunities to apply proportionality principles to the discovery that may be conducted in cases brought by or against the government. In fact, in some situations, proportionality may even be feasible to apply before litigation begins.

A. Pre-Litigation proportionality analysis

One of the most significant challenges for parties, including government agencies, is how to fulfil their obligation to preserve ESI that may be relevant to a dispute. In the context of civil discovery, the courts have imposed sanctions against parties or their counsel for violations of the common law duty to preserve relevant information when litigation has been filed, or when litigation is reasonably anticipated. *Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLP*, 685 F. Supp. 2d 456, 477-78 (S.D.N.Y. 2010); *Jones v. Bremen High Sch. Dist. 228*, 2010 WL 2106640, at *6-10 (N.D. Ill. May 25, 2010); *Doe v. Norwalk Cmty. Coll.*, 248 F.R.D. 372, 380-82 (D. Conn. 2007). Although Rule 37(e) states that, "[a]bsent exceptional circumstances," a court may not impose sanctions under the Rules on a party for its failure to provide ESI that has been lost "as a result of the routine, good-faith operation of an electronic information system," FED. R. CIV. P. 37(e), the rule interprets good-faith operation to require a party's intervention to "modify or suspend certain features of that routine operation to prevent the loss of information, if that information is subject to a preservation obligation." FED. R. CIV. P. 37 advisory committee's note (2006).

In some situations, proportionality issues can be addressed before the litigation begins. The Sedona Conference® *Principles* explain that "[t]he burdens and costs of preservation of potentially relevant information should be weighed against the potential value and uniqueness of the information when determining the appropriate scope of preservation." 11 SEDONA L. J. at 291. The *Principles* recognize that the Rules do not apply until litigation has begun, but observe that the courts have invoked their inherent authority to sanction parties for "pre-litigation preservation failures." *Id.* Acknowledging that no decisions exist that apply the Rules' proportionality factors to the pre-litigation context, the *Principles* recommend that "parties who demonstrate that they acted thoughtfully, reasonably, and in good faith in preserving or attempting to preserve information prior to litigation should generally be entitled to a presumption of adequate preservation." *Id.*

Several commentators also have concluded that a party reasonably anticipating litigation should be able to undertake what it reasonably believes to be proportional preservation activities, including the

decision not to preserve non-reasonably accessible information sources, and that the party may reasonably conclude that its preservation obligation should not exceed the value of the potential litigation. *See* The Honorable Paul W. Grimm, Michael D. Berman, Conor R. Crowley, & Leslie Wharton, *Proportionality in the Post-hoc Analysis of Pre-litigation Preservation Decisions,* 37 U. BALT. L. REV. 381, 405, 410 (2008). These authors express the concern that "litigants may feel compelled to expend enormous sums to preserve ESI that need not be preserved, [that] will never be produced in discovery, and that may greatly exceed the economic value of the claims presented." *Id.* at 384. They also point out that the uncertainty of what a party must preserve before litigation can lead to "coercive demands and settlements." *Id.* at 402.

One district judge observed, albeit in dictum, that "[w]hether preservation or discovery conduct is acceptable in a case depends on what is *reasonable*, and that in turn depends on whether what was done – or not done – was *proportional* to that case and consistent with clearly established applicable standards." *Rimkus Consulting Grp. v. Cammerata*, 688 F. Supp. 2d 598, 613 (S.D. Tex. 2010) (emphasis in original, citation omitted); *but see Orbit One Communications, Inc. v. Numerex Corp.*, 2010 WL 4615547, at *6 (S.D.N.Y. Nov. 17, 2010) (expressing concern that applying proportionality principles to preservation issues "may prove too amorphous to provide much comfort to a party deciding what files it may delete or backup tapes it may recycle").

What does this mean in a potential case involving the federal government? An agency may reasonably anticipate that litigation will be filed against it as a result of a dispute with a private party. Where, for example, the agency has terminated a contract with the private party, or has denied a grant or other benefit to that party, the party may have alerted the agency that it will file suit in a federal or state court. The private party may have submitted a demand letter that describes the nature of the case it will file if the dispute is not resolved. An agency may also have announced to a regulated industry or issued a formal notice to a company of the agency's intention to implement or enforce a rule or regulation, and the agency may have received a direct threat of litigation as a result of the announcement or notice. In those situations, the agency may have an opportunity to evaluate the scope of its potential preservation obligation and what efforts at preservation will be reasonable and sufficient.

The agency also may wish to contact the United States Attorney's Office or a litigating Division for advice or assistance in crafting a reasonable litigation hold. This contact may present an opportunity for the Department attorney and the agency to develop a litigation hold that is proportional to the anticipated litigation. For example, the agency and the Department attorney may conclude that the claim is worth $100,000. With that in mind, they can try to evaluate the anticipated costs of discovery, including preservation.

If the private party has notified the agency of its intention to file suit, the Department attorney can consider whether it will be helpful to contact the party's counsel and discuss preservation issues. In some situations, the Department attorney may determine that the other party may agree to limits on the preservation of ESI and, if so, that agreement can be memorialized as part of the parties' "meet and confer" process, discussed later in this article. *See infra* Part IV.C. In other situations, the Department attorney may conclude that the opposing party will not be reasonable with respect to preservation issues. In that situation, the Department attorney will consult with the agency and determine what kind of preservation is reasonable.

When there is communication about the parties' anticipated preservation efforts, the Department attorney has the opportunity to explain that the costs of preservation must be proportional to the amount at stake in the case and that the agency does not intend to expend its funds to preserve ESI sources that are not reasonably accessible or of little or no relevance to the claims or defenses in the case. This

opportunity may be particularly applicable in small stakes cases, particularly those in which the costs of preservation could be substantial. The Department attorney also may be able to argue that much of the information would be privileged or protected from discovery. If the agency, after consultation with the Department attorney, imposes what it concludes is a reasonable litigation hold, the Department should later be able to defend that hold against a motion for sanctions if the private party argues that the ESI it has requested in discovery was not preserved. The Department attorney can argue that the agency took reasonable preservation measures and that the agency was not required to preserve volumes of ESI of little or no relevance to the dispute. The Department attorney can later inform the court that the opposing party did not describe the alleged relevance of the ESI sources demanded or did not explain why they should be preserved.

Pre-litigation discussions about preservation merit serious consideration and may reduce discovery costs. At the same time, it is important to be realistic about the level of cooperation – or the opportunity to cooperate – that may occur at this incipient stage of the dispute process. A party's demand letter may provide too general a description of the legal claim to be of much value to the agency in identifying potentially relevant ESI sources. The letter may lack much factual detail or, if it contains some detail, the letter may be overly broad in its description of potentially relevant ESI sources.

For these reasons, before litigation is filed, an agency may face considerable uncertainty in evaluating or responding to a private party's preservation demands. That uncertainty, however, should not discourage the parties from exploring cost-effective efforts to define the scope of preservation and potential discovery in the litigation that is reasonably anticipated.

Finally, the agency may face the dilemma of whether and how to preserve potentially responsive ESI sources as the litigation proceeds and the burdens of preservation may extend not only to sources that the agency concludes are not reasonably accessible (like backup media) and active, but also to online ESI sources that may be of little relevance. The private party, however, may expect or demand that various ESI sources not be deleted or made less accessible while the litigation proceeds. On the other hand, the agency will have to bear what could be substantial costs if it preserves that information and the uncertainty of when it will be able to delete or destroy the information.

The Sedona Conference® *Principles* address the problem of the party's failure to preserve relevant accessible information. It explains that "[a] failure to preserve relevant information in an accessible format at the outset of litigation should be weighed against a party seeking to avoid the resultant burden of restoring the information," and cites cases holding that a party who fails to preserve that information may be required to produce it even though it is no longer in a readily accessible format. 11 SEDONA CONF. J. at 298. In addition, the Committee Note to Rule 26(b)(2)(B) explains that a party's identification of ESI sources as not reasonably accessible "does not relieve the party of its common-law or statutory duties to preserve evidence." *See* FED. R. CIV. P. 26 advisory committee's note (2006).

The Department attorney should raise these issues as soon as feasible in the case. The attorney should confer with the agency about the preservation costs associated with specific ESI sources and obtain an estimate that can be provided to opposing counsel and to the court.

B. The pleadings stage

In many cases, the Department attorney will learn of litigation against the United States or one of its agencies only after the complaint has been served on the agency and on the United States. The Department attorney will, of course, want to consult with the agency as soon as possible to determine whether a litigation hold is in place. If not, the Department attorney must then consult with the agency so

that a litigation hold is promptly imposed. If the agency already has a litigation hold in place as to the potentially relevant ESI, then the Department attorney and agency counsel can evaluate the reasonableness of that hold, including its scope; for example, the volume of ESI to be preserved, the number and size of the affected agency offices, and the number of key custodians involved in the preservation.

Even as the Department attorney is evaluating preservation issues, the attorney may be able to apply proportionality principles to the scope of preservation. Early communication with opposing counsel about the scope of the case may lead to some agreements as to the scope of the anticipated discovery. Informal exchanges of information about the parties' claims may be feasible in some situations.

At this early stage of the litigation, the parties may have little knowledge about what information will be relevant to the claims or defenses described in the pleadings. The complaint and answer may each state the relevant facts in only general terms. A lack of specificity will inevitably complicate the parties' understanding of the potential scope of E-Discovery.

