

Electronic
Discovery
Year-End
Update

2012

GIBSON DUNN

Moving
Beyond
Sanctions and
Toward
Solutions to
Difficult
Problems

January 14, 2013

2012 YEAR-END ELECTRONIC DISCOVERY AND INFORMATION LAW UPDATE

To Our Clients and Friends:

Moving Beyond Sanctions and Toward Solutions to Difficult Problems

Introduction

In our prior electronic discovery mid-year and year-end reports, the lead story was sanctions, as numerous decisions imposing onerous penalties for real or perceived e-discovery failures caught the attention of the legal community. By contrast, 2012 was the year of predictive coding, and of meaningful rules reform becoming an important step closer.

After garnering significant attention from the legal press and commentators, predictive coding became the subject of several published opinions in 2012. These initial decisions are likely the first steps toward embracing a technology that may, according to its proponents, significantly reduce the time and expense associated with e-discovery. On a macro level, the adoption of predictive coding and other forms of technology-assisted review has the potential to drastically alter the way in which documents are reviewed for production. Previously, however, in the absence of judicial approval, many litigants were unwilling to use this technology. That may well change now, following several decisions approving review methodologies involving predictive coding. Yet many questions remain. Will the technology fulfill its promise of more efficient, cost-effective and speedy review of large volumes of documents? Will it alter how litigation matters are staffed? Or is it merely the latest review technology that, while useful, neither obtains widespread adoption nor revolutionizes the landscape? These questions likely will be answered in the coming years and perhaps even as early as 2013, as more litigants use the technology. On a micro level, we expect that courts and parties increasingly will grapple with new issues relating to predictive coding, including questions about appropriate "seed sets," iterative training of the software, and quality control.

While advances in e-discovery technology are potentially game changing, so, too, are certain proposals for amendments to the Federal Rules of Civil Procedure, given the intense efforts toward reform throughout 2012. After nearly two and a half years of work, the federal Civil Rules Advisory Committee submitted a final proposal for a new federal sanctions rule for preservation failures to the Standing Committee on Rules of Practice and Procedure. The proposed revision to Federal Rule of Civil Procedure 37(e) seeks to limit the most serious sanctions for preservation failures--*e.g.*, case-terminating sanctions, issue or evidence preclusion, and adverse inference instructions--to those instances where the court finds that the failure to preserve was willful or in bad faith, or that the failure to preserve "irreparably deprived a party of any meaningful opportunity to present a claim or defense." The proposed rule also identifies several factors that a court should consider in determining whether a party failed to preserve discoverable information that reasonably should have been preserved, and whether the failure was willful or in bad faith. If adopted, the revised rule should help prevent the

imposition of harsh sanctions for inadvertent preservation failures. The Committee is also considering an amendment to Rule 26(b)(1) that would introduce the concept of proportionality into the permissible scope of discovery.

International e-discovery and the need to deal with foreign data protection and privacy law is another increasingly important trend. Several years ago, the cross-border transfer and disclosure of information in response to civil litigation and governmental investigations occurred far less often than today. The world continues to grow smaller as a result of commercial globalization and new technologies, which often increase the geographical scope of data that is relevant to litigation and investigations in the U.S. At the same time, foreign data protection and privacy laws have become pervasive and foreign data protection authorities more active in their enforcement of such laws. To assist litigants in navigating the conflicts that often arise between foreign data protection laws and U.S. discovery obligations, The Sedona Conference® issued in late 2011 its *International Principles on Discovery, Disclosure & Data Protection*. In 2012, the European Union's Article 29 Working Party--consisting of representatives of EU member state data protection authorities--responded favorably to the approach recommended in the *International Principles*.

Additionally, the European Commission in 2012 proposed replacing the 27 different data protection laws in each EU member state with a single data privacy regulation. The proposal includes provisions that companies likely will find appealing, such as only having to deal with one national data protection authority in the EU. Companies likely will find other proposed provisions less appealing, such as allowing individuals to require data controllers to delete all the individuals' online data (referred to as "the right to be forgotten"), and applying the EU rules on companies outside of the EU if they offer goods or services within the EU. Cloud computing has been an increasingly significant technological development, and EU bodies in 2012 addressed some of the legal issues associated with it. The European Commission also issued a communication stating its intention to facilitate the faster adoption of cloud computing within the EU because of cloud computing's potential to drastically reduce IT costs and to boost productivity, economic growth and jobs.

A shift in sanctions rulings also appeared to take place this year, as courts have gained more experience in dealing with alleged e-discovery failures and are more frequently favoring pragmatic solutions over punitive sanctions. Decisions have increasingly noted that remedial monetary sanctions, as well as other measures such as reopening discovery and hiring forensic analysts to search for spoliated data, are generally fairer and better at making the aggrieved party whole than punitive sanctions such as a default judgment. Consistent with that reasoning, in 2012 courts awarded monetary sanctions more than any other type of sanction for e-discovery failures. At the same time, the number of adverse inference sanctions awarded in 2012 exceeded that in 2011. Courts have taken care, however, to tailor such sanctions to the level of prejudice suffered by the injured party, often deferring a decision regarding an adverse instruction until after depositions have played out and the evidence that the parties intend to present to the jury has become clear. To the relief of many, case-terminating sanctions decreased this year, with courts only dealing that blow when bad faith drove the discovery misconduct and damage to the aggrieved party's case could not be cured with monetary sanctions or an adverse inference.

Parties' preservation obligations in advance of and at the outset of litigation continued to be a hot-button issue. Although new technological developments increasingly pose new challenges for preservation and collection in e-discovery (not to mention data security risks), courts in 2012 nevertheless still seemed more concerned with the extent to which a legal hold notice must be in writing, as opposed to only oral. Several decisions issued in 2012 show a continued move away from the bright-line holding in Judge Scheindlin's *Pension Committee* decision that an oral preservation notice is *per se* gross negligence--although the lack of a written notice is still likely to be viewed critically by a reviewing court, particularly when allegations of spoliation have been leveled. Also continuing a trend we have reported in the past several years, many decisions issued in late 2011 and in 2012 focused on precisely *when* a litigant's duty to preserve relevant evidence is triggered. Although most of these cases continued to consider when a defendant's duty to preserve arises, a few recent decisions have addressed when a plaintiff's duty to preserve arises. In these decisions, courts have held that a plaintiff's duty to preserve--like that of a defendant--arises when litigation is "reasonably foreseeable." Exactly when litigation is reasonably foreseeable, however, can be less than clear in practice.

In addition, the discoverability of social networking information--and relatedly, the obligation to preserve that information--continues to be an area where courts need to, and are, developing new and innovative ways to craft rules that properly account for the fluid nature of social networking sites. Specifically, in 2012, courts found themselves increasingly faced with difficult questions about the extent to which parties are obligated to preserve social media for and during litigation--and whether the modification of social media sites constitutes sanctionable spoliation. Obviously, to clamp down on the information flow on these sites for the sake of preserving material that is relevant to litigation could render them useless. At the same time, courts and litigants alike recognize that social media sites may contain information that is critical to parties' respective positions. With this in mind, one court this year even required a defendant in a trademark infringement case to recreate a Facebook page as it had previously existed, so that the Facebook page showed plaintiff in a photo that displayed "infringing trade dress." Courts also began to grapple with, and fashion different methods for determining, who is best positioned to collect the data contained on social media sites, some of which is publicly available, and some of which is protected by privacy settings. In addition, in 2012, courts increasingly focused on the related question of the extent to which social media information is authentic and reliable. In light of the distinct approaches so far, it remains to be seen how the law in this area will develop.

When The Sedona Conference® issued its *Cooperation Proclamation* in 2008, the concept of "cooperation" in litigation seemed to some to be utopian and unrealistic. Since then, cooperation--meaning sharing information and working collaboratively to address e-discovery challenges--has become integral in e-discovery pilot programs and standing orders; judicial decisions evaluating parties' preservation, review methodologies (including predictive coding), and whether to impose sanctions; in reform of the Federal Rules (*e.g.*, the proposed amendment to Rule 37(e) considers parties' cooperation as a factor in whether sanctions should be imposed); and in addressing the challenges of international e-discovery. In the past year, we increasingly saw a shift from broadly worded opinions addressing cooperation generally to a more narrow focus on specific issues, informed by a detailed review of the parties' e-discovery efforts. We expect this trend to continue. Although courts have continued to rebuke parties for their failure to cooperate, they are increasingly

concentrating on specific protocols, procedures, and agreements that can potentially minimize conflict early in the litigation process.

Similarly, 2012 saw the emergence of proportionality as an increasingly important--if underused--concept in e-discovery. It has explicitly been included in e-discovery pilot projects and standing orders, in proposed amendments to the Federal Rules of Civil Procedure, in cases evaluating predictive coding proposals, and in protocols for complying with foreign data protection laws in processing, reviewing and transferring information for production in U.S. litigation. Courts also continued in 2012 to limit broad ESI requests by considering the relevance of the data those requests likely would yield (through statistical sampling, for example), often limiting requests to certain time periods, specific custodians, and issues in dispute in the litigation.

Demonstrating that parties are often not availing themselves of the "no fault" claw back available with a Federal Rule of Evidence 502(d) order, privilege waiver issues--including whether the party facing a possible waiver took adequate steps to prevent and promptly rectify the inadvertent disclosure of privileged documents--frequently found their way to the courts in 2012. A clear, uniform definition of reasonable efforts to prevent the disclosure of privileged information under FRE 502(b) still has not emerged, and the decisions have been very fact-specific. Of particular note in 2012, some courts did not hesitate to find a waiver where they concluded that the producing party had not conducted a careful privilege review. Courts similarly found a waiver where the producing party failed to provide sufficient information to assess the reasonableness of that party's efforts to prevent disclosure of privileged information.

Finally, courts continued to focus more closely on the government's e-discovery obligations. It is becoming increasingly important for governmental entities--whether acting as a civil litigant, in an investigative or prosecutorial capacity, or as the custodian of public records--to have the proper practices in place to comply with e-discovery obligations. The failure to act appropriately could now result in sanctions, just as it would for a private litigant.

We invite you to review this update, which provides not only our analysis of e-discovery developments in 2012, but also our take on likely areas of interest in 2013. Recognizing that our report contains a lot of material, you may click on the links in the Contents list below to jump to particular topics.

*If you would like to **subscribe** to future E-Discovery updates and alerts, you may do so [here](#).*

Our past updates and alerts are available [here](#).

*Also, look out for our **2012 Year-End E-Discovery Update Webinar**, which will be announced soon. If you would like to request an invitation, you may do so [here](#).*

Contents

<u>Search Methodology (Predictive Coding)</u>
<u>E-Discovery Reform</u>
<u>International E-Discovery</u>
<u>Sanctions</u>
<u>Preservation</u>
<u>Social Media</u>
<u>Cooperation</u>
<u>Proportionality</u>
<u>Inaccessibility</u>
<u>Privilege</u>
<u>Governmental E-Discovery Obligations</u>
<u>Conclusion</u>

Search Methodology: Has Predictive Coding's Time Finally Come?

After receiving much attention (and enthusiasm) from commentators in recent years, the hot topic of predictive coding and computer-assisted review finally came before the courts in 2012, in a variety of circumstances with various outcomes--but all generally approving the use of predictive coding as a search methodology.

Predictive coding--also referred to as "computer assisted review" ("CAR") and "technology assisted review" ("TAR")--promises to significantly reduce the time and expense of reviewing large volumes of documents. In contrast with traditional "linear" review--which involves attorneys reviewing every document that hits a search term--predictive coding utilizes machine-learning technologies to categorize an entire set of documents as responsive or nonresponsive, based on human review of only a subset of the documents. While many litigants will still want to have attorneys review each document that is produced, predictive coding at a minimum allows parties either to eliminate from human review documents that the software has identified as likely to be irrelevant (subject to appropriate machine training and quality controls) or to prioritize review of those documents with the highest relevance scores. Because human review of all documents (even limited to those hitting search terms) can be extremely time consuming and expensive--by some estimates accounting for as much as 70 percent of all discovery costs--substantially reducing the number of documents that must actually be reviewed could significantly change the discovery process.

In perhaps the most widely followed case, Magistrate Judge Andrew J. Peck--a vocal advocate of computer assisted review[1]--approved a detailed predictive coding protocol and survived plaintiffs' subsequent recusal motion based on Judge Peck's alleged "appearance of partiality." [2] In *Da Silva Moore v. Publicis Groupe*, a class action employment case, the class alleged that defendant Publicis Groupe and its U.S. subsidiary MSL Group discriminated against female employees.[3] Following multiple discovery conferences with Judge Peck, the parties agreed in principle to an ESI protocol that included predictive coding.[4] Specifically, defendant MSL Group agreed to review and code a random sample of 2,399 documents "to determine relevant (and not relevant) documents for a 'seed

set' to use to train the predictive coding software." [5] To further train the software, MSL Group coded an additional 50 documents that they identified through keyword searching with Boolean connectors. [6] Using the same process, MSL Group then coded an additional 4,000 documents identified by keywords plaintiffs provided. [7] MSL Group further agreed to turn over to plaintiffs "[a]ll of the documents that are reviewed as a function of the seed set, whether [they] are ultimately coded relevant or irrelevant, aside from privilege." [8]

To "stabilize" the predictive coding software, MSL Group proposed using seven iterative rounds, *i.e.*, augmenting the "seed set" with additional examples of coded documents; "in each round they would review at least 500 documents from different concept clusters to see if the computer is returning new relevant documents." [9] After seven iterative rounds, MSL Group would review a random sample of 2,399 documents from documents coded by the computer as non-relevant to confirm that the documents determined by the software to be non-relevant were not, in fact, "hot"--or highly relevant--documents. [10] For each of these seven rounds and the final quality check, MSL Group agreed to turn over all of the documents reviewed to plaintiffs, except for privileged documents. [11] Over plaintiffs' objections, Judge Peck accepted MSL Group's proposal for seven iterative reviews, with the condition that additional reviews would be conducted if the parties did not agree that the software was stabilized after seven reviews. [12]

Judge Peck concluded:

[T]he use of predictive coding was appropriate considering: (1) the parties' agreement, (2) the vast amount of ESI to be reviewed (over three million documents), (3) the superiority of computer-assisted review to the available alternatives (*i.e.*, linear manual review or keyword searches), (4) the need for cost effectiveness and proportionality under [Federal Rule of Civil Procedure] 26(b)(2)(C), and (5) the transparent process proposed by MSL. [13]

Notably, considerations (2) through (4) may apply in many cases involving a large volume of electronic documents. Judge Peck added that MSL Group's "transparency in its proposed ESI search protocol made it easier for the Court to approve the use of predictive coding" because "such transparency allows the opposing counsel (and the Court) to be more comfortable with computer-assisted review, reducing fears about the so-called 'black box' of the technology." [14]

After Judge Peck's approval of MSL Group's proposed predictive coding protocol, plaintiffs filed objections to his order. [15] In overruling plaintiffs' objections and affirming Judge Peck's rulings, District Judge Andrew L. Carter echoed Judge Peck's focus on transparency in the predictive coding process, observing that MSL Group's "ESI protocol contains standards for measuring the reliability of the process and . . . builds in levels of participation by Plaintiffs," and also "provides that the search methods will be carefully crafted and tested for quality assurance, with Plaintiffs participating in their implementation." [16] Thus, Judge Carter rejected plaintiffs' contention that the ESI protocol would "deny Plaintiffs access to liberal discovery." [17] Likewise, Judge Carter rejected plaintiffs' arguments regarding the reliability of the predictive coding protocol as "premature," noting that Judge Peck "has ruled that if the predictive coding software is flawed or if Plaintiffs are not receiving the types of documents that should be produced, the parties are allowed to reconsider their methods and raise their concerns with the Magistrate Judge." [18]

Following Judge Carter's affirmance of Judge Peck's order approving MSL Group's predictive coding protocol, plaintiffs moved to recuse or disqualify Judge Peck based on "an appearance of partiality." [19] Specifically, plaintiffs asserted that Judge Peck's recusal was required because of his "public comments concerning the case," his "participation on pro-predictive coding panels with [MSL Group] defense counsel," his "numerous speaking engagements in favor of predictive coding, which were at least indirectly sponsored by [MSL Group's discovery vendor] and other e-discovery vendors," and his alleged failure to disclose these activities. [20] Judge Peck denied plaintiffs' recusal motion finding it both untimely and meritless, [21] and Judge Carter affirmed. [22] Judge Carter noted that "it is undisputed that the parties agreed to defendants' use of predictive coding and only disagreed on the scope and implementation. Predictive coding does not inherently favor one party over the other in this case." [23] Thus, Judge Carter concluded that Judge Peck's "decision accepting computer-assisted review . . . was not influenced by bias, nor did it create any appearance of bias." [24] "Moreover, Judge Peck's participation in CLE conferences and his relationship to an attorney in the defendant's firm do not warrant recusal." [25]

Although it was certainly the most watched, *Da Silva Moore* was not the only predictive coding case in 2012. In *Global Aerospace Inc. v. Landow Aviation, L.P.*, a multi-party action arising from the collapse of three hangars at Dulles Jet Center, defendants moved for a protective order approving the use of predictive coding to review approximately 250 gigabytes of ESI, which they estimated to equate to more than two million documents. [26] Defendants asserted that, "[a]t average cost and rates of review and effectiveness, linear first-pass review would take 20,000 man hours, cost two million dollars, and locate only sixty percent of the potentially relevant documents." [27] By contrast, predictive coding would--according to defendants--locate "upwards of seventy-five percent of the potentially relevant documents," at a fraction of the cost and in a fraction of the time of a traditional linear review. [28] Defendants proposed a coding protocol that would ensure recall--i.e., the fraction of relevant documents that are identified by a search--of at least 75%, and would give opposing counsel access to documents reviewed in the training, stabilization, and validation processes (with the exception of privileged and sensitive irrelevant documents). [29]

Plaintiffs opposed the motion, arguing that defendants' estimate of the potential review population was overstated because they "copied every file from every computer" without any "attempt to separate the files pertaining to the Dulles Jet Center from the files pertaining to [defendants'] many other business and personal ventures" and, thus, traditional linear review of the files generated by the potential custodians "simply is not an unmanageable task." [30] The Court overruled plaintiffs' objections and granted defendants' request, but made its order without prejudice to any party raising an issue as to the completeness or contents of defendants' document production or the continued use of predictive coding. [31]

Significantly, defendants were not the only proponents of predictive coding technology in 2012. In *Kleen Products LLC v. Packaging Corp. of America*, a consolidated antitrust action alleging that defendants conspired to fix prices in the containerboard industry, plaintiffs sought to require their adversaries to use "content-based advanced analytics" technology--a form of predictive coding--rather than the "antiquated Boolean search of [defendants'] self-selected custodians' ESI and certain central files" that defendants already had in place (and had used to produce documents). [32] Defendants objected to plaintiffs' proposal, arguing that it would require them to "jettison their previous work

product and adopt [a] new, untested document gathering and production protocol." [33] The dispute in *Kleen Products* culminated in two days of evidentiary hearings before Magistrate Judge Nan R. Nolan, during which plaintiffs' consultants testified regarding the efficacy of their proposed predictive coding protocol, and defendants' consultants testified regarding the discovery protocol already in place, including the development, testing, revision, and validation of defendants' keyword search terms. [34]

Judge Nolan ultimately declined to require defendants to adopt one technology over another and instead ordered the parties to meet and confer regarding modifications to the keyword search methodology that defendants already had in place. [35] That defendants had already substantially completed their review and plaintiffs were seeking to have them redo it using a predictive coding methodology factored significantly into this outcome. Judge Nolan also relied on Principle 6 of *The Sedona Principles*, [36] which states, "[r]esponding parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own electronically stored information." [37] The parties ultimately reached a stipulation by which plaintiffs withdrew their demand that defendants apply predictive coding for the first corpus of documents, but reserved the right to raise objections to defendants' search methodology--including the completeness of defendants' productions--and to propose alternative methodologies for later requests for production. [38]

This past year also saw the approval of a predictive coding protocol pursuant to stipulation. In *In re Actos (Pioglitazone) Products Liability Litigation*, the parties agreed to a detailed predictive coding protocol for the search and review of ESI collected from defendant Takeda Pharmaceutical Company Limited's electronic data sources. [39] Each side agreed to nominate three experts to collaboratively train the predictive coding software based on sample custodial and non-custodial populations. [40] The agreed-upon protocol also set forth procedures for stabilization and pre-review quality control of the predictive coding software, and post-review sampling of documents not produced after predictive coding. [41] The parties agreed to "meet and confer in good faith to resolve any difficulties and finalize the method for searching documents on a going forward basis," thus obviating the need for detailed court involvement in the predictive coding process. [42] District Judge Rebecca F. Doherty granted the parties' stipulation, thus formalizing the agreed-upon predictive coding protocol.

Another court *sua sponte* ordered the use of predictive coding in 2012. In *EORHB, Inc. v. HOA Holdings LLC*, an indemnification dispute related to the purchase of the Hooters restaurant chain, Delaware Court of Chancery Vice Chancellor J. Travis Laster *sua sponte* ordered the parties to use predictive coding or, alternatively, to show cause why predictive coding should not be used. [43] Vice Chancellor Laster reasoned:

The problem is that these types of indemnification claims can generate a huge amount of documents. That's why I would really encourage you all, instead of burning lots of hours with people reviewing, it seems to me this is the type of non-expedited case where we could all benefit from some new technology use. [44]

Vice Chancellor Laster also ordered the parties to pick a single discovery provider to warehouse both sides' documents, specifically, "one of these wonderful discovery super powers that is able to maintain the integrity of both [sides'] documents and insure that no one can access the other side's information." [45] This aspect of Vice Chancellor Laster's decision may give rise to concerns about the

confidentiality of each party's communications with the vendor. It remains to be seen whether Vice Chancellor Laster's decision to order the parties to use predictive coding and a single discovery vendor will motivate other courts to take similar actions.

U.S. District Judge Shira A. Scheindlin, influential in the e-discovery area as the author of the *Zubulake* opinions, has expressed her approval of predictive coding, albeit in *dicta*. In connection with the *National Day Laborer* case, which previously received attention for Judge Scheindlin's discussion of metadata production, Judge Scheindlin pointed out perceived shortcomings in keyword searches and explained:

There are emerging best practices for dealing with these shortcomings and they are explained in detail elsewhere. There is a "need for careful thought, quality control, testing, and cooperation with opposing counsel in designing search terms or 'keywords' to be used to produce emails or other electronically stored information." And beyond the use of keyword search, parties can (and frequently should) rely on latent semantic indexing, statistical probability models, and machine learning tools to find responsive documents. Through iterative learning, these methods (known as "computer-assisted" or "predictive" coding) allow humans to teach computers what documents are and are not responsive to a particular FOIA or discovery request and they can significantly increase the effectiveness and efficiency of searches. In short, a review of the literature makes it abundantly clear that a court cannot simply trust the defendant agencies' unsupported assertions that their lay custodians have designed and conducted a reasonable search.[46]

These decisions may be just the tip of the iceberg in a possible trend towards growing judicial recognition of--and receptiveness to--the potentially game changing technology of predictive coding. Depending in part on the success (or failure) of predictive coding in the cases discussed above and others, judicial recognition of computer-assisted review technology may continue to build in 2013. Any party desiring to use predictive coding might be wise to learn from the parties' mistakes and successes in these early cases.

Finally, predictive coding and other technologies will increasingly factor into discussions and disputes regarding burden and proportionality. Anecdotally, we have seen not only companies faced with burdensome and expensive discovery interested in using predictive coding because of its potential for cost savings, but also plaintiffs in asymmetrical litigation promoting it in response to--or as a means of avoiding--defendants' arguments regarding burden and the time needed to complete review and produce large document sets. Indeed, while on the one hand the Civil Rules Advisory Committee is considering including the concept of proportionality in the Federal Rules' description of the permissible scope of discovery in Rule 26(b)(1)--see our discussion in the Reform section below--on the other hand The Sedona Conference® in its recently issued post-public comment version of its *Commentary on Proportionality in Electronic Discovery*[47] includes as one of its six proportionality principles that "Technologies to reduce cost and burden should be considered in the proportionality analysis." [48]

Litigants and courts will therefore need to be vigilant in preventing the use of such technologies from becoming a justification for expanding the scope of discovery beyond an appropriate focus on

documents relevant to the issues in dispute, and thereby exacerbating the very problems that the technologies seek to address.

[Back to top](#)

E-Discovery Reform: Significant Progress Toward Retooling a Flawed Process

Critics of the e-discovery *status quo* have been heard loud and clear, and while significant reform is not here yet, it appears that real and meaningful progress is being made toward rule amendments addressing sanctions and unduly burdensome discovery.

Reform of Federal Rules Make Significant Progress

The federal Civil Rules Advisory Committee continued to work to address issues related to preservation and sanctions raised at the 2010 Duke Conference. The Committee made significant progress this past year, and on November 2, 2012 unanimously voted to present a new sanctions rule related to preservation to the Standing Committee on Rules of Practice and Procedure.[49] After consideration of the proposal, the Standing Committee may refer it to the Judicial Conference for submission to the Supreme Court for final approval. The proposed sanctions rule reflects nearly two and one-half years of Committee work and the input of individuals and organizations such as The Sedona Conference®.[50]

Earlier discussions about a rule regarding sanctions and preservation focused on adding a new Rule 37(g), but the Committee decided instead to focus on amending Rule 37(e), which currently provides that absent exceptional circumstances a party cannot be sanctioned for failing to produce electronically stored information lost as a result of the routine, good faith operation of an information system.[51] The proposed rule revision would replace that language with language limiting the most serious sanctions for preservation failures--*e.g.*, case terminating sanctions, issue or evidence preclusion, and adverse inference instructions--to those instances where the court finds that the failure to preserve was willful or in bad faith, or that the failure to preserve "irreparably deprived a party of any meaningful opportunity to present a claim or defense." [52] One of the goals of the proposed rule is to "overturn the decision of the Second Circuit in *Residential Funding Corp. v. DeGeorge Fin. Corp.*, 306 F.3d 99 (2d Cir. 2002), which authorized sanctions for negligence."

The proposed rule sets forth several factors that a court should consider in determining whether a party failed to preserve discoverable information that reasonably should have been preserved, and whether the failure was willful or in bad faith: (a) the extent to which the party was on notice that litigation was likely and that the information would be discoverable; (b) the reasonableness of the party's efforts to preserve the information, including the use of a litigation hold and the scope of the preservation efforts; (c) whether the party received a request that information be preserved, the clarity and reasonableness of the request, and whether the person who made the request and the party engaged in good-faith consultation regarding the scope of preservation; (d) the proportionality of the preservation efforts to any anticipated or ongoing litigation; and (e) whether the party sought timely guidance from the court regarding any unresolved disputes concerning the preservation of discoverable information. A version of proposed Rule 37(e) is available in the Committee Materials.[53] During its November

meeting, the Civil Rules Advisory Committee decided to remove as a factor "the party's resources and sophistication in litigation." [54]

Beyond the proposed sanctions rule, the Civil Rules Advisory Committee continues to focus on other ways to reform the discovery process so as to be less onerous on litigants. The Duke Conference Subcommittee of the Civil Rules Advisory Committee is focusing on three main areas: (1) early stages of establishing case management; (2) scope of discovery; and (3) establishing cooperation among parties. [55] It is considering a variety of potential rules changes, including revising the language of Rule 26(b)(1) from permitting discovery of "information that appears reasonably calculated to lead to the discovery of admissible evidence" to instead "provide only that information need not be admissible in evidence to be discoverable." [56] Also under consideration is including the concept of proportionality within the description of the permissible scope of discovery, limitations on the number of requests for admission to 25 (except for those regarding authenticity of documents), a reduction in the number of depositions allowed per side from ten to five, and limiting the length of each deposition from seven to six hours. [57] There is also discussion about permitting parties to serve discovery requests before the Rule 26(f) conference. [58] Finally, to promote cooperation, the Duke Conference Subcommittee is considering amending Rule 1 in a manner that more clearly makes cooperation a goal. [59]

Additionally, the House Judiciary Committee Subcommittee on the Constitution has acknowledged that e-discovery issues are an area of potential concern for business. On December 13, 2011, it held a hearing on the "Costs and Burdens of Civil Discovery," following which two letters, one from the subcommittee majority members and one from the minority members, were sent to Judge Mark R. Kravits, Chairman of the U.S. Judicial Conference Committee on Rules of Practice and Procedure, and Judge David G. Campbell, Chairman of the Civil Rules Advisory Committee. Both letters express concern over the current state of e-discovery in complex civil litigation. The letter from the majority members states that a proposed rule should limit the scope of discovery to information that is relevant and material to the claims and defenses in each case, that ordinary business practices of an organization should guide court's expectations, greater cost-shifting should be employed, and rules should encourage parties to police themselves and focus on the most efficient means to obtain truly critical evidence. [60] The letter from the minority members expresses greater apprehension toward change, and urges the Rules Advisory Committee take into account "the tremendous benefit that discovery provides" as it considers "whether reform is needed."

Overall, the proposed rule amendment limiting sanctions for preservation failures along with other proposals before the Civil Rules Advisory Committee indicate that meaningful progress is being made toward limiting the circumstances under which courts can impose onerous sanctions and providing litigants and courts with tools to streamline unduly burdensome discovery.

Congressional Attempts to Promote Increased Privacy

On November 29, 2012, the Senate Judiciary Committee voted to advance to the Senate H.R. 2471, 112th Cong., a bill that would amend the 1986 Electronic Communications Privacy Act ("ECPA") and the ("VPAA"). [61] Currently, the ECPA permits the government to engage in warrantless discovery of emails stored on a service providers' server for more than 180 days. If H.R. 2471 is enacted into law as

it currently stands, the "180-day rule" will be eliminated, and instead a warrant, based on a showing of probable cause, will be required in order for law enforcement to obtain emails from a service provider.[62]

The bill would also require disclosure to the customer or subscriber that records were collected by law enforcement or another government entity.[63] If law enforcement obtained the records, the disclosure must be made within ten days; if any other governmental entity obtained the records, the disclosure must be within three days.[64] The bill provides for delayed notification of up to 180 days if the warrant applicant can show potential risks to the investigation or danger to others that would result from notification.[65]

As we have previously reported, there have been calls to reform the ECPA over the past several years, and during the past two years Senator Patrick Leahy has twice introduced proposals to reform the ECPA.[66] The effort to reform the ECPA has been met with resistance from law enforcement officials based on concerns that it will hinder criminal investigations.[67] While the New York Times reports that the "bill is not expected to make it through Congress this year and will be the subject of negotiations next year," in our view, the movement of the bill out of committee represents progress towards greater data privacy protections.[68] As H.R. 2471 provides exemptions from the notice requirement, however, it is quite possible that end users may remain unaware that law enforcement is collecting and reviewing their data.

State and Local Rulemaking

In our last update, we reported that state courts and bar associations had continued to propose and adopt rule amendments designed to govern e-discovery. In that update, we highlighted proposed amendments that were being considered by the Pennsylvania Supreme Court. These amendments, which were adopted on June 6, 2012, and took effect on August 1, 2012, govern the process of requesting and producing electronically stored information.[69]

Breaking with the trend of states following the Federal Rules, the Pennsylvania Supreme Court chose to reject the federal jurisprudence, noting in its explanatory comments that "there is no intent to incorporate the federal jurisprudence surrounding the discovery of electronically stored information." [70] Rather, the comments instruct Pennsylvania courts to continue to apply a proportionality analysis, as was previously required under Pennsylvania law, when determining whether e-discovery is appropriate.[71] Additionally, the Pennsylvania Rules of Civil Procedure still do not expressly protect (1) against demands for data that are "not reasonably accessible," or (2) against sanctions for the inadvertent destruction of data.

Florida also amended its rules of civil procedure to address e-discovery issues. On July 5, 2012, the Florida Supreme Court adopted all seven proposed amendments, which require parties to discuss potential e-discovery issues at the outset of a case, and set out rules governing requests for and the production of ESI.[72] These amendments, which took effect on September 1, 2012, generally mirror the Federal Rules of Civil Procedure. One significant difference from the Federal Rules is that Florida has continued the trend of states declining to implement a mandatory meet-and-confer requirement. A second difference is that Florida's Rule 1.201 provides special e-discovery rules for parties involved in

"complex litigation," which is defined as a case that is "likely to involve complicated legal or case management issues and that may require extensive judicial management to expedite the action, keep costs reasonable, or promote judicial efficiency." [73] In such cases, the parties must now meet prior to the initial case management conference in order to discuss the possibility of an agreement governing the discovery of electronically stored information.

Various jurisdictions have also been addressing e-discovery in less formal ways. On September 10, 2012, for example, New York approved a "pilot program" requiring parties to meet-and-confer before their initial case management conference and to fill out a joint proposed Electronic Discovery Order. [74] An Electronic Discovery Order must outline the anticipated need for and extend of e-discovery in a case, as well as any potential e-discovery issues that might arise during the litigation. At the moment, the pilot program is limited to those cases filed after June 15, 2011, in Part 48 of the New York Supreme Court's Commercial Division. [75]

New York's pilot program is similar to other pilot programs recently implemented in various federal jurisdictions. Notably, the U.S. District Court for the Southern District of New York implemented a similar pilot program in November 2011 (the "SDNY program"). [76] The SDNY program requires a joint e-discovery submission and proposed order that is similar to the Electronic Discovery Order required in the New York Superior Court pilot program. The SDNY program also requires parties to discuss e-discovery during the initial case management conference. [77] At the moment, the SDNY program is currently limited to "complex civil cases," which includes class actions, multi-district litigation, or cases involving certain areas of law specified in the court's standing order. [78]

Most recently, on November 27, 2012, the Northern District of California approved a revised standing order that is similar to New York's pilot program. [79] The Northern District of California program includes an e-discovery "checklist" to be used in connection with the initial Rule 26(f) conference. [80] This checklist lists a series of issues that the parties are urged to resolve at the outset of a litigation, including preservation of ESI, proportionality and costs, production formats, and privilege issues. The Northern District of California program also includes a set of guidelines suggesting how parties might cooperate to resolve e-discovery disputes. [81] Finally, the program includes a model stipulated order [82] that parties are "encouraged to use . . . as the foundation for the Rule 26(f) meet-and-confer process." [83] The model order contains provisions that would govern most of the e-discovery issues identified in the Northern District's e-discovery checklist.

The Northern District of California noted in its press release its "hope[]" that the Model Stipulated Order will be a widely used tool for litigants just as the court-approved Stipulated Protective Orders have been in patent and other cases." [84] The Northern District of California program apparently applies to all civil cases filed in the Northern District of California. While the steps recommended in the program are not mandatory, the district does "require counsel to be familiar with [the program] and confirm in the initial case management statement that they have reviewed the Guidelines regarding preservation and decided whether to enter into a stipulated order governing e-discovery." [85]

In the coming year, we anticipate that states and federal courts in their local rules and standing orders will continue to update their rules to address various e-discovery issues. Massachusetts, for one, will

likely implement e-discovery rules, which it has been considering since early 2011.[86] We will report on additional developments in client alerts and in our 2013 Mid-Year Update.

[Back to top](#)

International E-Discovery: It's A Small World

One of the most significant recent developments in e-discovery has been how increasingly common the need to preserve, collect and review ESI located in foreign jurisdictions has become. Several years ago, the cross-border transfer and disclosure of information in response to civil litigation and governmental investigations was far less frequent than it is today. Rapidly increasing commercial globalization combined with rapid technological change, the ease of transferring and storing data across traditional geographic borders, and the explosion of data volumes has changed the discovery landscape tremendously.

As The Sedona Conference® put it in its recently published *International Principles on Discovery, Disclosure & Data Protection*, "[t]oday, an employee from a Toronto company can conduct business from a cafe in Paris, while sending electronic messages to customers in Dubai that attach documents from 'cloud' servers located in Singapore, Dallas, and Amsterdam." As a result, "agreements among nations concerning cross-border discovery"--such as the Hague Convention--"made in the age before personal computers and the Internet" (not to mention smart phones, tablets and other devices) "are now severely outdated." [87]

Since the U.S. Supreme Court's 1987 ruling in *Aérospatiale* that litigants are not necessarily required to use the procedures of the Hague Convention to obtain discovery in foreign jurisdictions, U.S. courts have in many circumstances held that parties' discovery obligations under the Federal Rules of Civil Procedure include collecting, reviewing and producing documents and information located abroad without the requesting party being limited to the procedures of the Hague Convention. During the same period of time, foreign nations--most notably in the European Union, but also in virtually all geographical regions--have increasingly enacted data privacy laws and "blocking" statutes. The resulting conflicts between U.S. discovery obligations and foreign laws restricting the processing and transfer of information have created significant challenges for litigants.

EU Reaction to The Sedona Conference's International Principles

Given the generally cool reception of European Union data protection authorities in the past to U.S. discovery, their positive reaction in 2012 to *The Sedona Conference® International Principles on Discovery, Disclosure & Data Protection*, published in December 2011, was a noteworthy development.