C. The "meet and confer" process – issues to raise

The Rule 26(f) "meet and confer" process may be the most feasible opportunity for the parties to address proportionality issues. *See* FED. R. CIV. P. 26(f). In that setting, the parties can identify and, if practical, limit the legal and factual issues, including the scope of the discovery, in the litigation. As a result of one or more meet and confer sessions, counsel can provide the court with either their agreements on the scope of discovery or identify the issues upon which they disagree and need the court to resolve. Courts now expect the parties to cooperate in the discovery process in order to reduce discovery burdens and many judges have endorsed *The Sedona Conference® Cooperation Proclamation* urges that litigants adopt a cooperative approach to discovery and emphasizes cooperation as a means of achieving cost-effective discovery. *See The Sedona Conference® Cooperation Proclamation* (July 2008), accessible at www.thesedonaconference.org/contents/tsc_cooperation_proclamation.pdf.

In preparation for the meet and confer session with opposing counsel, the Department attorney should first become familiar with the agency's ESI sources and what kinds of ESI are maintained on them. Being conversant with those systems will make it easier for the Department attorney to determine whether some ESI sources are not reasonably accessible without the agency's expenditure of undue effort or cost. The Department of Justice attorney should work with agency counsel and agency program, information technology, and records management staff to secure an understanding of the agency's information systems. As a result of those consultations, the Department attorney will be able to explain the agency's ESI sources and their limitations to opposing counsel. In some cases, the Department attorney may be able to prepare an estimate concerning the amount in controversy so that the Department and the agency can evaluate what is at stake in the litigation and assess what discovery will be proportional to the case. *See Mancia v. Mayflower Textile Services. Co., Inc.*, 253 F.R.D. 354, 364 (D. Md. 2008) (directing the parties to attempt "to identify a foreseeable range of damages from zero if the [p]laintiffs do not prevail, to the largest award they could likely prove if they succeed," from which the court could estimate what was "at stake" in the case within the meaning of Rule 26(b)(2)'s proportionality analysis).

The Department attorney may also find it helpful to match the elements of the legal claim with the likely sources of information, whether in physical (hard copy) or ESI format, that are likely to yield the critical information that would support the elements of the plaintiff's claims. The Department attorney could also approach this issue from the agency's vantage point, identifying information sources

likely to support its defenses to those claims. It would also be useful to rank the sources of information as to the greatest possible relevance to the case and to rank those sources by level of accessibility.

In some cases, the parties may be able to compare their accessible ESI sources to the information that they intend to identify as their Rule 26(a)(1) "initial disclosures." *See* FED. R. CIV. P. 26(a)(1). Under that rule, the parties must identify, *inter alia*, "a description by category and location, of all documents, electronically stored information, and tangible things that the disclosing party has in its possession, custody, or control and may use to support its claims or defenses, unless the use would be solely for impeachment." In *Tamburo v. Dworkin*, 2010 WL 4867346 (N.D. Ill. Nov. 17, 2010), for example, the magistrate judge directed that the parties to fulfill their Rule 26(a)(1) obligations before engaging in formal discovery. *Id.* at *3. It is important to recognize, however, that an agency's initial disclosures necessarily may be quite general. Realistically speaking, at the beginning of the litigation, the agency may not have identified all of the ESI sources that potentially support its claim. Its description of ESI sources may be general in nature. If that is the case, then it may be difficult for the agency and the Department attorney to identify or evaluate what ESI sources will be "reasonably accessible" for discovery. That level of specificity will likely be more feasible only when the parties are identifying their formal discovery, including their anticipated Rule 34 requests. *See* FED. R. CIV. P. 34.

If, however, the parties can first identify for potential collection and production those sources of information, they will have accomplished two related objectives. First, the parties will have identified the evidence upon which they may rely to establish their respective claim or defense. Second, they will have agreed to make that information available for the other party's review or inspection.

An additional challenge in achieving proportionality in discovery is differentiating between the central claims or issues in the litigation and the claims or issues that are tangential or peripheral. One reasonable approach may be to determine, if only in a preliminary manner, whether specific counts of the complaint or counterclaim, or the answer's affirmative defenses, can be resolved without resort to discovery. If the parties can agree, they can propose a briefing schedule to the court for the resolution of discrete legal issues.

Similarly, to the extent the parties can identify the scope of the legal claims, *e.g.* how far back in time information will be relevant, and whether information sources in specific offices or locations can be excluded as not relevant to the claims or defenses, identification of the relevant information sources will be facilitated. *See, e.g.*, *Caldara v. N.J. Transit Rail Operations, Inc.*, 2010 WL 1912656, at *3 (D.N.J. May 7, 2010) (determining that the scope of deposition discovery was to be limited geographically and temporally); *Rosenbaum v. Becker & Poliakoff, P.A.*, 2010 WL 623699, at *9 (S.D. Fla. Feb. 23, 2010) (applying Rule 26(b)(2)(B) to impose temporal scope on E-Discovery requests); *Takacs v. Union County*, 2009 WL 3048471, at *3 (D.N.J. Sept. 23, 2009) (determining that plaintiffs' document discovery demands were not proportional to the needs of the case). If the parties are not able to agree, they at least should be able to agree that the court should decide the issue. Early judicial resolution of discrete legal or factual issues may result in efficiencies.

The parties should agree to investigate the feasibility of identifying and producing the most accessible ESI sources first during the discovery period. The parties also should agree that the least accessible information sources will be investigated, if at all, after all other ESI sources have been identified, collected, and produced. The Sedona Conference® *Principles* suggest that backup media will fit within this latter category. *See* 11 SEDONA CONF. J. at 297. Where, for example, a party can establish a factual contention from accessible information, no reason exists to require the other party to search files that are not reasonably accessible. *See BBVA Compass Ins. Agency, Inc. v. Olson*, 2010 WL 4004518, at

*2-3 (D. Colo. Oct. 12, 2010) (in denying additional search, court notes that requesting party had "ample evidence" to establish a fact).

"Phased" discovery is not necessarily going to achieve proportional discovery. Parties must exercise care in its planning and execution. For example, the parties should evaluate the information sources that will be identified, collected, and produced in the first phase of discovery. Their focus should be on the information most relevant to the claims or defenses. Although a party requesting discovery may be reluctant to assign an artificial priority to the relevance of some information categories, especially if that party knows little about the other party's information sources, some ranking is inevitable. In less complicated cases or in cases where the court has imposed a short time period for discovery, phased discovery also may be unrealistic and unnecessary.

D. Defining and narrowing the scope of discovery

The meet and confer process may result in the parties' agreement as to the nature and the scope of the discovery they will conduct in the case. Disputes over discovery, however, may be inevitable. If that is the case, the Department attorney will need to determine how best to involve the court in resolving the dispute. Given the substantial costs involved in the preservation and collection of ESI, it may be crucial to obtain a prompt court ruling that defines and delimits the scope of discovery for the case.

One of the innovative features of the December 2006 Rules amendments was the explicit recognition that parties requesting E-Discovery should focus their requests on information sources that are the most accessible, the most convenient, and the least expensive. The Sedona Conference® *Principle 2* also endorses this approach: "Discovery should generally be obtained from the most convenient, least burdensome, and least expensive sources." 11 SEDONA CONF. J. at 291, 296. The *Principle*s explain that the parties must limit their discovery when the requested material can be obtained from sources "more convenient, less burdensome, or less expensive" as specified in Rule 26(b)(2)(C)(i). *Id.* at 296. Its commentary explains that the "parties should carefully weigh these factors when determining which source is optimal." *Id.* at 297. When a court decides whether to limit what could be potentially burdensome or expensive discovery, it must be able to assure itself that the requested discovery will be sufficiently valuable to justify the expenditure of the parties' resources.

In resolving disputes under Rule 26(b)(2)(B), the party resisting production of the ESI has the burden to demonstrate that the sources are not reasonably accessible without undue burden or cost. A court will not accept uncorroborated assertions that discovery will be unduly burdensome or, for that matter, sweeping assertions that the discovery will yield highly-relevant or unique information supporting the party's claim. If, for example, an agency concludes that it will experience difficulties in accessing or producing ESI sources or asserts that the project will consume substantial agency resources, the agency will need to corroborate its contentions with affidavits or declarations from the agency information technology and/or records management staff. The affidavit or declaration will need to describe in specific detail the costs that would have to be incurred if the ESI sources are identified, collected, reviewed, and produced. If the affidavit or declaration lacks sufficient detail, the court will not accept the agency's contentions as the burden of the discovery. *See, e.g.*, *Federal Trade Comm'n v. Nationwide Connections, Inc.*, 2007 WL 246201, at *2 (S.D. Fla. Aug. 27, 2007) (holding that defendant's declarations as to allegedly burdensome discovery lacked sufficient detail).

Although it may be difficult in some cases for the parties to agree on what discovery is "sufficiently important" to justify the burden and expense of its production, the *Principles* urge that discovery "should be limited if the burden or expense of producing the requested information is disproportionate to its importance to the litigation." 11 SEDONA CONF. J. at 299. The *Principles*

acknowledge that a court may have difficulty in making that assessment, because it "may be impossible to review the content of the requested information until it is produced." *Id.* When confronted with potentially burdensome discovery, however, a court will try to assess whether the burden can be justified by the value of the requested information in supporting a party's case. *See United States ex rel. McBride v. Halliburton Co.*, 2011 WL 208301, at *7 (D.D.C. Jan. 24, 2011) (discovery in a qui tam action, the court explains that plaintiff-relator failed to show that emails not produced by defendant were "crucial" to her proof or "highly probative" of any relevant fact).