International e-discovery is one of several areas in which The Sedona Conference® has provided particularly useful guidance for those dealing with e-discovery issues. In 2008, The Sedona Conference's Working Group on International Electronic Information Management, Discovery and Disclosure (also known as "Working Group 6" or "WG6") published *The Sedona Conference® Framework for Analysis of Cross-Border Discovery Conflicts*, which among other things provided a framework for analyzing and potentially resolving (or at least minimizing) conflicts between the need

to gather relevant information from foreign jurisdictions, on the one hand, and data privacy regulations and blocking statutes that restrict or block such discovery, on the other. WG6 has since invited data protection regulators to participate in its meetings and conferences, and it has actively engaged the EU's "Article 29 Working Party on Personal Data Protection," made up of representatives from all 27 EU member nation data protection authorities, in sharing ideas and developing potential solutions to the potential conflicts between U.S. discovery obligations and EU data privacy law. That process ultimately led to The Sedona Conference's publication of the *International Principles* in late 2011--the current version of which is subtitled "European Union Edition" because of its focus on EU data protection requirements (The Sedona Conference® plans to publish additional editions focused on other regions).

The *International Principles* sets forth six principles--along with helpful commentary--regarding management of the conflicts that may arise in cross-border discovery: (1) that courts and parties should demonstrate due respect to foreign data protection laws; (2) where full compliance with both foreign data protection laws and discovery obligations are in conflict, courts and data protection authorities should judge a party's conduct under a standard of good faith and reasonableness; (3) preservation and discovery of protected data should be limited to that which is relevant and necessary to support any party's claim or defense; (4) protective orders should be employed to protect the confidentiality of protected data; (5) producing parties should be prepared to demonstrate that they have addressed data protection obligations and instituted data protection safeguards; and (6) protected data should only be retained as long as necessary.

Additionally, the *International Principles* envisions a three-stage approach for parties seeking to avoid or minimize conflicts that might otherwise arise between U.S. discovery and foreign data protection laws: (1) using a stipulation or protective order from the U.S. court to provide special protection for data covered by the foreign data protection laws; (2) phasing discovery so there is time to implement data protection processes and to determine whether the same or substantially similar information is available from the non-protected sources; and (3) implementing a "legitimization plan" to maximize both compliance with foreign data protection laws and U.S. discovery obligations. The Sedona Conference® has included as appendices to the *International Principles* a model stipulated protective order and a sample transfer protocol that can be used to provide evidence of the steps taken to best comply with applicable data protection laws in processing and transferring the data.

In a letter to the leaders of WG6 dated June 12, 2012, the Article 29 Working Party stated that it had "with great pleasure" taken note of *International Principles*--a remarkably enthusiastic response by the standards of typical EU data protection authority pronouncements. It further stated that the *Principles* are an "important step towards bridging the gap between the different legal systems on civil procedure and data protection which exist in Europe and the U.S. in practice." The letter noted that Principle 3--regarding the importance of necessity and proportionality in processing and transferring protected data--is "the most important one from a European point of view" and added that it "echoes the position taken by the Working Party that any filtering of data prior to discovery should be carried out locally in the European country in which the personal data is found." The letter includes several caveats, including that employee data such as email may be afforded greater protections in Europe and that an employee's consent "is a questionable basis for disclosing his or her personal data" (but also noting that the separation of workplace and private email may provide a solution). The letter concluded that the

Working Party shares the view "that through cooperation conflicts of law and their practical effects can and should be minimized."

Further European Union Developments

Further developments in the EU include the Article 29 Working Party's issuance in July 2011 of its Opinion 15/2011, which provides a thorough analysis of the concept of "consent" in EU data privacy law, and a proposal in January 2012 for comprehensive reform of the European data protection framework. That framework dates back to 1995, when the EU issued its Directive 95/46/EC, which has been very influential in inspiring data protection legislation in jurisdictions outside of the EU. The Directive seeks to protect the privacy of individuals while allowing the free movement of personal data within EU member states. But it restricts the transfer of personal data to nations that do not ensure an "adequate level of protection" (the EU considers the U.S. to be such a jurisdiction).

The Directive requires each EU member state to enact legislation consistent with its provisions and to establish a supervisory authority to monitor and enforce compliance. Article 29 of the Directive set up a "Working Party" comprised of representatives of each member state's data protection authority. This Article 29 Working Party is an independent advisory body responsible for, among other things, making recommendations and issuing opinions regarding the processing of personal data in the EU.

With respect to the processing and transfer of data for purposes of litigation, the Article 29 Working Party in February 2009 issued Working Document 1/2009 on pre-trial discovery for cross border civil litigation (also known as "WP 158"). WP 158 provides guidelines for trying to reconcile the demands of the litigation process in foreign jurisdictions with the data protection obligations of Directive 95/46. It recognizes that there are three potential grounds for legitimacy under the Directive for processing personal data (which is defined very broadly) for litigation purposes: (1) where the data subject has provided consent, (2) that it is necessary for compliance with a legal obligation, or (3) that it furthers a legitimate interest of the data controller or the party to whom the data is disclosed.

After pointing out limitations and complexities in relying upon consent of the data subject, and that an obligation imposed by foreign law may not qualify as a "legal obligation" in EU member states, the Working Party recognized that compliance with the requirements of a foreign litigation process may be "necessary for the purposes of a legitimate interest"--i.e., promoting or defending a legal right--provided that these interests are not overridden by the "rights and freedoms of the data subject who has no direct involvement in the litigation process." The Working Party stated that balancing those interests "should take into account issues of proportionality, the relevance of the personal data to the litigation and the consequences for the data subject." Among steps that can be taken, the Working Party stated, are reviewing the data within the EU to cull out irrelevant material so that a much more limited data can be disclosed outside the EU and, if possible, "anonymising" or "pseudonymising" the data--a potentially burdensome and perhaps not possible task if that means redacting names or other personal information.

In mid-2011, the Article 29 Working Party issued its Opinion 15/2011 on the meaning of "consent" for purposes of Directive 95/46 and Directive 2002/58/EC, as amended by Directive 2009/136/EC, concerning the processing of personal data and the protection of privacy in the electronic

communications sector (the "e-Privacy Directive"). Highlights of the Opinion include the following: (1) that consent requires an unambiguous, affirmative indication signifying that the data subject's agreement to the processing of his or her personal data; (2) that the consent be freely given, *i.e.*, that it is "a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences if he or she does not consent"; (3) that the consent should be specific and specify the exact purpose of the processing; and (4) that the data subject should be fully informed of how his or her data will be treated. *For more information about Opinion 15/2011, see our client alert [here](#).*

More recently, in January 2012 the European Commission proposed fundamental reform of the EU data protection framework through a single, comprehensive regulation that would supersede Directive 95/46. Under the existing framework, each EU member state is allowed to enact its own data protection legislation pursuant to the principles of the Directive. That has led to 27 somewhat differing laws, along with significant differences in member states' interpretation and enforcement of their laws. The Commission seeks instead to have a uniform set of rules, although the data protection authority of each member state would still enforce them. The Commission also seeks to "modernise" data privacy rules to deal with the rapid technological developments--*e.g.*, social networking, cloud computing, location-based services and smart cards) and globalization that have occurred since Directive 95/46 was issued 17 year ago.

In addition to a single set of rules, provisions in the reform proposal include: (1) a "right to be forgotten" providing individuals with the ability to require companies to delete their online data; (2) the right to transfer personal data from one service provider to another; (3) requiring data controllers to notify data subjects of data breaches without undue delay and within 24 hours where feasible; (4) application of the EU rules to companies outside of the EU if they offer goods or services in the EU or monitor the online behavior of EU citizens; (5) providing that companies will only have to deal with a single national data authority (in the EU state where the company has its main establishment); and (6) strengthened national data protection authorities.

When and to what extent the proposed reform will be enacted remains to be seen. It appears unlikely that draft legislation will be ready by the targeted April 2013 date. Some of the provisions are highly controversial and would be difficult to implement--for example, the "right to be forgotten." But there is consensus that the current framework, with its 27 different laws and inconsistent enforcement, needs to be reformed to achieve greater consistency across the EU. We expect that there will ultimately be a uniform regulation, although it may not be in 2013 and it may be significantly different from what has been proposed to date. *For more information on the proposed EU data protection regulation, see our alert [here](#).*

Cloud computing has been an increasingly significant technological development, and EU bodies in 2012 addressed some of the legal issues associated with it. On July 1, 2012, the Article 29 Working Party issued its Opinion 05/2012 on Cloud Computing, which provides guidance on controlling law in the context of cloud computing. The Opinion explains that the cloud client is the data controller, and the location of the cloud client determines jurisdiction. If the cloud client is "established in various Member States, processing the data as part of its activities in these countries, the applicable law shall be that of each of the Member States in which this processing occurs." This means that the centralization of data storage does not necessarily result in centralization of applicable data protection

law. Opinion 05/2012 also emphasizes that cloud providers must ensure "fair and legitimate processing of personal data," consistent with EU data privacy law, with an emphasis on transparency.

Finally, in September 2012, the European Commission issued a communication entitled *Unleashing the Potential of Cloud Computing in Europe*, in which the Commission states that it seeks to enable and facilitate the faster adoption of cloud computing because of its potential to "slash users' IT expenditure" and to boost productivity, growth and jobs. To achieve those goals, the Commission identified three "key actions" that it intends to take: (1) cutting through the "jungle of standards" imposed by individual cloud vendors and implementing uniform standards and certification; (2) requiring "safe and fair" contract terms and conditions to address the problem of insufficiently specific and imbalanced contracts with cloud providers; and (3) setting up a "European Cloud Partnership" to provide an umbrella for the initiatives of member states to shape the cloud computing market by exercising the public sector's ability as the EU's largest purchaser of cloud services to influence such matters as features, performance, security, data portability and technical requirements.

The Commission's communication on cloud computing, along with the proposal for a uniform data privacy regulation, provides hope for a more consistent approach to data protection within Europe. The Commission expressly recognized in its communication that the "fragmentation . . . due to differing national legal frameworks and uncertainties over applicable law" is a key area of concern for the commercially effective use of cloud computing. Recognizing the global nature of cloud computing the Commission set forth as a policy goal that it will "build on its on-going international dialogues with the USA, India, Japan and other countries, as regards, *inter alia*, key themes related to cloud services . . . , such as data protection; access to data by law enforcement agencies and the use of Mutual Legal Assistance Agreements to avoid confronting companies with conflicting requests from public authorities"

We will continue to follow the developments in Europe and report on the direction of reform in our future updates. *For an update regarding specific developments in Germany, see the data protection discussion in our Year-End German Law Update [here](#).*

Expansion of Foreign Data Protection Legislation

There has been an increasing global trend toward greater data privacy and protection. According to a recent study, the number of data privacy laws globally had reached 89 by February 2012.[88] And the growth in new laws has been accelerating over the past four decades--eight in the 1970s, 13 in the 1980s, 21 in the 1990s, 35 in the 2000s, and 12 in just the first two years of the 2010s.[89]

The geographical distribution of the 89 laws by region is also diverse, with the greatest concentration in Europe. The number of laws in different regions is as follows: EU member states (27); other European nations (23); Asia (9); Latin America (8); Africa (8); North Africa/Middle East (5); Caribbean (4); North America (2); Australasia (2); Central Asia (1); Pacific Islands (0).[90]

In 2012, there also was either draft or pending legislation in at least ten nations, and others have expressed an intention to draft such legislation. Thus, it is increasingly likely--indeed, almost certain--that parties in U.S. litigation where ESI is located overseas will need to navigate potentially conflicting U.S. discovery obligations and foreign data protection laws.

U.S. Judicial Developments

The U.S. judicial framework for analyzing cross-border discovery disputes is based on the Supreme Court's 1987 *Aérospatiale* decision, in which the Court held that litigants in the U.S. are not bound to utilize the procedures of the Hague Convention to obtain discovery in foreign jurisdictions. The Supreme Court, relying on the Restatement (Third) of Foreign Relations, held that in deciding whether to issue an order pursuant to the Federal Rules of Civil Procedure directing production of information located abroad instead of using the Hague Convention, the U.S. court should consider the following factors: (1) the importance to the investigation or litigation of the information requested; (2) the degree of specificity of the request; (3) whether the information originated in the United States; (4) the availability of alternative means of securing the information; and (5) the extent to which noncompliance with the request would undermine important interest of the United States, or compliance with the request would undermine important interests of the nation-state where the information is located.

Some U.S. courts have demonstrated a willingness to show some deference to foreign data privacy laws if litigants could articulate, and provide evidentiary support for, a significant foreign interest in data privacy, and also demonstrate that the foreign interest outweighed the U.S. litigants' need for the information. But the rulings are far from consistent, as demonstrated by two directly conflicting decisions out of the Southern District of New York involving the same Chinese bank secrecy laws. The court in *Tiffany (NJ) LLC v. Forbse*, relied in part on a November 2011 letter from Chinese bank regulatory agencies in finding that China's interest in enforcing its bank secrecy laws was sufficient to justify use of the Hague Convention for discovery from two nonparty banks (it also found that for a third nonparty bank, the requesting party's interest in the data outweighed the foreign privacy interest).[91] By contrast, in *Gucci Am. Inc. v. Weixing Li*, the court denied nonparty Bank of China's motion to reconsider an order directing it to comply with a Rule 45 subpoena, even where it argued that bank-secrecy laws prevented disclosure and provided the court with the same November 2011 letter from Chinese bank regulatory agencies that the *Tiffany* court had relied upon.[92]

Simply stating that a blocking statute or data privacy law exists continued to be insufficient evidence, in the view of many courts, to justify limiting discovery or to persuade the court to resort to the procedures of the Hague Convention.[93] And while courts have been willing to consider comity interests, U.S. courts may refuse to recognize the foreign interest as legitimate when a foreign nation fails to actively promote and pursue those interests. For example, in *Wultz v. Bank of China Ltd.*[94], the parties had originally agreed to rely on the Hague Convention to conduct discovery from the Bank of China to address concerns about Chinese bank-secrecy laws.[95] On August 31, 2011, U.S. District Judge Shira Scheindlin issued a Letter of Request pursuant to the Hague Convention to the Ministry of Justice in China to request evidence from the Bank.[96] More than 13 months later, however, the court still had not received a response from the Chinese Ministry of Justice.[97] As a result, the requesting party sought to compel production from the Bank.[98]

Judge Scheindlin largely granted the motion to compel due to the Ministry's failure to respond, and because (1) it appeared that some of the requested information was physically present in the United States; (2) the Bank had never been sanctioned by the Chinese government for complying with American court-ordered discovery; and (3) in one instance where the Ministry of Justice did in fact

respond to a Letter of Request, the Ministry substantially limited the response and, according to Judge Scheindlin, chose "not to defer to the relatively broad scope of American discovery." [99] Although Judge Scheindlin granted the motion to compel, she recognized some limited Chinese interests, for example exempting the Bank of China from producing confidential regulatory documents created by the Chinese government (as such production "is clearly prohibited under Chinese law"). [100] Judge Scheindlin also ordered that the parties had to meet and confer to limit discovery requests related to Chinese bank regulatory action. [101]

While much of the cross-border discovery discussion and analysis tends to focus on the decisions of federal courts, the SEC announced on December 3, 2012 that it is instituting administrative proceedings against Chinese firms associated with each of the Big Four accounting firms, as well as the Chinese firm associated with BDO because the Chinese firms had not produced audit documents of Chinese companies under SEC investigation. [102] The Chinese firms had pointed out that they could not comply with the SEC's requests due to, among other things, Chinese state secrecy law, which prevents audit documents from being removed from China. Based on the SEC press release, and the SEC Order in connection with the proceedings, it appears the SEC's position is foreign entities conducting audits of companies subject to SEC regulation must comply with SEC requests for information in the same manner as U.S.-based entities. [103]

We will continue to report on developments in the international e-discovery area. *For a general overview of the subject, see our E-Discovery Basics installment on Cross-Border E-Discovery [here](#).*

[Back to top](#)

Sanctions: Less Dramatic, More Pragmatic, But Still Troubling

Marking a departure from previous updates, the subject of sanctions is not our lead story for 2012. For starters, this year has witnessed a dearth of the dramatic opinions of past years, such as *Pension Committee*, *Victor Stanley* and *Rimkus*. More importantly, there have been major developments in the areas of predictive coding, rules reform and international e-discovery. Punitive sanctions remain a significant threat hanging over litigants and counsel, however, particularly where they can be imposed for inadvertent conduct. And unless meaningful rules reform is enacted and followed, sanctions will continue to contribute to the "collective anxiety" that surrounds e-discovery, as Magistrate Judge Paul Grimm astutely commented in his 2010 *Victor Stanley II* decision.

In our 2011 Mid-Year Report, we noted that the number of reported federal cases where a party sought sanctions for an alleged e-discovery failure was on pace for a significant increase in 2011 over the prior year. In 2012, however, we observed a *decrease* from 2011 levels. For the full year in 2012, we found 120 reported decisions where parties sought sanctions, up from 89 in 2009 and 100 in 2010, but down from the 150 reported decisions we found in 2011. [104] Similar to our findings from 2011, the percentage of cases where courts granted sanctions remained fairly constant, with courts awarding some form of sanctions in 69 cases, or 57.5% of the reported decisions (similar to the 60% of the decisions we identified in 2011). (Although we mention some of the 2011 cases in our discussion below, the 2012 statistics are of course limited to 2012 decisions.)

Of note, the numbers we have compiled for sanctions decisions are based on searches of publicly reported federal court decisions, a methodology we employed in past Mid-Year and Year-End E-Discovery Updates. Obviously, because many decisions go unreported, we cannot claim to have found every sanctions decision in 2012 or in previous years. A study prepared for the Judicial Conference's Advisory Committee on Civil Rules that the Federal Judicial Center ("FJC") published at the end of 2011, however, provides some empirical evidence of the relative numbers of sanctions motions and the frequency with which courts grant them.[105]

The FJC Study involved a comprehensive search of electronic dockets in civil cases filed in 2007-2008 in 19 federal districts, including the Northern District of California, the Northern District of Illinois, the Southern District of Texas, the Southern District of Florida and the Eastern and Southern Districts of New York. It found 209 cases in which a party brought a spoliation motion, which amounted to only 0.15% of cases filed in 2007-2008 in the 19 districts. The allegedly spoliated evidence included ESI in 53% of these 209 cases, meaning that the number of cases involving e-discovery spoliation claims represented only approximately 0.08%--obviously a very small number, prompting the ABA Litigation News to publish the following headline on the cover of its Fall 2011 issue (along with a picture of a mushroom cloud of flame): "*Spoliation: Not As Incendiary As You May Think*." [106] In ESI cases culminating in an order on a sanctions motion, the FJC Study found that courts granted motions 34% of the time and denied them 66% of the time--almost the opposite ratio from what we saw in the 2011 reported decisions (60% granted and 40% denied) and in the 2012 reported decisions (57.5% granted and 42.5% denied).