The *Principles* also emphasize that, at least in some cases, it will be clear that the requested evidence is important, or even outcome determinative. 11 SEDONA CONF. J. at 299. In such cases, the court may be able to determine that more extensive discovery will be necessary. The court, however, will need the parties' input in order to evaluate the nature or scope of that discovery. The *Principles* recommend that "[e]xtrinsic information and sampling may assist in the analysis of whether requested discovery is sufficiently important to warrant the potential burden or expense of its production." 11 SEDONA CONF. J. at 291, 299. The *Principles* emphasize that the parties and the court should take advantage of available technology in their efforts. *Principle 6* expressly states that "[t]echnologies to reduce cost and burden should be considered in the proportionality analysis." *Id.* at 291, 301. In cases involving a potentially large universe of ESI, the use of search terms agreed to by the parties may be able to narrow the scope of the discovery. *See Federal Trade Comm'n v. Church & Dwight Co., Inc.*, 2010 WL 4283998, at *4 (D.D.C. Oct. 29, 2010) (magistrate judge cites *Principle 6* in recommending that the parties consider the use of agreed search terms to reduce the burden of discovery).

Department attorneys will want to assess anticipated or requested discovery against the factors identified in Rule 26(b)(2)(C), and the 2006 Committee Note quoted *supra*, and may want to focus in particular on the "needs of the case," the "importance of the issues at stake in the litigation," and the "importance of the proposed discovery in resolving the issues." *See* FED. R. CIV. P. 26(b)(2)(C)(i)- (iii) advisory committee's note (2006). In cases involving damages, the amount in controversy will be important, and the parties' resources may also be a relevant factor. *See* FED. R. CIV. P. 26(b)(2)(C)(iii). The *Major Tours* and *Young* decisions are important reminders that, in cases involving discovery against public agencies, courts must take into account that agency resources are constrained and, in the current economy, are even more constricted.

In applying proportionality principles, it also is important to keep in mind that, under Rule 26(b)(2)(B), a party that is required to produce "tier 2" information after a showing of good cause by the requesting party may do so, subject to conditions prescribed by the court. The Committee Note explains that conditions may include "limits on the amount, type, or sources of information" or may also include "payment by the requesting party of part or all of the reasonable costs" of obtaining information from the sources. *See* FED. R. CIV. P. 26 advisory committee's note (2006). Where, for, example, the agency has determined that the identification and production of the ESI will involve substantial costs, it should demand that the opposing party defray those costs or at least share them on an equitable basis.

This issue may take on particular importance when the discovery involves compliance with a Rule 45 subpoena issued by one of the parties in litigation that does not involve the federal government or one of its agencies as a party. Rule 45(c)(1) explicitly states that the party serving a subpoena "shall take reasonable steps to avoid imposing undue burden or expense" on a person subject to a subpoena. *See* FED. R. CIV. P. 45(c)(1). Rule 45(d)(1)(D) specifically incorporates the two tier provisions of Rule 26(b)(2)(B) when a nonparty receives a subpoena for the production of ESI. *See* FED. R. CIV. P. 45(d)(1)(D). Courts are more willing to impose cost-shifting or cost-sharing when the nonparty may be required to produce voluminous ESI and also take into account whether the nonparty has any interest in the underlying litigation. *See Degeer v. Gillis*, 2010 WL 5096563, at *20-21 (N.D. Ill. Dec. 8, 2010)

(imposing cost-sharing and citing the defendants' failure to cooperate with the nonparty in the development of search terms as a controlling factor); *Universal Del., Inc. v. Comdata Corp.*, 2010 WL 1381225, at *8 (E.D. Pa. Mar. 31, 2010) (imposing 50/50 cost sharing in a case in which the nonparty formerly was a party and, in turn, the subsidiary of a party, and had agreed as part of its dismissal as a party to preserve ESI to the same extent as if it were a party). In these situations, the agency should try to work with the parties to reach an agreement on a reasonable scope and manner of ESI production and should also demand that the parties bear the resulting costs.

E. The role of non-monetary factors

In actions to enforce constitutional or statutory rights, the nature of the parties' claims or defenses may be an additional factor in the parties' attempt to evaluate the respective costs and benefits of their discovery. The Sedona Conference® *Principle 5* recommends that nonmonetary factors "should be considered when evaluating the burdens and benefits of discovery." 11 SEDONA CONF. J. at 300. It explains that the Rules already recognize that proportionality "encompasses nonmonetary considerations," citing the provisions of Rule 26(b)(2)(C)(iii) and Rule 26(g)(1)(B)(iii), respectively stating that the court and the party promulgating discovery consider, *inter alia*, the "the importance of the issues at stake in the action." *Id.* The *Principle* also explains that "[a]ny proportionality analysis should consider the nature of the right at issue and any other relevant public interest or public policy considerations and whether, under the particular circumstances of the case, there should be restrictions on discovery." *Id.* at 301.

Courts have observed that, in actions to enforce federal statutes, including the antitrust and civil rights laws, parties may have the right to broad discovery. *See, e.g.*, *In re Aspartame Antitrust Litigation*, 2008 WL 2275531, at *1 (E.D. Pa. May 13, 2008); *Robbins v. Camden City Bd. of Educ.*, 105 F.R.D. 49, 55 (D.N.J. 1985). In each case, however, the parties and the court must consider what specific discovery is appropriate given the nature of the case. *See United States ex rel. McBride v. Halliburton Co.*, 2011 WL 208301, at *7 (D.D.C. Jan. 24, 2011) (discovery in a qui tam action, the court explains that "[a]ll discovery . . . is subject to the court's obligation to balance its utility against its cost.").

That important issues may be at stake in a case does not mean that more discovery is presumptively appropriate. For example, consider a lawsuit in which the plaintiffs demand a prospective injunction against a federal agency based on the agency's alleged violations of a constitutional right. Plaintiffs' counsel may urge that broad, and presumptively unlimited, discovery is appropriate against the agency. Counsel may also argue that only broad discovery can identify the origin of the illegal or unconstitutional policy or practice, its scope or extent, the employees of the defendant agency responsible for that policy or practice, and any past or current effects of that policy or practice on the citizens injured by it. If the plaintiffs' financial resources are limited, their counsel will argue that the full costs of discovery must be incurred by the defendants.

Faced with those arguments, a court may conclude that more discovery will proceed, but that could be an overly simplistic response. The defendant agency can explain that plaintiffs' factual claims are inherently weak, that the challenged policies are constitutional under settled law, or that there were only a few incidents of alleged illegality, and that the proposed discovery sweeps too widely. More importantly, the agency could argue that the costs of the discovery will be a burden on its operations or will require the diversion of its funds and resources from other public programs or operations. For example, in *Young v. Pleasant Valley Sch. Dist.*,2008 WL 2857912 at *3 (M.D. Pa. July 21, 2008), the court cited the cost that the school district would incur to comply with plaintiffs' proposed discovery,

specifically distinguishing the district's situation and its budgetary constraints, from that of a for-profit corporation.

In one employment discrimination case against a federal agency, *McPeek v. Ashcroft*, 202 F.R.D. 31, 34 (D.D.C. 2001), the court also recognized that the agency would incur substantial costs in restoring backup tapes of its e-mail system. The court observed that, to the extent agency employees would be required to search the backup tapes, diversion could mean that "the function of the agency suffers to the detriment of the taxpayers." *Id.* at 34. To resolve the burden issue, the court authorized a limited sampling of potentially relevant tapes. *Id.* at 34-35. Based on the sampling, the court ordered the restoration of only one additional tape. *Id.* at 33, 35-37.

Proportionality principles will remain relevant to the analysis of non-monetary cases. In those cases, the court may evaluate whether good cause exists to grant a request for otherwise possibly burdensome discovery. In actions brought by the United States, Department attorneys may be able to advocate that the importance of the issues at stake in the litigation – for example, the enforcement of constitutional or statutory rights – supports broad discovery.

V. Conclusion

In evaluating discovery requests that may involve extensive ESI, Department attorneys will need to determine the nature of the discovery at issue and balance the respective benefits and burdens of that production. It can be expected that, during the next several years, many courts will become more sophisticated in addressing E-Discovery disputes and will expect the parties to consider proportionality in developing their discovery plans. Department attorneys will need to be prepared to conduct that analysis and advocate their clients' positions effectively.❖

ABOUT THE AUTHOR

❑**Theodore C. Hirt** has been an attorney in the Civil Division since August 1979. He has been a Trial Attorney, Senior Trial Counsel, and Assistant Director in the Federal Programs Branch. Since June 2008, he has been handling immigration appeals in the federal circuits in the Division's Office of Immigration Litigation. He has been extensively involved in the federal rule-making process and he continues that work in his capacity as an advisor to the Assistant Attorney General for the Civil Division, who serves as *ex officio* on the Civil Rules Advisory Committee. Mr. Hirt has also assisted in coordinating E-Discovery issues within the Department and the Civil Division, lectured on E-Discovery issues to federal agencies and other audiences, and written several articles addressing E-Discovery issues.✠

The views expressed in this article are those of the author and should not be construed as formal guidance.

Privilege Review in the Discovery Process: The Role of Federal Rule of Evidence 502

Daniel S. Smith
Trial Attorney
Environmental Enforcement Section
Environment and Natural Resources Division
U.S. Department of Justice

I. Introduction

Despite rapid improvements in the sophistication of tools that process E-Discovery, no method has developed that reliably substitutes for a careful, page-by-page manual review to prevent privileged material from being released to opposing counsel in discovery. The lack of a speedy and efficient method to execute a privilege review does not seem likely to change in the near future.

Because of the sheer volume of information, even a manual privilege review often cannot feasibly be performed on every page that is subject to discovery. Today, many hard drives can hold at least 500 million pages of text. If one attorney could review 500 pages of text for privilege in an hour, it would take nearly 1,000 attorneys to review a single full hard drive in 6 months. *See* Jason R. Baron et al., *The Sedona Conference® Best Practices Commentary on the Use of Search and Information Retrieval Methods in E-Discovery*, 8 SEDONA CONF. J. 189, 198 (2007) (discussing methods used to confront search and retrieval problems in the discovery process).

The challenge of efficiently reviewing a large volume of material in the discovery process has become evident in litigation. The Civil Division of the U.S. Department of Justice has handled at least two cases where the litigation databases exceeded one billion pages. Verizon spent $13,500,000 on privilege review in a single case, Patrick L. Oot, *The Protective Order Toolkit: Protecting Privilege with Federal Rule of Evidence 502*, 10 SEDONA CONF. J. 237, 239 (2009) (discussing the expensive nature of reviewing large volumes of information), and the Office of Federal Housing Enterprise Oversight spent $6 million on privilege review for a case in which it received a subpoena and was not even a party to the litigation. *In re Fannie Mae Sec. Litig.*, 552 F.3d 814 (D.C. Cir. 2009).

Although one is seldom presented with a scenario as bleak as needing a battalion of privilege reviewers to work full time for many months, the impracticality of reviewing collections for privilege using traditional page-by-page review is a real problem. Before the adoption of Rule 502, litigants that faced an impossible privilege review were forced to rely on claw-back or quick peek agreements to protect privilege. In a claw-back agreement, the parties to the agreement exchange information with only a limited privilege review. In the event that the parties discover that a privileged document has been produced, the producing party may "claw it back" by demanding that the recipients return or destroy all copies of the document. In a quick peek agreement, the producing party allows the requesting party to inspect documents that have not been reviewed for privilege. The requesting party identifies documents that it wishes to have produced and then the producing party reviews those documents for privilege

before providing the requesting party with copies that it can keep. In either case, the parties agree not to argue that the disclosure of privileged information under the agreement results in the waiver of the privilege.

Serious weaknesses accompany claw-back and quick peek agreements. First, the parties to the agreement cannot prevent non-parties from arguing that the disclosure of privileged material under the agreement has waived the privilege. Thus, even the inadvertent disclosure of privileged information in full compliance with the terms of a claw-back agreement can result in waiver of the privilege, depending on how strictly courts apply the doctrine of waiver in that jurisdiction.

Second, the consequences of waiver can be severe. Under the attorney-client privilege, the waiver of privilege over one document can result in the waiver of privilege over all documents of the same subject matter. *See, e.g.*, *In re Grand Jury Proceedings*, 78 F.3d 251, 255 (6th Cir. 1996). While this doctrine, known as subject-matter waiver, often does not apply to the work product protection, *see, e.g.*, *In re United Mine Workers of Am. Emp. Benefit Plans Litig.*, 159 F.R.D. 307, 311 (D.D.C. 1994), the waiver of privilege over even a single document can have severe consequences for both the client, who may lose the case, and the attorney, who may be subject to disciplinary action. Consequently, the stakes are very high when it comes to protecting privilege, yet it is increasingly common that the cost of a manual privilege review would approach or exceed the value of the issues at stake in the litigation. Solving that problem is the main impetus behind the new Federal Rule of Evidence 502.

Rule 502 is not a solution to all problems, but it is far better than nothing for the federal government. This article will discuss Rule 502 from a litigator's perspective and will primarily focus on part (d) of this rule and its potential for streamlining privilege review. Specifically, Part II will discuss the provisions of the rule. Part III will explain the benefits and risks of entering into a 502(d) order, the potential for overestimating the benefits of a 502(d) order, and some additional concerns a court might have about entering such an order. Part IV will outline a framework for determining whether a 502(d) order is desirable in a particular case. Lastly, Part V will explain that clients can minimize the risks of 502(d) orders by improving the way that they manage information.

II. The provisions of Rule 502

In its opening words, Rule 502 sets forth a very important limitation, stating that it applies only to the attorney-client privilege and work product doctrine, defined in paragraph (g). Rule 502 *has no impact on any other privileges or protections*, including the deliberative process privilege, that are uniquely applicable to the government.

Paragraph (a) of Rule 502 addresses subject-matter waiver. This provision establishes that in a federal proceeding, the disclosure of privileged information does not result in subject-matter waiver unless the waiver is intentional and the disclosed and undisclosed communications "ought in fairness to be considered together." An advisory committee note to subdivision (b) of this rule defines a "federal proceeding" by stating that it includes, but is not limited to, an administrative agency that exercises its "regulatory, investigative or enforcement authority." FED. R. EVID. 502 advisory committee's note (2007). Notably, this provision creates the first national standard for the application of subject matter waiver. Jonathan M. Redgrave & Jennifer J. Kehoe, *New Federal Rule of Evidence 502: Privileges, Obligations, and Opportunities*, 56 FED. LAW. 34, 36 (2009).

Paragraph (b) addresses inadvertent disclosure. Prior to the adoption of Rule 502, circuit courts were split as to which test to apply to determine whether an inadvertent disclosure resulted in a waiver of privilege. Rule 502(b) adopts the "middle" or "intermediate" test, stating that a party can avoid waiver if

it can show that "the holder of the privilege" – not necessarily the disclosing party – took reasonable steps to prevent disclosure and to rectify any errors. Rule 502(b) quickly became the subject of decisions in which courts interpreted and applied the provision in different ways. *See* Oot, *supra*, at 242-50 (discussing cases). It may be some time until a consensus emerges in the interpretation of Rule 502(b).

Paragraph (c) addresses disclosures that have taken place in an earlier state proceeding. The provision states that if there is an order in the state court proceeding concerning waiver, that order applies. However, in the absence of a state court order, the disclosure does not result in waiver if it would not have been a waiver had it occurred during a federal proceeding or had it not resulted in a waiver in the state where the disclosure occurred.

Paragraph (d) contains the key provision of the rule. It states that a federal court may issue an order that a disclosure in the litigation pending before the court does not result in waiver. This paragraph does not require that the disclosure be inadvertent within the meaning of Rule 502(b). Subject to the court's approval, the parties may specify a standard of care that must be followed in order to avoid waiver of the privilege or, perhaps more commonly, the parties may agree that no disclosure, regardless of the standard of care, results in a waiver.

In case the language in Rule 502(d) were not clear enough, paragraph (e) expressly states that an agreement among the parties, such as a claw-back or quick peek agreement, does not prevent a third party from claiming that the privilege has been waived unless the agreement is incorporated into an order under paragraph (d).

Paragraph (f) provides an important buttress to Rule 502 by declaring that state courts must honor the effect of a 502(d) order. It also declares that a state court may not find that a disclosure that occurred in a federal proceeding waived a privileged, if the disclosure would not have resulted in waiver under Rule 502.

III. 502(d) orders

The changes to the law of waiver enacted by Rule 502(a) and (b) are important and could have implications in many cases. The ramifications of Rule 502(a) and (b) in a case are dwarfed, however, by the importance of deciding whether to invoke Rule 502(d), the one provision that has the greatest potential to impact the course of the litigation and which does not automatically apply to every case.

With a 502(d) order, parties can opt out of the standard of care required by Rule 502(b) and protect the claim of privilege even if the disclosure was not "inadvertent" within the meaning of this rule. The order might specify certain procedural steps that are sufficient for protecting privilege, such as key word searching, or it may state that disclosure of privileged information does not result in a waiver regardless of the circumstances. If the 502(d) order specifies the steps that the parties must take to preserve a claim of privilege, then those steps essentially stand in for the "reasonable steps" under Rule 502(b). A 502(d) order simply stating that no disclosure results in a waiver is sometimes called an "irrespective-of-care" order. As discussed in more detail below, such orders have been criticized on several grounds. *See* Jessica Wang, *Nonwaiver Agreements After Federal Rule of Evidence 502: A Glance At Quick-Peek and Clawback Agreements*, 56 UCLA L. REV. 1835, 1846-47 (2009).

A. Benefits

A properly executed 502(d) order can have tremendous value. In cases involving a large document and/or a large data exchange, a 502(d) order can save millions of dollars and thousands of hours of privilege review time. In smaller cases, a 502(d) order can ensure that the cost of privilege

review is proportional to the issues at stake in the litigation, allowing the dispute to be decided on the merits rather than on the basis of a disproportionate privilege review burden. Frequent litigators, such as the federal government, may accumulate substantial savings from 502(d) orders in various cases, allowing them to shift resources away from litigation and toward the execution of their goals and missions. In cases of any size, a 502(d) order can reduce or eliminate side litigation over whether a disclosure of privileged information resulted in a waiver.

In the face of such potential benefits, litigators might legitimately ask, Why not enter into a 502(d) order in every case in federal court? Because such orders rarely harm the client's interest and could save significant sums of money or minimize the consequences of a disclosure of privileged information, most litigators will find that the scales weigh heavily in favor of seeking a 502(d) order. However, one should not assume that a 502(d) order is appropriate for every case.