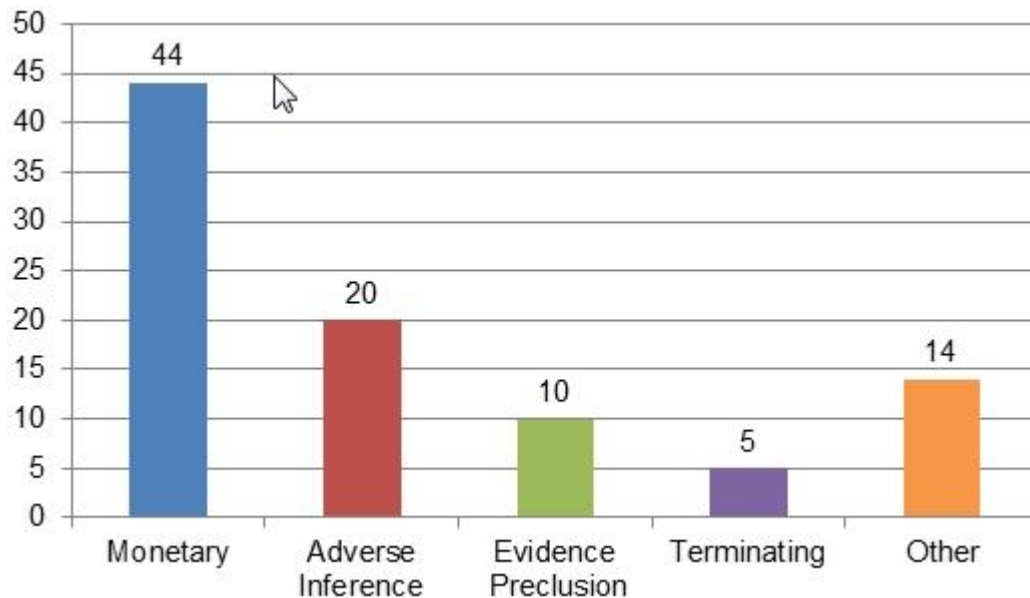
So what might account for the discrepancy in the ratios of sanctions decisions granted and denied according to the FJC Study, as opposed to what we see in reported decisions? We suspect that the numbers and ratios in the FJC Study better reflect what is actually taking place in the courts, as decisions granting sanctions are more likely to be published than opinions, docket entries, or minute orders denying them. Additionally, decisions granting sanctions may be more "newsworthy" than those denying them, and it is possible that reporting services are therefore more likely to publish decisions granting sanctions.

Despite the statistics from unpublished decisions in the FJC Study, no one can deny the weight that the reported decisions (particularly "outlier" decisions imposing extreme sanctions on grounds that arguably fall outside of mainstream thinking in the area) can carry--both in influencing companies in their preservation decisions, in incentivizing litigants to pursue e-discovery sanctions as a litigation tactic, and in increasing anxiety levels for virtually everyone. All this, coupled with the lack of uniform national standards, often leads to enormous burdens and likely over-preservation.

Moreover, as the FJC study acknowledges, as it examined decisions in only one period of time, it does not and cannot report on trends. *See* FJC Study at 5 ("this study cannot account for trends"). While not providing scientific precision, our methodology of comprehensively reviewing and analyzing reported decisions over the course of the past year and comparing our findings with prior years' results, by contrast, allows for some insight into the emerging trends. For example, as discussed in more detail below, in 2012 courts seem to have shifted somewhat in the types of sanctions awarded, appearing to favor the pragmatic over the punitive as they gain experience grappling with alleged e-discovery failures. Decisions have increasingly noted that monetary sanctions, as well as other creative sanctions

such as reopening discovery and hiring forensics analysts to search for spoliated data, are generally fairer and better at making the aggrieved party whole than punitive sanctions such as a default judgment.

***January 1 through December 31, 2012, Sanctions Awarded in E-Discovery
By Type and Percentage of Reported Cases Where Sanctions Granted***



Note: Sanctions were awarded in 69 reported cases we surveyed. Some involved awards of multiple types of sanctions (and for that reason, the number of cases identified in the chart above adds up to more than 69). In particular, monetary sanctions were often granted in conjunction with another sanction.

Monetary sanctions generally take the form of fees and costs incurred for discovering the failure and litigating the motion. For example, in *Straitshot Communications, Inc. v. Telekenex, Inc.*[107], even though defendants "engaged in bad faith spoliation of evidence . . . within the scope of his employment [by defendant]," the court declined to order greater sanctions. Similarly, in *In re Delta/AirTran Baggage Fee Antitrust Litig.*,[108] the court recognized the "general lack of diligence" demonstrated by defendant but awarded only reasonable attorney fees after defendant produced 60,000 missing responsive documents and hard drives that were not uploaded into the search platform. The court refused to preclude defendant from using the new evidence, finding that "the prejudice to Plaintiffs is mitigated by the revised case schedule, which includes additional discovery time and adjusted summary judgment deadlines." [109]

While rare, courts continue to issue very large, punitive monetary sanctions in egregious situations. For example, in *Multifeeder Tech., Inc. v. British Confenctionery Co. Ltd.*, the court imposed \$600,000 in expenses and attorneys' fees and \$25,000 to be paid to the court for evidence spoliation just before computer imaging. And in *Rosenthal Collins Grp., LLC v. Trading Techs. Int'l, Inc.*, the court imposed a \$1 million monetary penalty and case-terminating sanctions because it found that plaintiff's agent

engaged in "egregious conduct" such as deliberately modifying and destroying a significant amount of evidence.[110]

Adverse Inference and Evidence Preclusion: The frequency of adverse inference sanctions in decisions granting sanctions went from 25% in 2010, to 30% in 2011, to 29% (20 of the 69 decisions granting sanctions) in 2012. Meanwhile, courts granted evidence preclusion in ten cases (14% of the decisions granting sanctions) in 2012, versus 9% in 2011 and 11% in 2010.

Consistent with the apparent trend of more frequently tailoring sanctions to the level of prejudice that the injured party suffers, several courts have begun reserving a right to impose an adverse inference following the entry of evidence at trial as a means of ensuring that the sanction for spoliation remedies the offense. For example, in *Océ North America, Inc. v. MCS Services, Inc.*[111], the Court opined that it was too early in the litigation to grant an adverse instruction, as it was "unclear what type of evidence the parties plan to present to the jury and what the implications of the lack of data on the[] two [destroyed] laptops may be in light of the fact that there are at least twenty other laptops containing Océ data." [112] Similarly, in *Scentsy, Inc. v. B.R. Chase, LLC*[113], the court allowed additional depositions to determine whether spoliation had occurred.[114] If the testimony revealed spoliation, the court pledged to "consider giving an adverse inference instruction at trial or dismissing some or all of [plaintiff's] claims." [115]

Of note, the level of culpability required to grant an adverse inference remains an open question.[116] Some courts require proof of bad faith before imposing an adverse inference sanction, as "only the bad faith loss or destruction of a document will 'support an inference of consciousness of a weak case.'" [117] Other courts are split as to whether negligence or gross negligence is required.[118] Still others reframe the question in terms of whether the destruction was willful or inadvertent.[119]

Obviously, an adverse inference instruction can be tantamount to a case-terminating sanction. In a noteworthy example from 2011, *E.I. du Pont de Nemours & Co. v. Kolon Industries, Inc.*[120], the court denied plaintiff's request for default judgment as a sanction where certain of defendant's executives and employees intentionally had deleted relevant files and emails, because plaintiff had not "suffered the degree of prejudice required under the case law to enter default judgment"--among other things, "an overwhelming majority" of the deleted emails had been recovered from backup tapes and produced. Additionally, defendant had issued two litigation hold notices and "implemented a widespread effort to preserve files." Having found case-terminating sanctions to be inappropriate, and despite the apparent lack of substantial prejudice, the court nevertheless decided to grant an adverse inference jury instruction, ostensibly perceiving it to be a much lesser sanction. At trial, plaintiff won a staggering \$919 million verdict.

Case-Terminating Sanctions: Terminating sanctions continue to decrease compared to what we observed in 2011 and 2010. Of the 69 reported decisions we found granting sanctions in 2012, only five granted terminating sanctions (7%). This is a sizable decrease from 2011 and 2010, when approximately 14% and 22%, respectively, of the reported sanctions cases ended with terminating sanctions.

As expected, this harshest of sanctions was reserved for instances in which the discovery misconduct was palpable and greatly prejudiced the moving party. Bad faith was almost always required, as well as damage to the aggrieved party's case that could not be cured with monetary sanctions or an adverse inference. For example, in *Pringle v. Adams*, the court awarded dismissal as sanction against a plaintiff who, despite being aware of the duty to preserve, had disposed of hard drives containing potentially relevant evidence.[121] In *Taylor v. Mitre Corp.*, the court granted default judgment and monetary sanctions against plaintiff for "egregious" conduct after plaintiff destroyed an old computer containing relevant files with a sledge hammer and installed and ran an "Evidence Eliminator" program to destroy evidence on a new computer before a court-ordered forensic inspection could take place.[122]

There were further developments in 2012--and on January 3, 2013--in the widely publicized *Rambus* cases (against Micron Technology, Inc. in the District of Delaware and against Hynix Semiconductor in the Northern District of California). Rambus was found to have pursued a litigation preparation strategy that included at least one "shred day" whose alleged purpose was in part to destroy documents that might be harmful to it in anticipated patent litigation with companies including Micron and Hynix. Demonstrating the often subjective nature of determining whether serious sanctions are warranted, the District of Delaware granted case-terminating sanctions while the Northern District of California denied them. Both decisions were appealed to the Federal Circuit. The District of Delaware had concluded that Rambus had a duty to preserve because it destroyed documents after litigation became reasonably foreseeable. Based on the same facts, the Northern District of California found that litigation was not reasonably foreseeable because litigation was not "imminent" and depended on several contingencies.

The Federal Circuit affirmed the District of Delaware's finding of spoliation in the *Micron v. Rambus* case, but found that the trial court had inadequately stated the factual basis for its imposition of case terminating sanctions, which required clear and convincing evidence of bad faith on the part of the producing party and prejudice to the requesting party.[123] It reversed the Northern District of California's decision in the *Hynix v. Rambus* case, holding that the trial court had applied too narrow an interpretation of the "reasonably foreseeable" standard, and that a duty to preserve had arisen in any event before the second of two company "shred days." [124] It remanded the *Hynix* decision with instructions that the findings in the *Micron* decision be given "preclusive effect with respect to the issues of when Rambus's duty to preserve began and whether Rambus spoliated documents." [125]

On remand, the Northern District of California concluded that Rambus had "spoliated documents in bad faith or at least willfully," and the spoliation prejudiced Hynix.[126] But it refused to grant terminating sanctions, noting that the case had already been fully litigated and that Rambus did not intentionally destroy especially damaging documents.[127] Instead, the court "exercise[d] its discretion to fashion a remedy under its inherent power to sanction spoliation." [128] The court determined that an appropriate remedy would recognize the validity of Rambus's patents, but punish the spoliation and preclude Rambus from enjoying a royalty rate that would place "Hynix at a competitive disadvantage." [129]

Continuing the pattern of inconsistent decisions at the district court level, the Delaware District Court in its decision on remand on January 3, 2013, deemed Rambus' destruction of evidence "intentional,

widespread, advantage-seeking and concealed," imposed case dispositive sanctions, and declared the Rambus patents unenforceable against Micron.[130]

Other Sanctions: Courts have continued to show more willingness to craft sanctions that directly address and remedy the problem before them, rather than to simply mete out punishment. For example, in cases in which a party unjustifiably withheld documents, courts allowed the reopening of discovery or the re-deposition of a witness.[131] Some courts have attempted to cure the prejudice the injured party incurred by requiring the culpable party to find alternative sources for the spoliated documents or to determine the relevance of the spoliated documents, for example requiring a party to pay for the restoration and review of data on backup tapes.[132]

[Back to top](#)

Preservation: Data Sources Proliferate While Case Law Provides Little Specific Guidance

Technological change continues to dramatically impact how we work, communicate, create and store information. Smartphones and tablet computing devices with a myriad of apps, some of which save and share information in the cloud, are proliferating--so much so that companies are beginning to approve employees' use of their personal devices for business purposes. Although traditional email, calendar and contact information may still come to and from these devices through company servers, other information may only be retrievable from the devices themselves or from cloud storage that may not be in the custody or control of the company. While companies can restrict the use of thumb drives by inactivating USB ports on computers, for example, employees can save and share documents in a drop box in the cloud using a wireless Internet connection. Some well-known and popular devices, for example, backup data on some applications to a cloud service that does not enter into enterprise agreements, instead contracting only with individual users. These developments pose obvious challenges for information security, and also for preservation and collection in e-discovery. The case law, however, has not really kept up with these developments, other than by recognizing generally that--depending on the circumstances--parties often should consider data sources beyond traditional email.

Rather, much of the discussion in the cases has been mired in the issue of whether a legal hold notice must be in writing or whether an oral notice can be sufficient. In 2012, many courts continued to reject Judge Shira Scheindlin's controversial holding in *Pension Committee of University of Montreal Pension Plan v. Banc of America Securities, LLC*[133], that the failure to issue a *written* preservation notice is gross negligence *per se*. [134] Indeed, the Second Circuit went so far as to expressly abrogate the *Pension Committee* holding this year in *Chin v. Port Authority of New York & New Jersey*. [135] In *Chin*, the Second Circuit court put the proverbial nail in the coffin for this aspect of *Pension Committee*, holding that "'the better approach is to consider [the failure to adopt good preservation practices] as one factor' in the determination of whether discovery sanctions should issue." [136]

Reflecting this trend away from a bright-line proscription, several courts in the past year have grappled with the issue of whether and when a litigant can satisfy its preservation obligations by issuing only an oral preservation notice. A few courts that addressed this question suggested that an oral preservation notice can indeed suffice in the proper circumstances. For example, one court observed that an oral

preservation notice may be appropriate when a litigant is a small company and there are few custodians who need to receive a notice.[137]

Nevertheless, the majority of courts addressing oral litigation holds this year were critical, and--while still continuing to eschew Judge Scheindlin's bright-line approach--warned that a litigant that issues only an oral preservation notice does so at considerable peril. For example, in *Scentsy, Inc. v. B.R. Chase, LLC*, the court stated that "[g]enerally . . . orally requesting certain employees to preserve relevant documents . . . is completely inadequate. It is very risky--to such an extent that it borders on recklessness." [138] In *Sloan Valve Co. v. Zurn Industries, Inc.* [139], plaintiff in a patent infringement action brought a motion for sanctions against defendant for issuing oral preservation notices that allegedly were untimely and incomplete. In granting the motion, the court observed that several custodians could not recall whether they were even issued oral preservation notices, and even where they did recall receiving such notices, they still could not recall the scope of the preservation instructions that they received. [140] *Scentsy* and *Sloan Valve* serve as reminders that even where courts are willing to accept that oral preservation notices may sometimes be appropriate, parties relying on them may face considerable difficulties when, years after the oral preservation notice is given, no evidence of the preservation notice exists beyond custodians' often less than perfect memories.

Also continuing a trend we have reported in the past several years, many decisions issued in late 2011 and in 2012 focused on precisely *when* a litigant's duty to preserve relevant evidence is triggered. Although most of these cases continued to focus on when a defendant's duty to preserve arises, a few recent decisions have addressed when a plaintiff's duty to preserve arises. These courts have held that a plaintiff's duty to preserve--like a defendant's duty--arises when litigation is "reasonably foreseeable," which may predate the filing of the complaint by a significant period of time. [141] In one case, defendant in a False Claims Act action brought a motion for sanctions against the government plaintiff for failing to timely issue a preservation notice. [142] The court rejected the government's argument that the duty to preserve was triggered only when the government intervened to pursue litigation against defendant, and instead held that the duty to preserve was triggered when the government investigated defendant for alleged manipulation of the Medicaid funding program and engaged in settlement negotiations with it months before the government intervened in the case. [143]

Issuing a legal hold notice alone may be insufficient to meet a party's preservation obligations. Indeed, one court stated that "a party's mere circulation of a litigation hold is insufficient to meet its discovery obligations . . . ; rather, a party must take affirmative steps to ensure that potentially relevant evidence is diligently identified and preserved[.]" [144] While courts still have not set clear guidelines for what precise follow-up steps are required after issuing a preservation notice, several courts in 2012 discussed taking reasonable steps to suspend automatic deletion of potentially relevant information from information systems. [145]

Other decisions from late 2011 and 2012 did little to clarify what other particular follow-up steps courts expect of parties and their counsel, beyond general admonitions that some form of follow-up interaction is required. [146] One court held that defendant's preservation efforts were insufficient even though defendant issued a written preservation notice *and* required recipients of the hold notice to certify their compliance with the notice. [147] According to the court, these were not "adequate steps to

preserve relevant documents." [148] But what follow-up steps would have been adequate were not addressed in detail, and generally they appear to remain up for debate. While the courts have not set forth detailed guidelines regarding the steps to be taken in implementing a legal hold, litigants can refer to best practice sources such as The Sedona Conference®'s *Commentary on Legal Holds* and *The Sedona Principles* for guidance.

As part of courts' increased scrutiny of parties' preservation efforts, courts also have continued to expand the scope of what has been called "discovery about discovery," including a party's ability to obtain discovery about another party's preservation efforts. In general, courts have continued to recognize that preservation notices likely are protected from discovery by the attorney-client privilege. [149] However, "there has been a growing trend among courts to find the attorney-client privilege is lost when spoliation has occurred." [150]

Even when the preservation notice itself is not held discoverable, courts have continued to encourage--and at times compel--the disclosure of information relating to a party's preservation efforts. [151] To that end, some courts over the past year have encouraged and rewarded parties that voluntarily disclosed information about the scope of their preservation efforts. [152] Based on this trend, parties should not be surprised if information related to their preservation efforts are later deemed discoverable and scrutinized by courts and their adversaries.

We will continue to monitor and report on trends in the preservation area. *For a general overview of preservation issues, see our two installments on preservation in the E-Discovery Basics series [here](#) and [here](#).*

[Back to top](#)

Social Media: Preservation And Production Of "Public" Information

Discovery of social media information continues to be an area where courts are crafting new and innovative electronic discovery rules to properly account for its fluid nature. Recently, the judiciary has shown an increasingly deft understanding of how social media technologies function, an understanding that has enabled courts to better govern the preservation, collection, and authentication of social media information during the discovery process. Assisting in this area, The Sedona Conference® issued its *Primer on Social Media* in October 2012 with the goal of providing information to the bench and bar regarding the basics of social media and its discovery in litigation.