B. Risks

Genuine, if somewhat small, risks for the client exist, especially with orders that apply irrespective of care. Also, while it is not clear how Rule 502(d) will be applied, a court may refuse to issue such an order for other reasons. This latter concern should motivate litigators to prepare to make a showing of genuine need for the order where it exists.

Although the risks associated with a 502(d) order are probably small, a 502(d) order may increase the risk of disclosure of privileged information in some circumstances, even when the parties do not intend to disclose material without engaging in some form of privilege review. The potential consequences of such a disclosure are well known. While the 502(d) order may prevent opposing counsel from being able to use a privileged document as evidence, the harm of disclosing privileged information comes not just from an adversary being able to introduce it as evidence, but also from an adversary merely seeing it. Knowing privileged information may allow opposing counsel to change strategy or to take deposition testimony about subjects that otherwise may have been overlooked. That, in turn, may ultimately change the outcome of the case. *See* Wang, *supra*, at 1846-47.

The first way that obtaining a 502(d) order may increase the risk of disclosure of privileged information is by creating a deadline crisis. In a small case with significant amounts of privileged information, litigators may find that a page-by-page privilege review is feasible and is the best way to prevent disclosure of privileged information that opposing counsel may be able to use. However, in the event that the privilege review takes longer than anticipated – a real possibility that may occur for a number reasons – the party may find it more difficult to obtain an extension of discovery deadlines if there is a 502(d) order in place. Opposing counsel may argue that the parties and the court agreed to a truncated privilege review and that the 502(d) order provides the means to meet the discovery deadline by preserving the claim of privilege, even if the material is disclosed with little or no review for privilege. While the need to protect privileged information should trump this argument in many cases, 502(d) makes it harder to show good cause for an extension of the deadline.

The second way in which a 502(d) order may increase the risk of disclosure of privileged information is by exerting its psychological pull on counsel. Faced with a burdensome and expensive privilege review, tight deadlines, and limited resources, relying on the 502(d) order and truncating the privilege review will be extremely tempting. A litigator would likely find it easy to cut short the privilege review or conduct a low quality review, dangerously assuming that the 502(d) order will protect the client. *See* Wang, *supra*, at 1851-54 (proposing that irrespective-of-care 502(d) orders can make the attorney's interests inconsistent with the client's).

Another way that a Rule 502(d) order may increase risk to the client is by facilitating data dumping by opposing counsel. Martin R. Lueck et al., *Federal Rule of Evidence 502(d) and Compelled Quick Peek Productions*, 10 SEDONA CONF. J. 229, 235 (2009). Freed from the cost of reviewing material for privilege, it may become easier to pursue a strategy of burying opposing counsel with a large volume of irrelevant or tangentially relevant material. Even if the receiving party manages to stay afloat of the volume of information, the order will shift costs from the producing party – who may not have to review the documents at all – to the receiving party that will have to review the documents for relevance and will have to segregate potentially privileged information until its status can be resolved with opposing counsel or the court. *Id.*

Each of the risks described above are somewhat greater if the 502(d) order is silent about the standard of care a party must use to preserve a claim of privilege under the order. Nothing in Rule 502(d) prevents a court from authorizing parties to disclose documents to each other without any privilege review and without waiving any privileges. However, abandoning any privilege review carries the greatest risk of giving opposing counsel the advantage of knowing privileged information. A more sophisticated approach would specify certain methods of privilege review for each type of document or each document collection that, if adhered to, would preserve the claim of privilege. In *Hopson v. Mayor and City Council of Balt.*, 232 F.R.D. 228 (D. Md. 2005), a case that was decided before the existence of Rule 502 but was important in its development, the court contemplated having the producing party use the cost-benefit balancing factors in Rule 26(b)(2) to "marshal the specific facts that would justify less than full pre-production privilege review." *Id.* at 244. Developing such an order would also provide a good opportunity to counsel the client on the risks and benefits of various privilege review methods. However, a 502(d) order that is too specific or requires too much privilege review may create a standard that cannot be met and may forgo much of the benefit of the 502(d) order, arriving at something not much different from the protections the parties already have under Rules 502(b) and (e).

C. Weighing the benefits against the risks

In addition to underestimating the risks associated with disclosing privileged information to an adversary, one can overestimate the benefits of a 502(d) order. While a one terabyte hard drive could hold 500 million pages of text, it is very unlikely that 100 percent of the hard drive would be filled with pages of text. In most cases, large portions of it will be empty or filled with operating system and program files that need not be reviewed for privilege. It may also contain digital photographs that can be reviewed much more quickly than the equivalent volume of text. For example, three megabytes of text might fill 96,000 pages and take 194 attorney-hours to review, while three megabytes of digital photographs might consist of a single photo that an attorney can review in a few seconds.

Similarly, very large collections of data can often present fewer privilege review problems than smaller collections. While Wal-Mart's data center, for example, may store a petabyte (1,000,000 gigabytes) or more of data, one would expect that much of that data is inventory and sales transaction data that does not require page-by-page review for privilege. In fact, massive databases often need not be produced in their entirety. For example, if a dispute were to arise about consignment fees being paid to a supplier by a retailer, the supplier probably does not need data regarding every sales transaction recorded by the retailer. Rather, the supplier would only be interested in summary data regarding the transactions that involved the product at issue.

D. Impact of 502(d) orders on the rights of non-parties

In addition to being cognizant of the concerns above, a court may have concerns about the impact of the order on the rights of non-parties. A 502(d) order can convert what would be a waiver of privilege under Rule 502(b) and render it a non-waiver. It is perhaps one thing if this ruling affects the parties to the action over which the court has jurisdiction and perhaps another thing if this ruling affects the rights of third parties, who will most often be a private plaintiff in parallel litigation in state or federal court but who may also be a member of the community regulated by an agency. If the potential for such a situation comes to light before the order is entered, courts may expect the parties to justify the order with a specific showing of need.

The possibility of rendering any disclosure of privileged information, intentional or not, a non-waiver, may create some potential for abuse. Parties could conceivably engineer litigation for the purpose of protecting disclosures that would otherwise waive claims of privilege for good policy reasons. No evidence that Rule 502(d) was intended to allow parties to make selective waivers of privilege exists and courts can be expected to decline to enter the orders if they perceive such an effect. Edward J. Imwinkelried, *A Crash Course in Rule 502*, 46 TRIAL 38 (July 2010).

The risks to clients and third parties may cause some courts to hesitate to enter a 502(d) order that protects privilege irrespective of care. In order to ensure that only those disclosures that are impossible, or at least genuinely difficult to avoid, are being protected, a court may wish to include some description of the privilege review that the parties will conduct. In order to justify procedures that might be considered less than reasonable care in some cases, the court may wish to incorporate findings that explain the need for the order, such as the volume of information that may be potentially responsive. Currently, however, specifying the privilege review procedures and the reasons for them does not appear to be the norm. More commonly, the privilege review procedures are left to the discretion of the parties. Procedural requirements, if any, deal with time limits for making a claim of privilege after the party learns of a disclosure of privileged information.

IV. Determining whether to seek a 502(d) order

While 502(d) orders are not necessary in every case and should not be entered into without proper contemplation, they are a necessity in the largest cases and a good protection against waiver of privilege in many others. The question then becomes, How does one determine whether to seek a 502(d) order in a particular case? The answer depends on early case assessment and case planning.

A litigator that is genuinely interested in reducing the cost and burden of discovery, particularly E-Discovery, will recognize the need to plan for discovery as much as possible. Before discovery begins and before the 26(f) conference takes place, one should identify the issues at stake in the litigation, identify the sources, types, and volumes of information likely to be exchanged in discovery, and develop a plan for collecting, processing, reviewing, and producing that material. Having determined the volume of information that is likely to be exchanged, a litigator can estimate what it would cost in terms of time and resources to review the discovery materials for privilege using the traditional page-by-page method. The litigator should also sample collections of potential discovery materials and interview document custodians to estimate the amount and sensitivity of privileged information. Finally, the litigator should determine what tools are available to assist in a traditional privilege review or to substitute for it. Unless the litigator is very familiar with these tools, it may be necessary to experiment with them on samples of the discovery material or to speak with litigators who have employed them in similar cases.

Having conducted the analysis described above, a litigator should be able to form a plan for conducting a privilege review and be able to articulate specific reasons supporting the adoption of that plan. Armed with this information, litigators can meaningfully counsel their client on the risks and benefits of various methods of privilege review and of a having the court enter a 502(d) order. Once the litigator and client have made a decision, the same information can then be articulated to the court in support of, or in opposition to, a 502(d) order.

While advocating for a 502(d) order, a litigator must remember that privileges other than the attorney-client privilege and the work product doctrine are not within the scope of Rule 502 and cannot be preserved by the 502(d) order. The parties can, however, include in the terms of the order a claw-back agreement that covers any other applicable privileges. The incorporated claw-back agreement may not bind third parties, but the law of waiver for such privileges may be different such that a disclosure under the circumstances would not constitute a waiver in any event.

When privileges other than the attorney-client privilege and the work product doctrine are implicated in discovery, litigators should weigh more carefully the benefits of a full privilege review. If a 502(d) order is still advisable, the attorney should also consider increasing the rigor of the privilege review efforts so that they can maintain that the efforts were proportional to the issues at stake in the litigation. This consideration will increase the chances that any disclosure of material subject to other privileges can be characterized as inadvertent and will thus help to preserve the privilege.

V. Clients' role in minimizing the risks

Rule 502 has tremendous potential to facilitate litigation by reducing the consequences of disclosure of privileged information and allowing litigants and courts to adopt privilege review methods that are sensible in light of the issues at stake in the litigation. The most important provision in accomplishing this purpose is paragraph (d) that authorizes orders preserving claims of privilege, even with regard to third parties. While these orders offer several benefits, they also carry serious risks.

Litigants possess many opportunities to maximize the benefits and minimize the risks of 502(d) orders. As the Electronic Discovery Reference Model clearly indicates, discovery begins with information management. ELECTRONIC DISCOVERY REFERENCE MODEL, www.edrm.net. A client who wants to retain the option of using 502(d) with minimal risks of disclosing privileged information will make the segregation of potentially privileged information a regular feature of the information management plan. If a litigant is able to keep collections of records and data that do not contain privileged information, that client may be able to produce those collections in discovery pursuant to a 502(d) order with confidence that the collection will contain privileged information only if it was inadvertently placed there. Even in the absence of a 502(d) order, the efforts taken in the ordinary course of business to keep a collection of records free of privileged material may arguably count towards the "reasonable steps" needed to invoke the protection against waiver under Rule 502(b).

One caveat to this approach is that it transfers the responsibility for privilege determinations from specialists, namely, attorneys preparing to litigate a specific dispute, to perhaps thousands of record custodians, who may not fully understand the elements of a claim of privilege. Document custodians may fail to recognize the existence of a privilege or may reach inconsistent results in cases where multiple copies of a record exist. To be successful, a client would probably have to provide training and regular feedback to document custodians in order to get accurate privilege determinations.❖

ABOUT THE AUTHOR

❑**Daniel S. Smith** has been a Trial Attorney at the U.S. Department of Justice, Environment and Natural Resources Division, Environmental Enforcement Section, since being accepted in the Attorney General's Honors Program in 2002. He currently serves as an E-Discovery coordinator for the Environmental Enforcement Section.✠

The views expressed in this article are those of the author only and should not be construed as formal guidance. This article has not been adopted as the formal view of the Environment and Natural Resources Division, the Justice Department, or any other federal agency. This article does not create any right or benefit, substantive or procedural, enforceable at law by any person against the United States, its agencies, officers, or any other person.

E-Discovery – A Team Effort Between Attorneys and Technical Support Staff

Matthew C. Hammond
Trial Attorney & Civil Coordinator of E-Discovery Working Group
Antitrust Division
U.S. Department of Justice

Michael Lewis
Litigation Support Principal Systems Engineer
BAE Systems IT
EOUSA, Office Automation and Litigation Technology Service Center

I. Introduction

Before E-Discovery, paper ruled the day. Paper is static, easily Bates numbered, and understood as it relates to discovery. Attorneys know how to handle, track, review, and produce paper, printing out electronic documents and data for reference, storage, depositions, and discovery. Many are also comfortable with converting paper to static electronic images and searchable text. In the paper-only world, printers and copiers would be sufficient for any litigation support staff to handle discovery using simple and straightforward procedures. But today, well over 90 percent of all information is stored electronically, and attorneys are dealing with an avalanche of dynamic information that is easily altered and, for most attorneys and even some technical support staff, not well understood. Generally, individuals in this line of work do not understand the complexity of electronic systems or how to properly handle, collect, track, review, process, and produce electronically stored information (ESI), much less identify it in the first place.

II. The value of IT experts

Today, litigation demands information technology (IT) experts in all phases of an investigation or case where ESI is involved. In order to be successful, subject-matter technology experts who have an understanding of the goals and requirements regarding ESI must be an integral part of the litigation team. If litigation support and IT staff are not included from the very beginning, many things can go awry. The scenario below offers an example.

> An attorney needs to collect, review, and produce documents in a civil fraud investigation where an agency employee is accused of embezzling money by altering electronic invoices and authorization memos. He asks the agency IT personnel to give him copies of all the authorization memos and electronic invoices on a CD-ROM. They respond, "No problem. When do you want it?" The agency IT personnel produce 45 CD-ROMs of the potentially-altered memos, many stored only on the employees desktop, and also include Microsoft Excel files of invoice data exported from the invoice database. The attorney then says that he has what he needs. Six months later, the attorney is considering dropping the case because he lacks critical evidence and the resources to adequately process, review, and produce it.

So, what went wrong in the above situation? A non-exhaustive list provides a few answers:

- **Documents and data were not collected properly.** IT personnel gave the attorney exactly what he asked for but, as it turned out, not what he needed. First, by merely copying documents to 45 CD-ROMs (much less efficient than using a single hard drive), information about when the electronic documents were created, last accessed, and last modified was lost. Second, the files were not logically organized, making it difficult to identify custodians, prioritize processing and review, or adequately defend the procedures and methods used. Third, the database export only included the invoice data and not an audit trail on queries, access, or changes for the relevant records. As a result, the attorney has no evidence to show what was changed, when it was changed, or by whom it was changed.
- **The attorney assumed the "originals" would be preserved.** Believing that the attorney had what he needed, IT personnel went back to normal operations. They upgraded the invoice database and, by doing so, deleted the historical audit trail information. When the accused employee left the agency, his hard drive was reformatted following established and routine IT policy. As a result, critical data in the databases and on the accused employee's hard drive that should have been subject to a litigation hold was lost. The limited number of authorization memos stored on the server had been preserved under the litigation hold.
- **The IT personnel assumed they were finished when they delivered the 45 CD-ROMs.** IT personnel delivered exactly what the attorney requested from the database and employee's desktop. Thus, they had no reason to preserve other potentially relevant information in locations or systems that would impose a cost and burden on their operations.

More important than identifying what went wrong is asking, "*Why* did it go wrong?" The various explanations for this question generally boil down to a lack of communication between the attorney and the IT personnel. On one side, the attorney did not know how the agency's systems worked, the likely locations of potentially relevant information, or the impact of using improper methods to copy to CD-ROM when he made his narrow and specific request. Instead of explaining his needs and asking for more information, he assumed that copying to CD-ROM preserved everything, that audit information would be included in what he got from the electronic invoice database, and that he could always go back for more information. On the other side, the IT personnel did not know what the attorney ultimately wanted to do with the files and did exactly what they believed they were asked to do. If the IT personnel knew that information regarding who made alterations and when those alterations were made were important for the attorney, they would have given him appropriate information about where that information was and how to preserve it. With that knowledge, the attorney may have better overseen the litigation hold and avoided the loss of critical information.

III. Proactive steps to prevent problems

Diagnosing the cause of the disconnect between the IT personnel and attorneys illustrated above is beyond the scope of this article and probably offers little practical advice about day-to-day efforts. Instead, what may be more valuable are suggestions about how to avoid such a disconnect in the first place. Following these suggestions will decrease the amount of time spent overall on E-Discovery issues and remove obstacles to moving the investigation or case forward.

A. Involve IT personnel from the very beginning. IT personnel are instrumental in implementing and defining the necessary scope of any litigation hold or criminal preservation obligation. The agency IT personnel know their systems, their default settings (for example, autodelete every 30 days), their capabilities in exporting information in usable form, and the burden that preservation, collection, or production will place on the agency. IT personnel specialized in litigation support know the capabilities of a requesting attorney's review platforms and how information must be formatted in order for it to load properly into those platforms. They can also help translate communications between attorneys and opposing counsel's IT personnel and IT advisors. By making IT personnel a formal part of the team and including them at every phase of the case or investigation, IT personnel can and will be able to identify technical issues to be considered at an earlier stage in the process and, thus, save time later on.

B. Know your limitations and IT personnel's limitations. No matter how technically savvy an attorney may be, he does not know the intricacies of an agency's computer systems or his own office's systems that will be receiving and working with ESI. IT subject-matter experts must be identified and involved in the process to provide the insight, knowledge, and skills necessary to navigate these different systems. It is also important to remember that IT personnel are not attorneys and, especially in the case of agency IT personnel, they do not know the law, what is needed to prove the case, or the impact of the shortcuts they may take. An attorney should establish that no question is too simple or rudimentary and ask them for the same consideration for the many basic questions that the attorney will ask. Clearly defining the roles and expectations with IT personnel encourages them to speak up on topics of their expertise and ask pertinent questions regarding the attorney's expertise – the law.

C. Define your needs and requirements and share information. When requesting assistance or information from IT personnel, an attorney should clearly explain what he needs and set priorities. An attorney should explain the case sufficiently for IT personnel to understand what type of information is critical. If the attorney in the example above had only taken a few minutes to explain, the IT personnel may have realized that he was asking for the wrong things. By providing IT personnel with specific requests that are clear and understandable to IT personnel, the attorney communicates what they need to most effectively help him identify the important ESI. In the example above, the attorney requested specific files copied to a CD-ROM because that was a format he was familiar with. He should have explained that he needed the potentially-altered memos and invoices, as well as any information about who had access to the documents and files, who accessed them, who changed them, when they were changed, and what was changed. With the desired information clearly specified in this way, the attorney and IT personnel would have been able to discuss the best ways to deliver that information to the attorney, while also preserving its integrity. The attorney could then have expanded the scope of the litigation hold to the relevant sources of information and followed up with the IT personnel when the accused employee left the agency. Armed with the knowledge of what the attorney wants to do with the ESI, IT personnel can recommend the best software tools to use or at least explain the relevant trade-offs between using different software tools for review, analysis, and production.