One of the major issues courts have addressed is the extent to which parties have an obligation to preserve social media during litigation, and whether the modification of social media sites constitutes sanctionable spoliation. Of course, the very nature of social media sites is that they are constantly in flux--as users add or delete information, modify their profiles, and add new contacts. To prohibit these types of modifications for the sake of preserving evidence during the course of litigation that may last years or even decades would render social media sites useless. Thus the traditional discovery approach that would likely lead courts to sanction parties for modifying evidence is inappropriate when applied to social media sites. Nonetheless, courts and litigants also recognize that social media sites may contain information that is relevant in litigation.

Recognizing this conundrum, courts have attempted to fashion new rules and approaches to preserving and using social media sites as evidence. In an innovative decision in a trademark infringement case, the District of New Jersey required defendant to recreate a Facebook page as it had previously existed so that the Facebook page showed plaintiff in a photo that displayed "infringing trade dress." [153] The court justified this approach in two ways. First, defendant lacked the mindset required for spoliation because although defendant "was on notice that he had to preserve evidence, it would not have been immediately clear that changing his profile picture would undermine discoverable evidence." [154] Second, the court explained that "it may even be somewhat misleading to have printouts of [d]efendant's posts with the infringing picture, as if they always appeared that way," because "it is likely that many posts existed for a substantial portion of their lifetime without the allegedly infringing photograph." [155]

In contrast, in *Patel v. Havana Bar, Restaurant & Catering, Inc.* [156], the court held that when the plaintiff's sister-in-law asked for witness statements via Facebook message for use in on-going litigation, plaintiff's failure to provide the responding statements to opposing counsel was "clearly spoliation." [157] The court issued sanctions against plaintiff, including an adverse inference instruction and payment of attorney's fees and costs to defendant. [158]

The difference between the court's novel approach to spoliation in *Katiroll*, and the traditional approach employed by the court in *Patel*, may turn on the type of social media evidence at issue. While the evidence in *Patel* took the form of Facebook messages, which are necessarily static and therefore more akin to private emails, in *Katiroll* the evidence was the Facebook page itself, which is public and subject to constant changes by the user and others who visit the user's page. As new forms of interactive social media are created and become more prevalent, we expect courts to continue to implement innovative approaches to spoliation that properly account for the dynamic nature of some features of social media sites.

Another discovery issue unique to social media sites is how, and by whom, data contained on those sites should be collected. Social media sites may be both public and private, and although individual users control the information posted on the sites, the information (both in its current form and often in prior forms) is maintained on servers controlled by the site host or other related entities. Determining who should collect and produce information from social media sites and how that information should be produced necessarily requires evaluation of whether the discoverable information is publicly available or protected by privacy settings, the relevant dates of the information, and even whether the site hosts (e.g., Facebook or Linked In) may be subpoenaed directly for the information on their servers. In light of these different issues, courts have arrived at a variety of different approaches to the collection and production of social media sites, which generally fall into four categories: appointing a neutral expert to collect the data; permitting the requesting party to access the social media site and collect the information; requiring the account holder to produce information from the social media site; and permitting the third party to subpoena the host for the information. Each of these approaches has benefits and pitfalls.

Appointment of a neutral third-party expert to collect information from social media sites has the distinct advantage of ensuring the user's privacy and ensuring that the collection is forensically sound. One court, "appreciative of privacy concerns," appointed "a forensic expert as a special master" to

gather "only discoverable information." [159] Plaintiff-intervenors and other class members provided the social networking data "directly and confidentially to the special master," who then reviewed the documents *in camera* and ordered the production of specified relevant information. [160] One of the major limitations of such an approach is that it is costly and burdensome on the parties and the court, so a number of courts have opted to instead shift the burden back on the parties to ferret out the discoverable information.

Some courts take the approach that the requesting party should be permitted to collect any information it seeks from the website. Of course, to do so, the requesting party must have access to both public and private user files, which may raise privacy concerns for the user. Consistent with Rule 26(b), those courts have stated that a party "does not have a generalized right to rummage at will through information that [the opposing party] has limited from public view. Rather . . . there must be a threshold showing that the requested information is reasonably calculated to lead to the discovery of admissible evidence. Otherwise, the [party seeking discovery] would be allowed to engage in the proverbial fishing expedition, in the hope that there *might* be something of relevance in [the other party's] Facebook account." [161] These cases emphasize that the electronic format of the information requested does not shield it from traditional restrictions regarding the scope of discovery-- "[t]he fact that the information defendants [sought was] in an electronic file as opposed to a file cabinet does not give them the right to rummage through the entire file." [162]

While a few courts have ordered that full access to the social networking account in question be granted to the opposing party, [163] most courts have found such requests to be overly broad and have required the discovering party to submit more particularized requests. [164] At least one court put a temporal limitation on providing the requesting party access to the responding party's Facebook page. The court ordered a plaintiff to provide defense counsel with her Facebook login information, but limited defense counsel's access to 21 days. [165] The court concluded that this method was "the least burdensome way to conduct discovery," as "the entire cost of investigating [plaintiff's] Facebook information will be borne by [defendant]," and plaintiff "can still access her account while [defendant] is investigating." [166]

Some courts have required the user account holder to gather the data from her social networking accounts, and provide it directly to defendant, without disclosing passwords or involving the court. [167] But, of course, permitting the account holder to control the information that is produced from the social network site--especially given how easy it is to modify the information--risks virtually undiscoverable spoliation. Courts have been reluctant, however, to permit (or require) parties to obtain information directly from site hosts. These courts generally find that the account holder of the social media site is better positioned than the site host to produce the discoverable material. [168] In fact, in *Glazer v. Fireman's Fund Ins. Co.* [169], instead of having defendant to subpoena the relevant social networking site, the court required plaintiff, who had closed her previous account on that site, to create a new one so that she could produce the relevant communications herself. Part of courts' reluctance to require parties to seek information from site hosts directly is that to do so implicates the Stored Communications Act (the "SCA"), whereas production of social media information by an account holder does not. [170]

Implicit in the question of who should collect social media information and how it should be collected is whether the information is authentic and reliable. At least one court has expressed concern that "electronic writings can sometimes be open to question--computers can be hacked, protected passwords can be compromised, and cell phones can be purloined." [171] Some courts have required traditional types of foundational proof to admit Facebook messages into evidence where the account holders claim their account had been "hacked." [172] This foundation could be established by "the computer of the purported author for Internet history and stored documents or . . . seeking authenticating information from the commercial host." [173] However, at least some courts have not taken a particularly strict approach to excluding social media evidence on the ground that it is inauthentic or unreliable. In *Tienda v. State*, when a defendant sought to exclude information from a MySpace page on the ground that he did not create the page, the court stated, "It is, of course, within the realm of possibility that the appellant was the victim of some elaborate and ongoing conspiracy. Conceivably some unknown malefactors somehow stole the appellant's numerous self-portrait photographs, concocted [the messages] . . . along with stealing the photograph of the grinning appellant lounging in his chair while wearing his ankle monitor. But that is an alternate scenario whose likelihood and weight the jury was entitled to assess once the State had produced a prima facie showing that it was the appellant, not some unidentified conspirators or fraud artists, who created and maintained these MySpace pages." [174]

[Back to top](#)

Cooperation: No Longer Just A Utopian Concept

When The Sedona Conference® issued its *Cooperation Proclamation* in 2008, the concept of "cooperation" in litigation seemed to some to be utopian and unrealistic. Since then, cooperation--meaning sharing information and collaboratively addressing e-discovery challenges--has become integral in e-discovery pilot programs and standing orders; judicial decisions evaluating parties' preservation, review methodologies (including predictive coding), and whether to impose sanctions; in reform of the Federal Rules (*e.g.*, the proposed amendment to Rule 37(e) considers parties' cooperation as a factor in whether sanctions should be imposed); and in addressing the challenges of international e-discovery.

The courts in 2012 increasingly focused on specific ways that parties could cooperate (for example, by reaching agreement about the format in which certain documents would be produced) and on treating favorably litigants who attempted to cooperate (for example, by refusing to require defendants to re-run searches, unless plaintiffs bore the cost, where plaintiffs had declined an invitation to meet and confer and had failed to object to defendants' search terms before production). [175] This focus on specific areas of cooperation (rather than generalized calls for parties to get along) continued in 2012.

Across jurisdictions, we saw courts willing to get into the details of e-discovery in an effort to foster cooperation between parties. An increasingly common way that courts are exercising some control over e-discovery is through the use of pilot programs, standing orders, and other broadly applicable e-discovery policies. In an effort to address some of the most common logistical issues that arise in the context of e-discovery--and perhaps even to "force cooperation"--courts around the country are increasingly requiring counsel to engage in substantive discussions about the scope and nature of

electronic discovery, including the form of any eventual production, early in the litigation process.[176] These programs and orders go far beyond a generalized call for cooperation, and instead provide concrete mechanisms for parties to discuss and agree upon electronic discovery protocols before disputes arise. The District of Kansas, for example, asks counsel to confer and "attempt to agree" not only on big-picture issues like the scope of preservation, but also fairly specific issues, like how to handle embedded data and metadata.[177] In addition to its general guidelines, the Northern District of California publishes a checklist for Rule 26(f) conferences, covering some fairly detailed topics, including the "interdiction of any document destruction program," the "quality control method(s)" used to evaluate the accuracy of search methodology, and different production formats for different types of ESI.[178] We expect to see these kinds of pilot programs become increasingly common, some of which may become a permanent feature of courts' local rules.

One particular area where courts encourage cooperation early in litigation is in deciding upon the form of production. For example, in *Da Silva Moore*, Judge Peck set certain parameters for the form of production, but ordered the parties to meet and confer about the format of non-email ESI and about any imaging or formatting issues with the produced electronic files.[179] Similarly, in *Navajo Nation v. United States*, the court set basic production parameters but required the parties to work together to determine the best way to produce databases and other dynamic ESI, video files, and audio files.[180] In 2012, we also saw issues related to cooperation--e.g., transparency and communication--arise especially with regard to predictive coding. As discussed above, in *Kleen Products*[181] and *Da Silva Moore*, the courts commended the parties for collaborating and agreeing upon a general predictive coding plan.

In 2013, we expect courts to continue to recognize the value of technology-assisted review, either by affirmatively encouraging parties to consider using predictive coding or by commenting positively on their decision to do so. At the same time, we believe that courts increasingly will be forced to adjudicate disputes relating to technology-assisted review, such as questions about appropriate "seed sets" and permissible search algorithms. It may well behoove parties who end up litigating such issues to bear in mind Judge Facciola's comment from 2008 that courts likely will not want to waste judicial resources and split hairs when disputes relating to predictive coding could be resolved through a meet-and-confer process.[182]

The flip side of a generalized call for cooperation, of course, is the threat of rebuke from the court. In 2012, several courts expressed frustration when parties failed to cooperate with one another, and with the court, to resolve e-discovery disputes. In *Chura v. Delmar Gardens of Lenexa, Inc.*,[183] for example, the court acknowledged that the parties had technically satisfied the local rules by conferring about certain ESI before plaintiffs moved to compel production.[184] Nonetheless, the court noted that "neither side explains whether they have further attempted to resolve this [discovery] issue since the motion was filed, and if they have not made such an attempt, why they have not done so. The duty to cooperate in an effort to achieve the 'just, speedy and inexpensive' determination continues throughout the litigation." [185]

In *Vasudevan Software, Inc. v. Microstrategy Inc.*[186], the court remarked on the parties' inability to reach agreement. Plaintiff and defendant filed six motions to compel or to prevent the disclosure of

certain ESI. In ruling on the motions, the court specifically noted the parties' failure to attempt to resolve their discovery issues collaboratively:

The court must also note that the parties here have displayed little of the cooperation required of litigants in an endeavor such as this. The Model Order requires parties to "cooperate to identify the proper custodians, proper search terms and proper time frame," and the Sedona Principles emphasize the importance of collaboration between parties during discovery To ensure that [the parties] achieve more fully the collaboration expected of them, lead counsel shall meet and confer in person before any future discovery disputes are brought in this court.[187]

Other courts have issued similar calls for cooperation.[188]

Finally, in *Borwick v. T-Mobile West Corp.*[189], defendant, faced with a motion for sanctions on the basis of spoliation, raised plaintiff's failure to cooperate as a *defense* against sanctions. In that case, there was a dispute about the format in which certain audio files would be produced. Among other things, the court noted that plaintiff's "failure to confer alone is certainly grounds enough to deny the motion." [190] Thus, cooperation, or the lack thereof, can be a sword and a shield.

[Back to top](#)

Proportionality: An Increasingly Important Principle

Like cooperation, proportionality is becoming an increasingly important--if underused--concept in relation to e-discovery. The concept has explicitly been included in e-discovery pilot projects and standing orders, in proposed amendments to Federal Rules of Civil Procedure 26 (regarding the scope of discovery) and 37 (regarding whether sanctions should be imposed for preservation failures), in cases evaluating predictive coding proposals, and in protocols for complying with foreign data protection laws in processing, reviewing and transferring information for production in U.S. litigation. Moreover, courts continue to limit broad ESI requests by considering the relevance of the data those requests would yield (through statistical sampling, for example), often limiting requests to certain time periods, specific custodians, and issues in dispute in the litigation. In making this determination, courts in 2012 frequently relied on *The Sedona Conference® Commentary on Proportionality in Electronic Discovery*, originally issued in 2010 and the final post-public comment version of which was just issued in January 2013.[191]

The Commentary on Proportionality sets forth six principles: (1) that the burdens and costs of preserving potentially relevant information should be weighed against the potential value and uniqueness of the information when determining the appropriate scope of preservation; (2) that discovery should generally be obtained from the most convenient, least burdensome and least expensive sources; (3) that undue burden, expense, or delay resulting from a party's action or inaction should be weighed against that party; (4) that 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) that 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.

Applying these principles, wide-ranging requests, particularly those not constrained by time frame, custodian, or topic, were likely to be rebuffed or at least significantly narrowed by courts when presented with a dispute--although, in certain instances, that relief came with a price. For example, in *Chen-Oster v. Goldman, Sachs & Co.*, the court denied plaintiff's motion to compel the production of information contained in an older database because that search would "likely entail a significant incremental burden because it could not be searched with the same code" as that used to search other databases at issue even though the information sought was "central" to plaintiff's claims, was not available from other sources, the amount in controversy was "surely substantial," and defendant's "ample resources[.]"[192]

Where the parties or the court required more evidence before the proportionality factors could be weighed, courts have approved the use of limited, targeted discovery, including statistical sampling.[193] Thus, the assessment of proportionality in the context of production continues to occupy a nuanced, highly detailed role in the discovery process. Neither one size, nor one precedent, will fit all, but the principles governing the discussion have become somewhat clearer over the years: detailed assessments of benefit and cost are required, expert testimony (*e.g.*, that of an e-discovery vendor or specialist) can be helpful, overbroad discovery requests should not be enforced, and cooperation and open communication with opposing counsel is generally encouraged and, in some courts, required.

As the scope of any litigant's obligation to preserve potentially relevant information is still far from certain in 2012, litigants are still faced with a thorny dilemma: preserve it all (at great expense) or do so in a more targeted fashion (at the risk of being second-guessed by opposing counsel and the court). As with the proportionality assessment itself, the costs and benefits of each approach must be weighed in light of that litigant's particular circumstances. There is no one right way.

[Back to top](#)

Inaccessibility: Undue Burden Necessary, But Not Necessarily Sufficient

In 2012, courts continued to require specific and detailed showings of burden and lack of benefit before making an inaccessibility determination under Federal Rule of Civil Procedure 26(b)(2)(B). Successful arguments for inaccessibility generally included detailed calculations of the time and concomitant cost an ESI search would require, along with an explanation of the means through which the search would proceed.[194]

Claims of inaccessibility were most persuasive where good cause for production of the documents appeared to be absent (that is, where requesting parties were unable identify the particular types of documents that had not already been produced from accessible sources and that would be likely found through a search of the inaccessible sources). Indeed, counsel's failure or inability to make any showing to support its expressed "good faith belief" that "crucial," "highly relevant," and "material" documents would be found in demonstrably inaccessible locations "sp[oke] volumes" to one court, resulting in a denial of a motion to compel.[195] By contrast, half-hearted attempts to classify ESI as inaccessible have been met with incredulity, particularly when proffered in defense to a motion for sanctions.[196]

Importantly, while cost and burden are critical elements in determining accessibility, courts in 2012 emphasized that a showing of undue burden is *alone* insufficient to trigger a finding of inaccessibility. "While cost and burden are critical elements in determining accessibility, a showing of undue burden is not sufficient by itself to trigger a finding of inaccessibility. For example, the sheer volume of data may make its production expensive, but that alone does not bring it within the scope of Rule 26(b)(2)(B). Rather, the cost or burden must be associated with some technological feature that inhibits accessibility." [197]

[Back to top](#)

Privilege: Waiver Is Such Sweet Sorrow, Or Not If You've Obtained An FRE 502(d) Order

Waiver Battles Under FRE 502(b)

The inadvertent disclosure of privileged information remains an issue of significant concern for litigants and courts alike, particularly where large volumes of ESI are involved. Demonstrating the importance of avoiding the quagmire of waiver issues through a no-fault claw-back order under Federal Rule of Evidence 502(d), courts in 2012 continued to grapple with issues under the otherwise applicable FRE 502(b) regarding whether litigants took adequate steps to prevent and promptly rectify the inadvertent disclosure of privileged documents.

A clear, uniform definition of reasonable efforts to prevent disclosure of privileged information under FRE 502(b) still has not emerged, and the decisions have been very fact-specific. Of particular note in 2012, some courts did not hesitate to find a waiver under FRE 502(b) where they found that the producing party did not conduct a careful privilege review. [198] Similarly, some courts found a waiver where the producing party failed to provide sufficient information to assess the reasonableness of its efforts to prevent disclosure of privileged information. [199]

Although a bright-line definition of "reasonable efforts" under FRE 502(b) remains elusive, decisions from 2012 indicate that mere reliance on a discovery vendor to prevent disclosure of privileged documents--without any attorney involvement--likely will not be sufficient. In *Blythe v. Bell* [200], defendants hired an outside consultant to identify documents responsive to a list of search terms, remove all emails containing defendants' law firm's email address, and produce the remainder "without any review or sampling or other quality assurance to assess whether the consultant's efforts had been successful in eliminating privileged communications." The court concluded that this procedure did not constitute reasonable efforts to prevent disclosure of privileged communications; counsel cannot "altogether delegate the need to guard against production of privileged communications to an outside consultant." [201]

In addition to undertaking reasonable efforts to prevent disclosure of privileged information, FRE 502(b) requires the disclosing party to promptly take reasonable efforts to rectify a disclosure. A number of courts in 2012 considered the type of conduct that constitutes "reasonable" efforts to rectify the disclosure. [202]

No-Fault Claw Backs Under FRE 502(d)

Several cases in 2012 involved "claw-back orders" under FRE 502(d), which provides that a court may order that the privilege or protection is not waived by disclosure connected with the litigation pending before the court--in which event the disclosure is also not a waiver in any other federal or state proceeding. Such orders can be used in an attempt to strike a balance by allowing the parties "to conduct and respond to discovery expeditiously, without the need for exhaustive pre-production privilege reviews, while still preserving each party's right to assert the privilege." [203]

Privilege and Work Computers

Continuing a trend from 2011, courts in 2012 also addressed waiver of the attorney-client privilege where an individual employee uses a work computer to communicate with a personal attorney. With one significant exception from 2011, [204] courts have held that employees who communicate with their personal attorneys using work resources--at least where specific policies indicating an employer's right to monitor such communications exist--waive any privilege in those communications.

In the single exception from 2011, plaintiffs in a securities lawsuit had successfully argued that defendant waived privilege by failing to produce a privilege log. [205] As defendant prepared to produce privileged documents, it discovered communications between individual employees and their personal attorneys. Defendant notified the individual employees that the privileged documents were going to be produced, and the individual employees attempted to intervene in the case and seek a protective order. [206] The court held that, although defendant had a clear policy that stated that communications using its email server were not private (which would otherwise lead to a waiver of privilege), an implied joint defense agreement existed between the individual employees and defendant, and because of that implied agreement, the individual employees had not waived privilege in their communications with their personal attorneys. The court found that employees were right to "disregard[] the internal email communications policy" under this circumstance. [207]

Like the majority of decisions in 2011 [208], the single court to address this issue in a published decision in 2012 found that an employee waived the attorney-client privilege when he used a work computer to communicate with a personal attorney. [209] In *Chechele v. Ward*, a plaintiff alleging that defendant violated short-swing profit rule by profiting from the purchase and sale of his company's stock within a six-month period served a request for production of documents on the company. [210] In reviewing the email accounts of individuals likely to possess responsive documents, the company discovered responsive communications between defendant and other individuals, on one hand, and defendant's attorney, on the other. [211] The company withheld the communications from production at defendant's request, and plaintiff moved to compel production of the communications. [212] Noting that the company's computer and email usage policy "clearly notifie[d] [the company's] employees that their emails are not guaranteed to be confidential . . . and that email messages are considered business records and may be subject to discovery in the event of litigation," the court concluded that defendant "had no objectively reasonable expectation of privacy or confidentiality regarding his attorney-client communications and effectively waived the attorney-client privilege for those communications." [213]

In light of this clear trend toward finding a waiver of privilege, attorneys who communicate with their clients via their work email accounts would be wise to follow the American Bar Association's guidance regarding attorney communications with employees using employer resources.[214] The Opinion recognizes that clients may be unaware of the risks of using public or work-issued computers to communicate with an attorney and discusses the lawyer's duties to protect the confidentiality of communications.

[Back to top](#)

Governmental E-Discovery Obligations: No One Is Exempt From Sanctions

The Government as a Litigant

After the SEC's practice of destroying preliminary investigation materials grabbed headlines and sparked litigation in 2011[215], government record-keeping and document preservation continued to be scrutinized in 2012. Depending on the government's culpability and the prejudice suffered by the opposing party, courts have not been shy about imposing sanctions on government entities for spoliation of evidence, although courts continue to be reluctant to impose the most serious sanctions of dismissal or adverse inference absent a finding of bad faith.[216]

Contemporaneous with this increased scrutiny, several federal agencies have taken steps to improve their e-discovery and record preservation practices, and to encourage cooperation with litigants. For example, a recent set of revisions to the Federal Trade Commission's ("FTC") investigative procedures requires recipients of compulsory process to discuss ESI and other issues with the FTC within 14 days of receiving process, or before the deadline to file a motion to quash.[217] Similarly, a set of e-discovery recommendations for federal criminal cases prepared by the DOJ, the U.S. Attorney General, courts and the defense bar recommends early and, in complex cases, regular discussions regarding ESI discovery.[218] The *Recommendations'* ten basic principles also suggest conferring with individuals with technical knowledge, producing ESI in mutually agreed upon formats, using good faith efforts to resolve issues without court intervention, and preventing unauthorized access to ESI materials.[219] While nonbinding on the parties or the courts, all DOJ attorneys will be trained on the *Recommendations*. [220] The IRS also reissued an interim guidance memorandum on preserving ESI for litigation, but noted that the procedures were being re-evaluated and subject to change.[221]

More sweeping changes for government ESI record-keeping are on the horizon. Following up on a November 2011 Presidential Memorandum, the Office of Management and Budget issued a directive to executive branch departments and agencies, mandating electronic management of all permanent electronic records by 2019.[222] The Directive set deadlines for each agency to designate an official to oversee its records management program, and to establish records management training for agency staff.[223] By the end of 2013, the National Archives and Records Administration will issue revised guidance on transferring permanent electronic records and create new guidance on managing, disposing, and transferring email.[224]

Trends in the Investigative Context

In addition to e-discovery obligations the government may have as a party to litigation, government entities also continue to face separate disclosure obligations in the investigative capacity. In 2012, the Supreme Court decided the landmark case of *United States v. Jones*,^[225] which held that surreptitious GPS surveillance constitutes a "search" under the Fourth Amendment.^[226] In the wake of *Jones*, a number of defendants have argued that GPS data and other ESI used as evidence against them should be suppressed. As a temporary response to this initial outburst of criticism, most courts have applied a good-faith exception to conduct predating the *Jones* decision.^[227] But the long-term effect of *Jones* on government investigation has yet to mature.

Congress has attempted to directly address the electronic surveillance issues raised by *Jones* and its progeny through the Geolocation Privacy and Surveillance Act ("GPS Act").^[228] The GPS Act would require law enforcement to obtain a warrant before obtaining geolocation data from wireless or tracking devices.^[229] This bill awaits consideration by Congress. Further, a steady increase in government requests for information stored by internet service providers and on social media sites prompted renewed demands to modernize the Stored Communications Act ("SCA").^[230] The SCA sets the standards for government access to stored electronic communications. The SCA authorizes the government to obtain non-content records and content records over 180 days old using a subpoena or court order^[231], but requires a warrant to access the contents of stored communications less than 180 days old.^[232] Courts have reached conflicting opinions on what types of electronic communication are protected from government access under the SCA.^[233] In *United States v. Graham*, the court explicitly rejected a cumulative approach whereby "surveillance becomes a Fourth Amendment 'search' only after some specified period of time[.]"^[234] On this basis, the court held that cell site data held by third parties is not subject to the Fourth Amendment's probable cause standard, but the lower standards outlined in the SCA.^[235]

Relatedly, on November 29, 2012, the Senate Judiciary Committee approved a bill that will impose new restrictions on the government's ability to access data stored by electronic communications providers.^[236] Adopting the position of the Digital Due Process Coalition, which includes Amazon, AT&T, eBay, and Google, the ECPA Amendments Act would require a warrant for the government to compel production of the contents of stored communications, regardless of the messages' age.^[237] This legislation is expected to be the subject of negotiations with the House of Representatives in 2013, several House Republicans and various law enforcement organizations have voiced objections to the amendments.^[238] The trend in electronic government investigation thus favors greater protection for the individuals under investigation by requiring warrants for a broader scope of electronic searches.

[Back to top](#)

Conclusion

There has been a lot to report this year, as rapid advances in technology and globalization continue to dramatically modify the e-discovery landscape, requiring significant changes in how the rules, litigants and courts deal with e-discovery. The good news is that progress is being made in addressing e-discovery's challenges. The dense fog that often seems to surround e-discovery appears to have lifted

somewhat, and the collective anxiety lowered a little. Nevertheless, much remains to be done and meaningful reform of the rules is still needed. While such reform is closer than ever, it has not yet arrived. Until that time, the risk of outlier decisions in the sanctions area remains high. Additionally, while technological change in the form of predictive coding brings hope of easing the burden and expense of reviewing large volumes of documents, litigants and courts must be vigilant against it being used as a justification for overly broad discovery, which would potentially exacerbate the problem that it seeks to address. As in the past, we will continue to follow and report on this important field, which impacts almost every litigation matter as discovery more and more becomes e-discovery.

*If you would like to **subscribe** to future E-Discovery updates and alerts, you may do so [here](#).*

Our past updates and alerts are available [here](#).

*Also, look out for our **2012 Year-End E-Discovery Update Webinar**, which will be announced soon. If you would like to request an invitation, you may do so [here](#).*

[Back to top](#)

[1] See Andrew Peck, Search, Forward: Will Manual Document Review and Keyword Searches Be Replaced by Computer-Assisted Coding?, L. TECH. NEWS (Oct. 1, 2011).

[2] See *Da Silva Moore v. Publicis Groupe SA*, No. 11 Civ. 1279(ALC)(AJP), 2012 WL 607412 (S.D.N.Y.) Feb. 24, 2012) (Peck, Mag. J.) (approving predictive coding protocol) [hereinafter "*Da Silva Moore I*"]; *Da Silva Moore v. Publicis Groupe SA*, 868 F. Supp. 2d 137 (S.D.N.Y. 2012) (Peck, Mag. J.) (denying plaintiffs' recusal motion) [hereinafter "*Da Silva Moore III*"].

[3] See *Da Silva Moore I*, 2012 WL 607412, at *1.

[4] See *id.* at *3.

[5] *Id.* at *5.

[6] *Id.*

[7] *Id.*

[8] *Id.* (alterations in original).

[9] *Id.* at *6.

[10] *Da Silva Moore I*, 2012 WL 607412, at *6.

[11] *Id.*

[12] *Id.*

[13] *Id.* at *11.

[14] *Id.*

[15] *See Da Silva Moore v. Publicis Groupe SA*, No. 11 Civ. 1279(ALC)(AJP), 2012 WL 1446534 (S.D.N.Y. Apr. 26, 2012).

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] *Da Silva Moore III*, 868 F. Supp. 2d at 140.

[20] *Id.* at 156.

[21] *Id.* at 151-72.

[22] Order, *Da Silva Moore v. Publicis Groupe SA*, No. 11 Civ. 1279(ALC)(AJP) (S.D.N.Y. Nov. 8, 2012).

[23] *Id.* at 4.

[24] *Id.*

[25] *Id.*

[26] *See* Defs.' Memorandum in Support of Motion for Protective Order Approving the Use of Predictive Coding, *Global Aerospace Inc. v. Landow Aviation, L.P.*, Nos. CL 61040, CL 61991, CL 64475, CL 63795, CL 63190, CL 63575, CL 61909, CL 61712, CL 71633 (Va. Cir. Ct. Apr. 9, 2012), *available at* 2012 WL 1419842.

[27] *Id.*

[28] *Id.*

[29] Defs.' Memorandum in Support of Motion for Protective Order Approving the Use of Predictive Coding, *Global Aerospace Inc.*

[30] Opposition of Pls.: M.I.C. Indus., et al., to the Landow Defs.' Motion for Protective Order Regarding Elec. Documents and "Predictive Coding," *Global Aerospace Inc. v. Landow Aviation, L.P.*, Nos. CL 61040, CL 61991, CL 64475, CL 63795, CL 63190, CL 63575, CL 61909, CL 61712, CL 71633 (Va. Cir. Ct. Apr. 16, 2012), *available at* 2012 WL 1419848.

[31] Order Approving the Use of Predictive Coding For Discovery, *Global Aerospace*, Consol. Case. No. CL 61040 (Va. Cir. Ct. Apr. 23, 2012).

[32] Pls.' Statement of Position With Respect to Disputed Items for Dec. 15, 2011 Status Conference 4-5 & n.6, *Kleen Prods. LLC v. Packaging Corp. of Am.*, Case No. 1:10-cv-05711 (N.D. Ill. Dec. 13, 2011).

[33] *See* Defs.' Statement of Position With Respect to Disputed Items for Dec. 15, 2011 Status Conference 4-16, *Kleen Prods.*, Case No. 1:10-cv-05711.

[34] *See* Evidentiary Hr'g Tr., *Kleen Products*, Case No. 1:10-cv-05711 (Feb. 21, 2012); Evidentiary Hr'g Tr., *Kleen Prods.*, Case No. 1:10-cv-05711 (Mar. 28, 2012).

[35] Evidentiary Hr'g Tr. 297-300, *Kleen Prods.*, Case No. 1:10-cv-05711 (Mar. 28, 2012).

[36] *Id.* at 297-98,

[37] The Sedona Conference, *The Sedona Principles: Second Edition* 38 (June 2007).

[38] Stipulation & Order Relating to ESI Search, *Kleen Prods.*, Case No. 1:10-cv-05711 (Aug. 21, 2012).

[39] *See* Case Management Order: Protocol Relating to the Production of Electronically Stored Information ("ESI") 6-16, *In re Actos (Pioglitazone) Prods. Liab. Litig.*, MDL No. 6:11-md-2299 (W.D. La. July 27, 2012).

[40] *Id.* at 7-9.

[41] *Id.* at 10-15.

[42] *Id.* at 15-16.

[43] Hr'g Tr. 66-67, *EORHB, Inc. v. HOA Holdings LLC*, Civil Action No. 7409-VCL (Del. Ch. Oct. 15, 2012).

[44] Hr'g Tr. 67.

[45] *Id.* at 66.

[46] *National Day Laborer Organizing Network v. United States Immigration & Customs Enforcement Agency*, No. 10 Civ. 3488 (SAS), 2012 WL 2878130, at *1, *11-*12 (S.D.N.Y. July 13, 2012) (footnotes omitted).

[47] *The Sedona Conference® Commentary on Proportionality in Electronic Discovery* (Jan. 2013).

[48] *See id.*

[49] Draft Minutes, Civil Rules Advisory Committee, 12–13 (Nov. 4, 2012) [hereinafter "Draft Minutes"].

[50] *See id.* at 12.

[51] *Id.* at 3-4.

[52] *See Advisory Committee on Civil Rules*, 124, 127 (Nov. 1-2, 2012) [hereinafter "Committee Materials"].

[53] Committee Materials, at 127–29.

[54] Draft Minutes, at 12.

[55] Committee Materials, at 353–54 (Duke Conference: Initial Rules Sketches).

[56] Draft Minutes, at 13.

[57] *Id.*

[58] *Id.*

[59] *Id.* at 14-15.

[60] *See* Letter from Trent Franks, Chairman of House Judiciary Committee Subcommittee on the Constitution, to Judges Mark R. Kravits and David G. Campbell (Mar. 21, 2012).

[61] Originally, H.R. 2471 only focused on the Video Privacy Protection Act, but Senate Judiciary Committee Chairman Patrick Leahy obtained the necessary support to amend H.R. 2471 to also include amendments to the ECPA.

[62] *See* H.R. 2471, § 203.

[63] *Id.*

[64] *Id.*

[65] *Id.* § 204.

[66] *See* 2010 Year-End Report; 2011 Mid-Year Report; *see also* Press Release, Senate Judiciary Committee Approves Leahy-Authored Legislation to Update Video Privacy Protection Act, Electronic Communications Privacy Act (Nov. 29, 2012).

[67] *See, e.g.,* Charlie Savage, *Panel Approves a Bill to Safeguard Email*, N.Y. Times, Nov. 30, 2012, at B7 (discussing law enforcements opposition to the amendment).

[68] *See* Charlie Savage, *Panel Approves a Bill to Safeguard Email*, N.Y. Times, Nov. 30, 2012, at B7.

[69] *See In re Amendment of Rules 4009.1, 4009.11, 4009.12, 4009.21, 4009.23, and 4011 of the Pennsylvania Rules of Civil Procedure* [hereinafter "*Pennsylvania Amendments*"], No. 564, App'x at 1-4 (June 6, 2012).

[70] *Pennsylvania Amendments* at cmt. A.

[71] *Id.*

[72] *See In re Amendments to the Florida Rules of Civil Procedure--Electronic Discovery*, No. SC11-1542 (Fla. July 5, 2012).

[73] Fla. R. Civ. P. 1.201(a)(1).

[74] *See* N.Y. Sup. Ct. Comm. Div. Part 48 Commercial Case R.1a.

[75] *Id.*

[76] *See In re Pilot Project Regarding Case Management Techniques for Complex Civil Cases in the S.D.N.Y.*, No. 11-388, Standing Order M10-468 (S.D.N.Y. Nov. 1, 2011) [hereinafter the "*SDNY Order*"].

[77] *SDNY Order*, App'x at 10-11.

[78] *See SDNY Order* ¶ 2.

[79] *See Standing Order for All Judges of the Northern District of California* (N.D. Cal. Nov. 27, 2012) [hereinafter "*N.D. Cal. Order*"].

[80] *Checklist for Rule 26(f) Meet-and-Confer Regarding Electronically Stored Information* (N.D. Cal. Nov. 27, 2012).

[81] *Guidelines for the Discovery of Electronically Stored Information* (N.D. Cal. Nov. 27, 2012).

[82] *See Model Stipulated Order* (N.D. Cal. Nov. 27, 2012).

[83] Press Release, *Court Adopts New E-Discovery Guidelines Effective November 27, 2012* (Nov. 27, 2012).

[84] *Id.*

[85] *See* N.D. Cal. Order.

[86] *See Proposed Amendments to the Massachusetts [sic] Rules of Civil Procedure Regarding Discovery of Electronically Stored Information.*

[87] *Id.*

[88] See Graham Greenleaf, *Global Data Privacy Laws: 89 Countries, and Accelerating*, Privacy Laws & Business International Report, Issue 115 Special Supplement (Feb. 2012).

[89] *Id.*

[90] *Id.*

[91] *Tiffany (NJ) LLC v. Forbse*, No. 11 Civ. 4976 (NRB), 2012 WL 1918866 (S.D.N.Y. May 23, 2012).

[92] *Gucci Am. Inc. v. Weixing Li*, No. 10 Civ. 4974(RJS), 2012 WL 1883352 (S.D.N.Y. May 18, 2012).

[93] See *SNP Boat Serv. S.A. v. Hotel Le St. James*, No. 11-cv-62671-KMM, 2012 WL 1355550 (S.D. Fla. Apr. 18, 2012) (rejecting debtor's argument that the court should limit discovery based on French blocking statute because French authorities had started to enforce the statues and finding that the fact that French authorities "are only now enforcing the statue" does not change the long standing analysis); see also *Metso Minerals Indus., Inc. v. Johnson Crushers Int'l, Inc.*, 276 F.R.D. 504 (E.D. Wis. 2011) (relying on *Aerospatiale* for the proposition that a party "must do more than simply point to the blocking statute" and instead "must identify the specific French interests that would be undermined").