D. Listen and test. IT personnel are problem-solvers at heart and approach many tasks from a customer-service perspective because that is how they often view the users they support. In that vein, IT personnel will often give the quick, simplified answer to a question about their systems because they believe the attorney does not want to know all the complexities about their systems and the few limited exceptions to their simplified answer. They are right in that most attorneys do not want or need to know every detail about their systems, but attorneys do need to know the exceptions and whether those exceptions will cause a problem. The best way for attorneys to obtain the needed information without being overwhelmed is to actively listen to IT personnel's answers to their questions and, as with any witness, test the answers against the facts known to the attorney and the needs of his case. For example,

the attorney could have asked whether he would be able to tell when the documents were last modified from the copies on the CD-ROM, whether one CD-ROM would suffice, how the information would be organized, or whether he could tell which user made changes to an invoice. These questions allow the IT personnel to effectively analyze and approach the ESI in the context of how the attorney needs to use it, a critical analysis.

E. Keep IT personnel in the loop and communicate regularly. As the investigation or litigation progresses, maintaining consistent communication with IT personnel, both at the agency and in the office, remains important. If they know about pending deadlines, they can plan accordingly and raise concerns before the eleventh hour. If they know the case is still active, the probability that the litigation hold will fall through the cracks may decrease. Regular communication also provides opportunities for IT personnel to inform attorneys of any problems that may arise and to feel more comfortable initiating communications when needed.

F. Advocate on behalf of IT personnel. A case imposes a burden and cost on IT personnel for an agency or for the attorney's office. An attorney should listen to the needs of the IT personnel and do what he can to alleviate that burden and cost when appropriate. Can the attorney get opposing counsel to agree to or the court to order a limitation on the agency's preservation obligations, so that the IT personnel can save specific back-up tapes but not all of them in perpetuity? Can he work with agency counsel to get IT personnel the necessary authority to produce or preserve the relevant documents that may otherwise be prohibited by existing agency policy? Can the attorney, within the confines of his case, stipulate to certain facts making production of ESI in relation to them unnecessary? Can he agree to or propose staged discovery that imposes less of a strain on IT's resources?

G. When problems arise, focus on fixing them and not on assigning blame. If anyone senses that the goal is to pin the blame on them for a mistake or error, their natural response is to become less cooperative. In these sensitive moments where problems may easily occur or worsen, the attorney needs the IT personnel's full cooperation and assistance. By focusing on problem-solving rather than blame, the attorney will maintain IT personnel's continued assistance that often salvages the case. Here, it is important to remember that IT personnel are problem-solvers at heart and generally want to assist the attorney.

H. Involve IT personnel in all ESI discussions with opposing counsel. Attorneys need IT personnel to translate and help them understand what the other side is requesting or offering. IT personnel can help determine whether fulfilling a request is possible with the systems used by the agency or the attorney's office and whether it meets the attorney's needs to review and analyze the ESI. They will also be able to make sure the attorney asks the right questions so that the best-informed decisions may be made. To avoid awkward moments, an attorney may want to establish in advance how he would like the IT personnel to participate (for example, fly on the wall or participate when invited to answer).

I. For large investigations and litigations, identify a primary point of contact on both sides. Designating one person to take formal responsibility – legal and IT – for both sides in large investigations provides more accountability. Also, other staff know where to go for answers when issues arise. This idea is similar to designating a litigation hold coordinator who may be the same person, depending on the needs of the investigation or case.

J. Don't make promises without consulting IT personnel. Attorneys should keep in mind that agency IT personnel still have their day jobs and may also be supporting other discovery obligations for their agency. The agency has its own mission and daily obligations that should rarely grind to a halt because of the attorneys' requests. The attorney's litigation support staff also have other cases that they

are supporting. Recognizing that the attorney and IT personnel both have to balance the litigation's needs against other practical and legal demands remains an important element in this process. By consulting with IT personnel before making commitments, an attorney can avoid making promises to a court that cannot be kept and also possibly avoid pitfalls that are not intuitively obvious to the attorney. Moreover, failure to consult with IT personnel can have catastrophic consequences. In *In re Fannie Mae Sec. Litig.*, 552 F.3d 814 (D.C. Cir. 2009), a federal agency was held in contempt for failing to comply with discovery deadlines after agreeing to over 400 search terms. *Id.* at 816-17. This failure resulted in discovery costs totaling 9 percent of the agency's annual budget. *Id.* at 817. One can easily envision the case's outcome by imagining an attorney making promises to a court without having a full, thoughtful discussion with his IT personnel, a failure leading to such an outcome.

These suggestions are meant to strengthen the lines of communication between attorneys and IT personnel, but also allow both to focus on their expertise and strengths. By including IT personnel as part of the litigation team and setting out clear goals and requirements, the attorney acts as a project manager in the execution of an effective, thorough, and manageable approach to the discovery process and the case or investigation at large.

IV. Conclusion

In the last few years, spoliation sanctions have been on the rise for improperly employing preservation and collection methods. Many of these sanctions resulted from a lack of communication between the attorney and the technical support staff, thus highlighting the importance of a well-developed e-discovery team. ESI, in even the smallest cases, can consume a significant amount of time and resources. However, an attorney can avoid a considerable loss of important time and wasted resources by partnering with IT personnel, by spending the time to explain the case on the front-end, by defining roles and responsibilities, and by specifically describing the goals and needs of the case. Consequently, IT personnel can become an attorney's greatest asset.❖

ABOUT THE AUTHORS

❑**Matthew C. Hammond** is an attorney in the Telecommunications & Media Enforcement Section of the Antitrust Division of the U.S. Department of Justice. He joined the Antitrust Division in 1998 and has focused on civil investigations of mergers and acquisitions, primarily in the telecommunications industry. Mr. Hammond is also the civil coordinator for the Division's E-Discovery working group that creates exemplars and resources for use for both civil and criminal matters within the Division. He has participated in multiple panels on E-Discovery issues and been on the faculty for E-Discovery training at OLE's National Advocacy Center.

❑**Michael Lewis** is the Litigation Support Principal Systems Engineer at BAE Systems IT for EOUSA's General Integration/Office Automation and Litigation Technology Service Center. Since he joined EOUSA's contractor staff in 2008, Mr. Lewis has worked extensively as an enterprise litigation support application deployment engineer and collaborated with the EOUSA E-Discovery Working Group and EDOC training initiatives. He also serves as a guest instructor at the National Advocacy Center for OLE courses and supports a number of USAOs involved in complex E-Discovery issues.✠

Spoliation and the Work Product Doctrine

Ryan Struve
Trial Attorney
Antitrust Division

I. Introduction

The proliferation of electronic evidence and the prevalence of litigation in business affairs create a potential clash of legal standards between the preservation of evidence and the work product doctrine. The proliferation of electronic documents creates the need to effectively retain and store these documents, a task that can be crushingly expensive for both corporations and government entities. Moreover, litigation is becoming a more prevalent part of business life with corporations considering the potential legal ramifications of every business transaction, interaction, or collaboration. With increased litigation comes increased strategizing about how to avoid costly legal battles. These conversations are now taking place earlier and earlier in business ventures. As a result, more "work product" is being created.

The increase in electronically stored information, combined with the rising prevalence of litigation in business affairs, produces a notable legal tension. The standard used for the preservation of documents and the work product doctrine each play an important role when approaching today's legal landscape. However, although no court has directly ruled on the issue, it would be a mistake to conclude that the two standards are identical or are triggered at the same time. The doctrines of spoliation and work product derive from two different overarching goals, as well as different authority for the courts. For most private litigants, equating these standards is not an issue because most litigants do not start creating work product until after the point at which a litigation hold is implemented. However, investigative government agencies begin considering the implications of litigation well before the investigation reaches the point where litigation actually becomes a reasonably foreseeable possibility. A rule treating work product and spoliation doctrines equally would threaten to cause significant hardship on government investigators.

The rules for when entities need to implement litigation holds and the standards by which documents are considered legally protected work product under the Federal Rules of Civil Procedure are both commonly referred to as "reasonably foreseeable litigation" tests. Some courts have recently noted the similarity of the language of these tests and intertwined their requirements. For example, courts have used the work product privilege to construct the trigger date for when documents should have been retained under a litigation hold. One court referred to the "common sense" conclusion that if documents were included on a privilege log as work product and were thus created due to reasonably foreseeable litigation, the litigation was reasonably foreseeable for litigation hold purposes. *See Siani v. State University of New York at Farmingdale*, 2010 WL 3170664, *5 (E.D.N.Y. Aug. 10, 2010); *see also Crown Castle USA Inc. v. Fred A. Nudd Corp.*, 2010 WL 1286366, *10 (W.D.N.Y. Mar. 31, 2010) (where the duty to preserve evidence arose when communications, privileged under the work product doctrine, began).

This article will briefly describe the current legal standards for preservation of documents and the work product privilege and conclude with a discussion about the intersection of those doctrines and why courts should hesitate before equating them, especially when government investigative agencies are involved.

II. Document preservation/spoliation

Federal courts may impose sanctions on parties that violate a court order by not properly preserving documents. Fed. R. Civ. P. 37. Even before discovery orders have been issued, courts have exercised their power to control litigation by imposing sanctions on parties that unduly spoliate evidence. *See, e.g., Chambers v. NASCO, Inc.*, 501 U.S. 32, 43-55 (1991); *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2d Cir. 1999). The legal standard for what constitutes spoliation of evidence–or conversely when parties are obligated to begin collecting and preserving documents–is almost always articulated the same way.

Courts have generally held that the obligation to preserve evidence arises when a party has notice that the evidence is relevant to pending litigation or to litigation that is reasonably anticipated. *See, e.g., In re Terrorist Bombings of U.S. Embassies in E. Afr.*, 552 F.3d 93, 147-48 (2d Cir. 2008); *Stevenson v. Union Pac. R.R.*, 354 F.3d 739, 747 (8th Cir. 2004); *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779, 780 (2d Cir. 1999); *Renda Marine, Inc. v. United States*, 58 Fed. Cl. 57, 60-61 (Fed. Cl. 2003); *D'Onofrio v. SFX Sports Group, Inc.*, 2010 WL 3324964, at * 5 (D.D.C. Aug. 24, 2010); *Nucor Corp. v. Bell*, 251 F.R.D. 191, 194 (D.S.C. 2008) (citing *Silvestri v. Gen. Motors Corp.*, 271 F.3d 583, 590 (4th Cir. 2001)); *Easton Sports, Inc. v. Warrior LaCrosse, Inc.*, 2006 WL 2811261, at *4 (E.D. Mich. Sept. 28, 2006); *Crandall v. Denver*, 2006 WL 2683754, at *1 (D. Colo. Sept. 19, 2006) (quoting *Jordan F. Miller Corp. v. Mid-Continent Aircraft Serv., Inc.*, 1998 WL 68879, at *5 (10th Cir. 1998)); *Consol. Aluminum Corp. v. Alcoa, Inc.*, 2006 WL 2583308, at *2 (M.D. La. July 19, 2006); *Ball v. Versar, Inc.*, 2005 WL 4881102, at *3 (S.D. Ind. Sept. 23, 2005); *Mosaid Technologies Inc. v. Samsung Electronics. Co.*, 348 F. Supp. 2d 332, 335, 338 (D.N.J. 2004); *Townsend v. Am. Insulated Panel Co.*, 174 F.R.D. 1, 4 (D. Mass. 1997); *Telectron, Inc. v. Overhead Door Corp.*, 116 F.R.D. 107, 126, 127, 128 (S.D. Fla. 1987).

Commentators in the E-discovery field have stated that litigation must be "reasonably foreseeable," to trigger preservation obligations, which occurs "when an organization is on notice of a credible probability that it will become involved in litigation, seriously contemplates initiating litigation, or when it takes specific actions to commence litigation." Thomas Y. Allman et al., *The Sedona Conference Commentary on Legal Holds: The Trigger & The Process*, 11 SEDONA CONF. J. 267, 270 (2010) (discussing reasonable practices to employ when addressing legal hold triggers and process).

The goals of the spoliation doctrine are apparent. Courts recognize that litigating parties might have an interest in discarding potentially relevant information–particularly evidence damaging to them–once the party realizes that litigation is reasonably foreseeable. To promote the full examination of evidence at trial, courts require that parties retain all relevant information.

III. Work product

In contrast to spoliation, the standard for analyzing what constitutes work product is anything but universal. More than 70 years ago, the Supreme Court in *Hickman v. Taylor*, 329 U.S. 495 (1947), recognized the basic need for a lawyer to "work with a certain degree of privacy." *Id.* at 510. The Federal Rules later codified the Court's notion of work product by protecting from discovery "documents and tangible things that are prepared in anticipation of litigation . . . ." FED. R. CIV. P. 26(b)(3).

Circuits and courts vary in defining what constitutes work "prepared in anticipation of litigation." *Id.* While all courts recognize that there is a certain point in time when work product can be created, the courts describe that point very differently. One leading view requires that the party asserting the privilege prove that "even if no specific claim is contemplated," the litigation underlying a work product claim be "reasonably foreseeable." *See Schiller v. NLRB*, 964 F.2d 1205, 1208 (D.C. Cir. 1992). Other courts have admitted that "[l]itigation need not necessarily be imminent" so long as "the primary motivating purpose behind creation of the document was to aid in possible future litigation." *Exxon Chemical Patents, Inc. v. Lubrizol Corp.*, 131 F.R.D. 668, 670 (S.D. Tex. 1990). Even others have demanded that parties demonstrate "an identifiable specific claim of impending litigation," and that the parties must "establish more than a 'likely chance,' 'remote prospect,' or 'inchoate possibility' of litigation." *SmithKline Beecham Corp. v. Apotex Corp.*, 232 F.R.D. 467, 484 (E.D. Pa. 2005) (quoting *Harper v. Auto-Owners Ins. Co.*, 138 F.R.D. 655, 660 (S.D. Ind. 1991).

Again, the goals of the work product doctrine are easy to see. Courts do not want attorneys working on behalf of their clients to be concerned that every single thought put down on paper could eventually be read by opposing counsel. Therefore, to promote effective representation for litigants, those papers are protected, thus freeing the attorney from those concerns.

IV. Analysis

The standards used to determine whether a party has spoliated evidence and whether a document is protected work product, although very similar, must remain independent of each other. It is no surprise that some courts intertwine these standards, without concluding that the standards are identical. Such a conclusion would be misguided because each standard derives from significantly different sources of power for the court and ultimately works toward different goals. The spoliation rule, for example, is intended to prevent parties from undermining the legal process by destroying documents that would be relevant to reasonably likely future litigation. Conversely, the work product standard encourages effective representation of counsel by shielding attorneys' work product from discovery. It encourages parties to be proactive by considering the legal ramifications of their actions and, in turn, to create work product. Combining these two standards would require parties either to impose widespread and expensive litigation holds when considering a litigation strategy or to risk sanctions for spoliation of evidence. Such a combination would encourage parties to avoid consideration of litigation strategy and risk altogether.

Instead, courts should recognize that although litigation may be "reasonably foreseeable" in a work product scenario, litigation may not be sufficiently foreseeable that destruction of evidence by the party is a serious concern. One court appears to have taken this view. In *Hynix Semiconductor Inc. v. Rambus Inc.*, 591 F. Supp. 2d 1038 (N.D. Cal. 2006), the court ruled that while "Rambus began formulating a licensing strategy that included a litigation strategy as of early 1998, [it] did not actively contemplate litigation or believe litigation against any particular [defendant] to be necessary or wise" until "late 1999." *Id.* at 1064. As a result, the court concluded that Rambus was under no obligation to preserve documents in early 1998. *Id.* The court seemed to recognize that litigation strategy can be divorced from document retention, a praiseworthy conclusion that other courts should follow.

Conflation of these two standards also poses a problem for the typical litigant. The work product doctrine is designed to protect the thought processes of attorneys and operates as soon as the initial evaluation to bring an action is made. The development of questions such as this one often begins long before an attorney can identify what evidence might be potentially relevant to the litigation and thus whether the evidence is subject to the preservation obligation.

Combining the standards is even more problematic for government entities, particularly civil prosecutorial departments and divisions. These organizations investigate *potential* civil violations of the law, and in doing so will likely consider litigation strategy even in instances where actual litigation is an extremely remote possibility. A rule that equates document preservation with work product creation would require investigatory federal organizations to impose extremely costly litigation holds in almost every investigation. This result could be financially debilitating to organizations such as the Antitrust Division, that open many investigations but litigate very few. Instead, courts should recognize that federal organizations, especially those that investigate legal violations, occupy a special role in federal litigation and need a rule that does not require imposition of litigation holds at the beginning of any potential investigation. It is unclear whether a special rule for federal agencies is warranted, or simply a recognition by the courts that the work product and document preservation doctrines are not intertwined. Should courts ultimately begin concluding that for typical litigants, the two doctrines are intertwined, then courts should establish that such a rule would not apply to investigative agencies.

Such treatment is warranted for many reasons. First, federal investigative organizations do not face a substantial probability of litigation at the moment they commence an investigation. Rather, they face that probability at some point later in the investigation when it becomes clear that the organization has determined that litigation is likely to ensue. At the commencement of the investigation, however, attorneys may be developing work product to assist in the investigation to determine whether litigation is a likely outcome. Second, some federal investigative organizations do not carry the same risk of destruction of evidence inherent in the spoliation rule because government agencies typically collect documents from private companies and individuals and do not have the documents within the organization.

V. Conclusion

The explosion of electronic discovery in recent years has moved the discussion of document retention to the forefront of litigators' minds. In turn, courts have created rules designed to protect the litigation process from being skewed by the reckless destruction of evidence likely to be requested in litigation. In the process, however, courts have begun equating the spoliation standard with the work product rule simply because of the similarity of the language in each rule. By examining the goals of each standard, courts should realize that the similarities are only facial and do not penetrate the core of their analyses. Courts should be mindful to avoid equating these standards in litigation, especially in the case of federal investigatory agencies.❖

ABOUT THE AUTHOR

❑**Ryan Struve** joined the Department of Justice in 2005. He is currently a Trial Attorney in the Networks and Technology Enforcement Section of the Antitrust Division. His responsibilities include investigating and prosecuting civil antitrust violations in the technology and finance industries.✠

The views expressed in this article are those of the author alone and are not purported to reflect those of the United States Department of Justice.