[94] No. 11 Civ. 1266 (SAS), 2012 WL 5378961 (S.D.N.Y. Oct. 29, 2012).

[95] *Id.* at *1.

[96] *Id.*

[97] *Id.* at *2.

[98] *Id.* at *1.

[99] *Id.* at *8.

[100] *Id.* at *5.

[101] *Id.* at *4.

[102] Press Release, SEC Charges China Affiliates of Big Four Accounting Firms with Violating U.S. Securities Laws in Refusing to Produce Documents (Dec. 3, 2012).

[103] *Id.*; *In re BDO China Dahua CPA Co. Ltd.*, File No. 3-15116, Order Instituting Administrative Proceedings Pursuant to Rule 102(e)(1)(iii) of the Commission's Rules of Practice and Notice of Hearing (Dec. 3, 2012).

[104] We did not publish a year-end report in 2011 due to extraneous circumstances, but we nevertheless conducted a full analysis of 2011 e-discovery decisions.

[105] See Emery G. Lee III, Federal Judicial Center, *Motions for Sanctions Based Upon Spoliation of Evidence in Civil Cases* (2011) [hereinafter "FJC Study"].

[106] See also Henry R. Chalmers, *Successful Sanctions Motions Are Rarer Than You May Think*, ABA Litigation News Vol. 37, No. 1 at 8 (Fall 2011).

[107] No. C10-268 TSZ, 2012 WL 5880293 Nov. 20, 2012).

[108] 846 F. Supp. 2d 1335, 1358 (N.D. Ga. 2012).

[109] *Id.*

[110] *Multifeeder Tech., Inc. v. British Confenctionery Co. Ltd.*, No. 09-1090 (JRT/TNL), 2012 WL 4135848, at *9 (D. Minn. Sept. 18, 2012); *Rosenthal Collins Grp., LLC v. Trading Techs. Int'l, Inc.*, No. 05 C 4088, 2011 WL 722467 (N.D. Ill. Feb. 23, 2011).

[111] No. WMN-10-0984, 2011 WL 6130542 (D. Md. Dec. 7, 2011).

[112] *Id.* at *4.

[113] No. 1:11-cv-00249-BLW, 2012 WL 4523112 (D. Utah Oct. 2, 2012).

[114] *Id.* at *9.

[115] See also *Miller v. Four Winds Int'l Corp.*, 827 F. Supp. 2d 1175, 1188 (D. Idaho 2011) (Dale, Mag. J.) (reserving the right to issue an adverse inference ruling "at the appropriate time after considering the evidence").

[116] See, e.g., *Chin v. Port Auth. of New York & New Jersey*, 685 F.3d 135, 161-62 (2d Cir. 2012) (approving a case-by-case approach to sanctions and rejecting the rule from *Pension Committee of University of Montreal Pension Plan v. Banc of America Securities, LLC*, 685 F. Supp. 2d 456, 464-65 (S.D.N.Y. 2010) that failure to institute a litigation hold constitutes gross negligence per se).

[117] *McCargo v. Texas Roadhouse, Inc.*, No. 09-cv-02889-WYD-KMT, 2011 WL 1638992, at *9 (D. Colo. May 2, 2011) (Tafoya, Mag. J.); see also *Bozic v. City of Washington*, No. 2:11-cv-674, 2012 WL 6050610, at *10 (W.D. Pa. Dec. 5, 2012) (imposing adverse inference sanction only after determining that defendant spoliated evidence in bad faith).

[118] See, e.g., *GenOn Mid-Atl., LLC v. Stone & Webster, Inc.*, 11 Civ. 1299 HB, 2012 WL 1849101 (S.D.N.Y. May 21, 2012) (imposing adverse inference sanction where party was "at least negligent"); compare also *Siani v. State Univ. of New N.Y. at Farmingdale*, No. 09-CV-407 (JFB)(WDW), 2011 WL 2580361 (E.D.N.Y. June 28, 2011) (denying a request for an adverse inference because the spoliation was merely negligent rather than grossly negligent), with *Patel v. Havana Bar, Rest. & Catering*, No. 10-1383, 2011 WL 6029983 (E.D. Pa. Dec. 5, 2011) ("[E]ven 'negligent destruction of relevant evidence can be sufficient to give rise to the spoliation inference.'").

[119] *Compare Melendres v. Arpaio*, No. CV-07-2513-PHX-GMS, 2011 WL 6740709 (D. Ariz. Dec. 23, 2011) (adverse inference granted because the party intentionally shredded the evidence rather than lost it, though did not necessarily "intend to deprive an opposing party of relevant evidence"), *with Hudson v. AIH Receivable Mgmt.*, No. 10-2287-JAR-KGG, 2012 WL 1194329, at *6 (D. Kan. Mar. 14, 2012) ("Defendant's actions were not willful. Rather, [the] destruction of email . . . was the result of a misunderstanding.").

[120] 803 F. Supp. 2d 469 (E.D. Va. 2011),

[121] *Pringle v. Adams*, No. 10-1656-JST, 2012 WL 1103939 (C.D. Cal. Mar. 30, 2012).

[122] *Taylor v. Mitre Corp.*, No. 1:11-cv-01247, 2012 WL 5473573, at *2-*3 (E.D. Va. Nov. 8, 2012).

[123] *Micron Tech., Inc. v. Rambus Inc.*, 645 F.3d 1311, 1328-29 (Fed. Cir. May 13, 2011).

[124] *See Hynix Semiconductor Inc. v. Rambus, Inc.*, 645 F.3d 1336, 1346-47 (Fed. Cir. May 13, 2011).

[125] *Hynix Semiconductor Inc. v. Rambus Inc.*, No. 00-20905, 2012 WL 4328999, at *31 (N.D. Cal. Sept. 21, 2012).

[126] *Id.* at *39.

[127] *Id.* at *45.

[128] *Id.*

[129] *Id.*

[130] *Micron Tech., Inc. v. Rambus Inc.*, No. 00-792, 2013 U.S. Dist. LEXIS , at *70 (D. Del. Jan. 2, 2013).

[131] *See, e.g., Scentsy*, 2012 WL 4523112, at *9 (allowing additional depositions); *Hylton v. Anytime Towing*, No. 11-cv-1039, 2012 WL 1564527, at *4 (S.D. Cal. May 2, 2012) (McCurine, Mag. J.) (ordering plaintiff to sit for a second deposition).

[132] *See, e.g., EEOC v. New Breed Logistics*, No. 10-2696 STA/TMP, 2012 WL 4361449 (requiring party to pay for restoration and review of backup tapes); *Carrillo v. Schneider Logistics*, No. CV 11-8557-CAS (DTBx), 2012 WL 4791614 (ordering party to hire an outside vendor to collect ESI, review it for production, and determine if responsive documents were permanently destroyed).

[133] 685 F. Supp. 2d 456, 464-65 (S.D.N.Y. 2010).

[134] *See, e.g., Curcio v. Roosevelt Union Free Sch. Dist.*, 283 F.R.D. 102, 111 (E.D.N.Y. 2012) ("[A] blanket conclusion of gross negligence elevates form over substance.") (Tomlinson, Mag. J.); *Meyer Corp. U.S. v. Alfay Designs, Inc.*, No. CV 2010 3647 (CBA)(MDG), 2012 WL 3536987, at *7

(E.D.N.Y. Aug. 13, 2012) (Go, Mag. J.) (denying motion to sanction party for failure to produce evidence of written preservation notice); *YCB Int'l, Inc. v. UCF Trading Co.*, No. 09-CV-7221, 2012 WL 3069683, at *10 (N.D. Ill. June 12, 2012) (Mason, Mag. J.) ("[A party] need not have an official written policy regarding the preservation of documents related to litigation to avoid sanctions" (quoting *Diersen v. Walker*, No. 00 C 2437, 2003 WL 21317276, at *4-*5 (N.D. Ill. June 6, 2003))).

[135] 685 F.3d 135 (2d Cir. 2012).

[136] *Id.* at 162 (quoting *Orbit Comm'ns, Inc. v. Numerex Corp.*, 271 F.R.D. 429, 441 (S.D.N.Y. 2010)).

[137] *See Meyer Corp. U.S.*, 2012 WL 3536987, at *7 (impliedly approving of oral preservation notice).

[138] *Scentsy, Inc. v. B.R. Chase, LLC*, No. 1:11-cv-00249-BLW, 2012 WL 4523112, at *18 (D. Idaho Oct. 2, 2012); *See also Carrillo v. Schneider Logistics, Inc.*, No. CV 11-8557-CAS (DTB), 2012 WL 4791614, at *8 (C.D. Cal. Oct. 5, 2012) (Bristow, Mag. J) (holding defendant's preservation efforts insufficient where defendant only instructed key employees orally not to destroy or delete relevant documents).

[139] No. 10-cv-204, 2012 WL 1886353, at *12 (N.D. Ill. May 23, 2012).

[140] *Id.* at *13-14.

[141] *See, e.g., YCB Int'l*, 2012 WL 3069683, at *7 (holding plaintiff's duty to preserve evidence was triggered ten months before litigation commenced, when plaintiff's president emailed draft demand letter to use "as evidence in any future litigation").

[142] *United States ex rel. Baker v. Cmty. Health Sys.*, No. 05-279 WJ/ACT, 2012 WL 5387069, at *1 (D.N.M. Oct. 3, 2012).

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

[144] *915 Broadway Assocs. LLC v. Paul, Hastings, Janofsky & Walker, LLP*, No. 403124/08, 2012 WL 593075, at *9 (N.Y. Sup. Ct. Feb. 16, 2012).

[145] *Id.* ("[A] party must suspend its automatic deletion function . . ."); *Kravtsov v. Town of Greenburgh*, No. 10-CV-3142 (CS), 2012 WL 2719663, at *5 (S.D.N.Y. July 9, 2012) (holding defendants at least grossly negligent for failing to take steps to suspend automatic deletion of video recordings).

[146] *See, e.g., 915 Broadway Assocs.*, 2012 WL 593075, at *9 (holding that plaintiff did not take sufficient, but largely undefined, "affirmative steps" to ensure preservation); *United States ex rel. Baker*, 2012 WL 5387069, at *4 (holding that disappearance of documents "suggested a 'lackadaisical attitude' with which the Government approached its ongoing duty to monitor the litigation hold" but not discussing what further steps should have been employed); *E.I. Du Pont de Nemours & Co. v.*

Kolon Indus., Inc., 803 F. Supp. 2d 469, 501 (E.D. Va. 2011) (holding without further explanation that defendant and its counsel did not provide "sufficient instruction" to employees about importance of document preservation).

[147] *Carrillo*, 2012 WL 4791614, at *8-*9.

[148] *Id.* at *9.

[149] *See, e.g., Tracy v. NVR, Inc.*, No. 04-CV-6541L, 2012 WL 1067889, at *6 (W.D.N.Y. Mar. 26, 2012) (Payson, Mag. J.); *Magnetar Techs. Corp. v. Six Flags Theme Park Inc.*, No. 07-127-LPS-MPT, 2012 WL 3609715, at *8 (D. Del. Aug. 20, 2012) (Thynge, Mag. J.).

[150] *Magnetar Techs. Corp.*, 2012 WL 3609715, at *8 (granting motion to compel production of preservation notice); *see also Tracy*, 2012 WL 1067889, at *6 (holding it is "reasonable" to compel production of preservation notice upon "preliminary showing of spoliation").

[151] *See, e.g., Sloan Valve*, 2012 WL 1886353, at *14 (requiring defendant to file supplementary affidavit containing specific information about defendant's litigation hold and document retention policies so court could evaluate "the reasonableness of [defendant's] document preservation efforts"); *Brown v. West Corp.*, No. 8:11CV284, 2012 WL 5400043, at *2 (D. Neb. Nov. 5, 2012) (ordering disclosure of recipients of preservation notice and search terms, and that "any other information relevant to the scope and depth of the preservation or the search must be disclosed in detail"); *Cannata v. Wyndham Worldwide Corp.*, No. 2:10-cv-00068-PMP-VCF, 2011 WL 5598306, at *2 (D. Nev. Nov. 17, 2011) (Ferenbach, Mag. J.) (compelling disclosure of "information surrounding the litigation hold" including recipients and "kinds and categories of ESI" requested).

[152] *See Kleen Prods. LLC v. Packaging Corp. of Am.*, No. 10 C 5711, 2012 WL 4498465, at *8, *19 (N.D. Ill. Sept. 28, 2012) (Nolan, Mag. J.) (granting defendant's motion for protective order where defendant voluntarily disclosed information relating to its preservation notice and plaintiffs "violated the spirit of cooperation" by using that information to request additional discovery).

[153] *Katiroll Co., Inc. v. Kati Roll & Platters, Inc.*, No. 10-3620, 2011 WL 3583408, at *4 (D.N.J. Aug. 3, 2011).

[154] *Id.* at *4.

[155] *Id.* at *4 n.2.

[156] No. 10-1383, 2011 WL 6029983 (E.D. Pa. Dec. 5, 2011).

[157] *Id.* at *6.

[158] *Id.* at *11.

[159] *E.E.O.C. v. Original Honeybaked Ham Co. of Georgia, Inc.*, No. 11-cv-02560-MSK-MEH, 2012 WL 5430974, at *2 (D. Colo. Nov. 7, 2012) (Hegarty, Mag. J.).

[160] *Id.* at *2-*3.

[161] *Tompkins v. Detroit Metro. Airport*, 278 F.R.D. 387, 388 (E.D. Mich. 2012); *see also Howell v. Buckeye Ranch, Inc.*, No. 2:11-cv-1014, 2012 WL 5265170, at *1 (S.D. Ohio Oct. 1, 2012) (deeming overbroad a discovery request for all user names and passwords for every social media site).

[162] *Id.*; *see also Winchell v. Lopiccolo*, No. 7397/2012, 2012 WL 5933033 (N.Y. Sup. Ct. Oct. 19, 2012) ("[D]igital fishing expeditions are no less objectionable than their analog antecedents.")(internal quotation marks omitted).

[163] *Largent v. Reed*, No. 2009-1823, 2011 WL 5632688, at *8 (Pa. Ct. C.P. Nov. 8, 2011).

[164] *See, e.g., Tompkins*, 278 F.R.D. at 389.

[165] *Largent*, 2011 WL 5632688, at *8.

[166] *Id.* at *7.

[167] *See, e.g., Thompson v. Autoliv ASP, Inc.*, No. 2:09-cv-01375-PMP-VCF, 2012 WL 2342928, at *4-*5 (D. Nev. June 20, 2012) (Ferenbach, Mag. J.).

[168] *See, e.g., Anthony v. Atlantic Grp., Inc.*, Nos. 8:09-cv-02383-JMC, 8:09-cv-02942-JMC, 2012 WL 4009490, at *2 (D.S.C. Sept. 12, 2012) (finding it would subject defendants to an "unnecessary burden" to require them to "seek this information from the relevant service providers").

[169] No. 11 Civ. 4374 (PGG)(FM), 2012 WL 1197167, at *5 (S.D.N.Y. Apr. 5, 2012).

[170] *See, e.g., Juror Number One v. Superior Court*, 142 Cal.Rptr.3d 151, 158 (Cal. Ct. App. 2012) ("[SCA] protection applies only as to attempts . . . to compel Facebook to disclose the requested information. Here, the compulsion is on Juror Number One, not Facebook.").

[171] *Tienda v. State*, 358 S.W.3d 633, 641 (Tex. Crim. App. 2012).

[172] *See, e.g., State v. Eleck*, 23 A.3d 818, 822-25 (Conn. App. Ct. 2011).

[173] *Id.* at 823-24 (citing *Griffin v. State*, 19 A.3d 415 (Md. 2011)).

[174] *Tienda*, 358 S.W.3d 645-46.

[175] *See In re Nat'l Assoc. of Music Merchants, Musical Instruments & Equipment Antitrust Litig.*, MDL No. 2121, 2011 WL 6372826, at *2-*4 (MDL Dec. 19, 2011)).

[176] *See Standing Order for All Judges of the Northern District of California* (N.D. Cal. Nov. 27, 2012); *Guidelines for the Discovery of Electronically Stored Information* (N.D. Cal. Nov. 27, 2012); *In re Pilot Project Regarding Case Management Techniques for Complex Civil Cases in the S.D.N.Y.*, No. 11-388, Standing Order M10-468 (S.D.N.Y. Nov. 1, 2011); *Principles Relating to the Discovery of*

Electronically Stored Information (7th Cir. Aug. 1, 2010); *Guidelines for the Discovery of Electronically Stored Information* (D. Kan. Feb. 1, 2008) [hereinafter "Kansas Guidelines"].

[177] See Kansas Guidelines ¶ 4(d).

[178] *Checklist for Rule 26(f) Meet and Confer Regarding Electronically Stored Information*, at 1-2 (N.D. Cal.).

[179] *Da Silva Moore v. Publicis Groupe*, No. 11 Civ. 1279 (ALC) (AJP), 2012 WL 607412, at *22 (S.D.N.Y. Feb. 24, 2012).

[180] *Navajo Nation v. United States*, No. 06-945L, 2012 WL 5398792, at *3 (Fed. Cl. Oct. 17, 2012).

[181] No. 10-cv- 5711, 2012 WL 4498465, at *39 (N.D. Ill. Sept. 28, 2012).

[182] *Cf. Covad*, 254 F.R.D. at 149.

[183] No. 11-2090-CM-DJW, 2012 WL 940270 (D. Kan. Mar. 20, 2012).

[184] *Id.* at *11.

[185] *Id.*

[186] No. 11-cv-06637-RS-PSG, 2012 WL 5637611 (N.D. Cal. Nov. 15, 2012).

[187] *Id.* at *6.

[188] See, e.g., *Cannata v. Wyndham Worldwide Corp.*, No. 2:10-cv-00068-PMP-VCF, 2012 WL 528224, at *2 (D. Nev. Feb. 17, 2012) (noting that "[t]his District does not have the judicial resources to devote the time of a District or Magistrate Judge to review and approve search terms" and appointing a Special Master to oversee future discovery disputes); *Tadayon v. Greyhound Lines*, No. 10-1326 (ABJ/JMF), 2012 WL 2048257, at *6 (D.D.C. June 6, 2012) (ordering the parties to "meet and confer in person in a genuine, good faith effort to plan the rest of discovery . . . [and to] discuss and agree, if they can, on issues such as the format of any additional production").

[189] No. 11-cv-01683-LTB-MEH, 2012 WL 3984745 (D. Colo. Sept. 11, 2012).

[190] *Id.* at *2.

[191] See e.g., *Larsen v. Coldwell Banker Real Estate Corp.*, No. SACV 10-00401-AG (MLGx), 2012 WL 359466, at *7 n.2 (C.D. Cal. Feb. 2, 2012) (Goldman, Mag. J.) ("Courts are increasingly referring to the Sedona Principles for guidance in matters regarding electronic discovery."); *Chen-Oster v. Goldman, Sachs & Co.*, 285 F.R.D. 294, 302 (S.D.N.Y. 2012) (applying Sedona Conference proportionality principles and granting in part plaintiffs' a motion to compel production of information contained in four personnel databases for which Goldman, Sachs had "exaggerate[d] the burden associated with extracting [the] data"). See also *Larson v. AT&T Mobility LLC*, 687 F.3d 109, 122 (3d

Cir. 2012) (praising the *Commentary on Proportionality* as "a set of guidelines that offer a framework for best electronic discovery practices" and applying its proportionality principles to help discern the contours of a "reasonable effort" in the class action context).

[192] *Chen-Oster*, 285 F.R.D. at 308; *see also Oseman-Dean v. Ill. St. Police*, No. 11 C 1935, 2011 WL 6338834, at *5-*7 (N.D. Ill. Dec. 19, 2011) (narrowing broad ESI requests by reducing the time frame at issue and limiting the request to specific custodians); *ADT Sec. Svcs., Inc. v. Pinancle Sec., LLC*, No. 10 C 7467, 2012 WL 2920985, at *2 (N.D. Ill. July 11, 2012) (Holderman, J.) (citing Seventh Circuit Electronic Discovery Committee, *Principles Relating to the Discovery of Electronically Stored Information*, Principle 1.03 (2010)) (affirming Magistrate Judge's denial of motion to compel search of ten additional employees' computers using additional search terms to comply with a not "reasonably targeted, clear, and as specific as practicable" discovery request).

[193] *See Chen-Oster*, 285 F.R.D. at 304-06 (granting plaintiff's motion to compel where a "substantial portion" of the alleged burden was allocated to assuring the data quality was "pristine" but where the court concluded that the "standard for the production of ESI is not perfection" and "it would be sufficient, and far less burdensome, to sample the data extracted to determine if there are systematic errors requiring further attention rather than to implement the comprehensive quality review apparently contemplated by Goldman Sachs"); *Kleen Prods. LLC v. Packaging Corp. of Am.*, No. 10 C 5711, 2012 WL 4498465, at *18 (N.D. Ill. Sept. 28, 2012) (Nolan, Mag. J.) (recommending the use of sampling methods "[i]f feasible and cost efficient" in the event plaintiff eventually sought the recovery of defendant's archived media). *See also AT&T Mobility*, 687 F.3d at 131 n.33 (approving the use of statistical sampling methods to make an accurate proportionality determination, noting that "the value of much discovery information will be largely unknown until tested").

[194] *Kleen Prods.*, 2012 WL 4498465, at *5-*6 (Nolan, Mag. J.) (denying motion to compel premature production of backup tapes because although backup tapes are "presumptively inaccessible" and defendants provided affidavits indicating that restoration of backup tapes would cost each defendant at least \$200,000 (with some estimates well over \$1,000,000), "in any event" plaintiff's request was premature as it had completed only 20% of its first level review of defendants' documents and needed to wait to evaluate the sufficiency of information obtained from accessible sources first); *United States ex rel. Ifrah v. Cmty. Health Ctr. Buffalo, Inc.*, No. 05-CV-237A(F), 2012 WL 3136485, at *4 (W.D.N.Y. Aug. 1, 2012) (Foschio, Mag. J.) (denying plaintiff's motion for costs associated with reviewing defendant's backup tapes holding that information that may have been contained on overwritten backup tapes was not reasonably accessible to defendant (a regional not-for-profit health services provider) where the overwritten files could be recovered only through the use of a "specialized and expensive [forensic] software tool" at a cost of at least \$48,000 plus annual maintenance); *Murray v. Coleman*, No. 08-CV-6383, 2012 WL 4026665, at *2 (W.D.N.Y. Sept. 12, 2012) (Feldman, Mag. J.) (delaying ruling on plaintiff's motion to compel the production of defendant's DOCS document and email retention system until defendant filed an affidavit setting forth "(1) the document/email retention policy used by DOCS currently and during the relevant time periods, (2) the dates of emails 'reasonably accessible' for production in this litigation, (3) the back up or legacy system, if any, used by DOCS to preserve or archive emails that are no longer 'reasonably accessible' and whether responsive documents or data may potentially be found on such back up or legacy systems, (4) whether accessing archived or back up emails would be unduly burdensome or costly and why, and (5) the date

when a litigation hold or document preservation notice was put in place by DOCS regarding this matter and either a copy of or a description of the preservation or litigation hold utilized by DOCS").

[195] *Id.* (noting somewhat incredulously that counsel appeared "unprepared and slack-jawed at the thought of providing a foundation for th[eir] belief" that responsive documents would be found on the inaccessible media and that "[c]learly, providing such a foundation would have gone a very long way toward demonstrating the good cause required for the Court to force GE to make the search *despite that* the tapes are not reasonably accessible").

[196] *See Peter Kiewit Sons', Inc. v. Wall Street Equity Grp., Inc.*, No. 8:10CV365, 2012 WL 1852048, at *18-*20 (D. Neb. May 18, 2012) (Zwart, Mag. J.) (granting plaintiff's motion for costs for the forensic examination of defendant's computers and rejecting defendant's argument that the data sought was inaccessible because a key word search by its most "computer literate" employee failed to discover certain documents and it ultimately took plaintiff's professional vendor several weeks to recover the documents where defendant's employee had no formal computer science training, it offered no evidence that it ever spoke with a forensic examiner to evaluate the cost and burden of thoroughly searching the server, and "the length of [the professional vendor's] search ha[d] very little to do with whether the requested data was accessible").

[197] *Chen-Oster v. Goldman, Sachs & Co.*, 285 F.R.D. 294, 301 (S.D.N.Y. 2012) (Francis, Mag. J.) (collecting cases and granting plaintiff's motion to compel production of computerized compensation, promotion, and performance evaluation data spanning four databases and dating back over ten years because defendant failed to demonstrate that "the cost and burden associated with extracting ESI from any of the relevant databases [was] a function of the means of storage[,] rather than simply a function of volume"); *Adair v. EQT Prod. Co.*, No. 1:10cv00037, 2012 WL 1965880, at *4-*5 (W.D. Va. May 31, 2012) (Sargent, Mag. J.) (denying defendant's motion for protective order, ordering the production of admittedly accessible data, and refusing to shift the cost of review and production to plaintiff where although the data at issue exceeded 400 GB and would cost in excess of \$4.7 million to process, review, and produce, the court concluded that no review was necessary given that a claw-back provision was in place and defendant could sort the data by custodian, date, and use keyword searches to identify potentially relevant documents); *Indep. Mktg. Group v. Keen*, No. 3:11-cv-447-J-25MCR, 2012 WL 207032 (M.D. Fla. Jan. 24, 2012) (Richardson, Mag. J.) (granting in part defendant's motion to compel search and review of plaintiff's server noting that plaintiff could not contend its server was inaccessible because plaintiff itself identified the server in its initial disclosures as a source of potentially relevant information and because inaccessibility is generally reserved for backup tapes and fragmented or damaged data, "all of which require significant manipulation and reconstruction to become usable for responding to discovery requests").

[198] *See, e.g., Kilopass Tech. Inc. v. Sidense Corp.*, No. C 10-02066 SI, 2012 WL 1534065 (N.D. Cal. May 1, 2012) (holding that defendant did not take reasonable steps to prevent disclosure where "[defendant] failed to disclose to [its counsel] all of its prior attorneys," "[t]he third party vendor did not run the search terms against all production batches of documents," and defendant's counsel's "spot checking on various privilege search terms in various batches of documents" . . . allowed more than 1 in 50 privileged documents to escape their attention"); *U.S. Home Corp. v. Settlers Crossing, LLC*, Civil Action No. DKC 08-1863, 2012 U.S. Dist. LEXIS 101778 (D. Md. July 23, 2012) (holding that

"two brief phone calls" between plaintiffs' law firms regarding compliance with subpoena "does not constitute a reasonable precaution to protect the attorney-client privilege or work product protection").

[199] *Inhalation Plastics, Inc. v. Medex Cardio-Pulmonary, Inc.*, Civil Action No. 2:07-CV-116, 2012 WL 3731483, at *4 (S.D. Ohio Aug. 28, 2012) (King, Mag. J.) (holding that defendant failed to establish reasonable steps to prevent disclosure where defendant did not specify "who reviewed the production, what steps were taken to review the documents for privilege or whether the production was different in form from prior productions"; "did not produce a privilege log"; and "failed to adequately address the alleged inconsistencies between [the subject] production and all prior productions"); *see also Excel Golf Prods. v. MacNeill Eng'g Co.*, No. 11 C 1928, 2012 WL 1570772, at *3 (N.D. Ill. May 3, 2012) ("Merely listing the volume of production will not suffice [to demonstrate whether a party took reasonable steps to prevent disclosure.]").

[200] No. 11 CVS 933, 2012 WL 3061862, at *10 (N.C. Super. Ct. July 26, 2012).

[201] *Id.* at *11. *But see D'Onofrio v. Borough of Seaside Park*, Civil Action No. 09-6220 (AET), 2012 WL 1949854, at *11 (D.N.J. May 30, 2012) (Bongiovanni, Mag. J.) (holding that defendants' counsel did not waive privilege by delegating to a non-attorney clerical employee "the task of physically separating the documents flagged as privileged from the non-privileged documents and sending the non-privileged information to a vendor to be scanned on a disc for production").

[202] *See D'Onofrio*, 2012 WL 1949854, at *12-*16 (holding that defendants did not undertake reasonable efforts to rectify inadvertent disclosure where, "despite being on notice that something was amiss with their production of [potentially privileged documents], [defendants] failed to promptly re-check their production of same"); *Inhalation Plastics*, 2012 WL 3731483, at *5 (holding that defendant's notice that it intended to assert a claim of privilege as to 347 documents did not constitute reasonable efforts to rectify disclosure where defendant "did not identify any particular documents covered by the privilege, did not provide a proper privilege log and, beyond conclusory statements, . . . did not state a basis for the claimed privilege"), *Jacob v. Duane Reade, Inc.*, No. 11 Civ. 0160(JMO)(THK), 2012 WL 651536 (S.D.N.Y. Feb. 28, 2012) (Katz, Mag. J.) (holding that "Defendants did not act promptly or diligently in rectifying [an] inadvertent disclosure" because "even when Defendants' counsel became aware of the email which, on its face, suggested a privilege argument, he allowed a witness to be deposed about it, failed to make efforts to ascertain the identity of [defendants' in-house counsel], and failed to raise a privilege objection or demand the email's return for more than two months").

[203] *Adair v. EQT Prod. Co.*, Nos. 1:10CV00037, 1:10CV00041, 2012 WL 2526982, at *5 (W.D. Va. June 29, 2012) (rejecting defendant's request to shift the cost of traditional manual document review "because those costs could be mitigated by the use of electronic searching and production, together with the protections of the [previously entered] Protective and Clawback Orders"); *S2 Automation LLC v. Micron Tech., Inc.*, No. CIV 11-0884 JB/WDS, 2012 WL 3150387 (D.N.M. July 23, 2012) (entering claw-back order at defendant's request and noting, "In situations where a party can waive attorney-client privilege or work-product privilege by disclosure, producing parties will produce discovery more slowly to protect privileges, which ultimately increases costs for both parties"); *U.S. Bank Nat'l Ass'n v. PHI Variable Ins. Co.*, No. 12 Civ. 6811(CM)(JCF), 2012 WL 5395249 (S.D.N.Y.

Nov. 5, 2012) (Francis, Mag. J.) (declining to shift costs of reviewing documents for privilege, but entering a claw-back order to give producing parties "the option of conducting a more economical analysis while minimizing the risk of waiver").

[204] *See Pensacola Firefighters Relief Pension Fund v. Merrill Lynch, Inc.*, No. 3:09cv53/MCR/MD, 2011 WL 3512180 (N.D. Fla. Jul. 7, 2011) (Davis, Mag. J.).

[205] *Pensacola Firefighters*, 2011 WL 3512180, at *3.

[206] *Id.* at *2-*3.

[207] *See id.* at *7-*8.

[208] *See, e.g., Aventa Learning, Inc. v. K12, Inc.*, No. 830 F. Supp. 2d 1083 (W.D. Wash. 2011); *Hanson v. First Nat'l Bank*, No. 5:10-0906, 2011 WL 5201430 (S.D.W. Va. Oct. 31, 2011)).

[209] *See Chechele v. Ward*, No. CIV-10-1286-M, 2012 WL 4481439 (W.D. Okla. Sept. 28, 2012).

[210] *Id.* at *1.

[211] *Id.*

[212] *Id.*

[213] *Id.* at *2; *see also Dombrowski v. Governor Mifflin Sch. Dist.*, Civil Action No. 11-1278, 2012 WL 2501017, at *6 (E.D. Pa. June 29, 2012) (holding that plaintiff did not have a reasonable expectation of privacy in personal emails--including emails between plaintiff and her counsel--found on employer's computer and network server, where employer's privacy policy "specifically contemplated the monitoring of employees' [employer]-owned computers and email" and provided employer "a right of access to employees' computers, including email that could be found on the computers").

[214] *See American Bar Association, Standing Committee on Ethics and Professional Responsibility, Formal Opinion 11-4569, Duty to Protect the Confidentiality of Email Communications with One's Client* (Aug. 4, 2011).

[215] *See Citizens for Responsibility and Ethics in Washington v. SEC*, 858 F. Supp. 2d 51, 54, 57-63 (D.D.C. 2012).

[216] *Compare United States ex rel. Baker v. Cmty. Health Sys., Inc.*, Civ. No. 05-279 WJ/ACT, 2012 WL 5387069, at *6-*9 (D.N.M. Oct. 3, 2012) (imposing sanctions because the government's litigation hold was "woefully inadequate and go beyond mere negligence" and defendants were prejudiced thereby), *with SEC v. Mercury Interactive LLC*, No. 3:07-cv-02822-WHA (JSC), 2012 WL 3277165, at *7-*11 (N.D. Cal. Aug. 9, 2012) (declining to impose sanctions where the SEC deleted over five million pages of data due to a misunderstanding and defendants did not show sufficient prejudice).

[217] Revisions to FTC Rules of Practice, 77 Fed. Reg. 59,294, 59,305-07 (Sept. 27, 2012) (to be codified at 16 C.F.R. § 2.7).

[218] The Joint Electronic Technology Working Group, *Recommendations for ESI Discovery Production in Federal Criminal Cases* (Feb. 10, 2010), <http://www.fd.org/docs/litigation-support/final-esi-protocol.pdf>.

[219] *Id.*

[220] See Eric Topor, *Joint Federal Criminal E-Discovery Protocol Places Cooperation Above Motion Filings*, Bloomberg BNA Digital Discovery & e-Evidence (Mar. 1, 2012), <http://ediscovery.bna.com>.

[221] Internal Revenue Service, *Reissuance of Guidance for Complying with E-Discovery Rules*, SBSE-05-0912-075 (Sept. 11, 2012), available at <http://www.irs.gov/PUP/foia/SBSE-25-0912-075.pdf>.

[222] Office of Management and Budget, *Managing Government Records Directive 3* (Aug. 24, 2012), available at <http://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-18.pdf>.

[223] *Id.* at 3-4.

[224] *Id.* at 5.

[225] 132 S. Ct. 945 (2012).

[226] *Id.* at 949.

[227] See, e.g., *United States v. Pineda-Moreno*, 688 F.3d 1087, 1091 (9th Cir. 2012) (applying good-faith exception based on conflicting precedent prior to *Jones*).

[228] S. 1212, 112th Cong. (2011)

[229] S. 1212 § 2.

[230] 18 U.S.C. § 2701 *et seq.* See Joyce E. Cutler, *Government Requests to Google for User Data Up in First Half of 2012*, Bloomberg BNA Digital Discovery & e-Evidence (Nov. 22, 2012), <http://ediscovery.bna.com>.

[231] 18 U.S.C. § 2703(b)(1)(B), § 2703(d) (access to content records over 180 days old also requires notice to the subscriber).

[232] 18 U.S.C. § 2703(a).

[233] Compare *Juror Number One v. Super. Ct. of Sacramento Cnty.*, 206 Cal. App. 4th 854, 863-64 (2012) (noting that Facebook posts may be protected from disclosure under the SCA) with *State v.*

Harris, 949 N.Y.S. 2d 590, 593–94 (Crim. Ct. 2012) (holding that Twitter users have no reasonable expectation of privacy in "tweets," which are not protected by the SCA).

[234] 846 F. Supp. 2d 384, 401 (D. Md. Mar. 1, 2012).

[235] *Id.*

[236] Electronic Communications Privacy Act Amendments of 2012 [hereinafter "ECPA Amendments Act"], S. 2471, 112 Cong. (2012).

[237] S. 2471 § 203; *see also* Amy E. Bivens, *ECPA Update Would Extend Warrant Mandate for Police to Access Electronic Information*, Bloomberg BNA Digital Discovery & e-Evidence (Aug. 16, 2012), <http://ediscovery.bna.com>.

[238] *See* Charlie Savage, *Panel Approves a Bill to Safeguard Email*, N.Y. Times, Nov. 30, 2012, at B7; Alexei Alexis, *Leahy Unveils Revisions to ECPA Modernization Package*, Bloomberg BNA Digital Discovery & e-Evidence (Dec. 6, 2012), <http://ediscovery.bna.com>.



Gibson Dunn & Crutcher's lawyers are available to assist in addressing any questions you may have regarding the issues discussed in this update. The Electronic Discovery and Information Law Practice Group brings together lawyers with extensive knowledge of electronic discovery and information law. The group is comprised of seasoned litigators with a breadth of experience who have assisted clients in various industries and in jurisdictions around the world. The group's lawyers work closely with the firm's technical specialists to provide cutting-edge legal advice and guidance in this complex and evolving area of law. For further information, please contact the Gibson Dunn lawyer with whom you work or any of the following Chairs of the Electronic Discovery and Information Law Practice Group:

*Gareth T. Evans - Practice Co-Chair, Los Angeles/Orange County (949-451-4330,
gevans@gibsondunn.com)*

Jennifer H. Rearden - Practice Co-Chair, New York (212-351-4057, jrearden@gibsondunn.com)

G. Charles Nierlich - Practice Co-Chair, San Francisco (415-393-8239, gnierlich@gibsondunn.com)

© 2013 Gibson, Dunn & Crutcher LLP

Attorney Advertising: The enclosed materials have been prepared for general informational purposes only and are not intended as legal advice