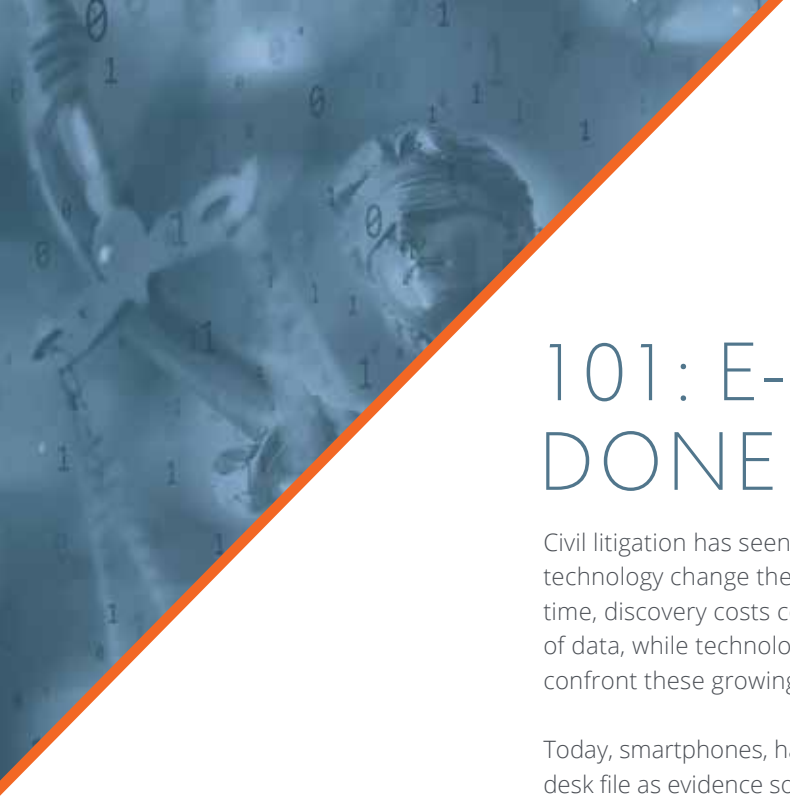

GUIDANCE SOFTWARE™

101: E-DISCOVERY DONE RIGHT

Civil litigation has seen sweeping changes as evidence goes digital and developments in technology change the way business organizations use and store information. At the same time, discovery costs continue to skyrocket with multiplication of the amounts and sources of data, while technology and the Federal Rules of Civil Procedure (FRCP) also evolve to confront these growing costs.

Today, smartphones, hard drives, and removable media have replaced the file cabinet or desk file as evidence sources. Moreover, digital information is fundamentally different from yesterday's banker's boxes of paper documents, raising new issues around, e.g., preservation and metadata. Accordingly, today's civil litigator finds a discovery practice that demands new ways of thinking and poses a different set of risk factors.

This E-Discovery 101 white paper explores best practices in three of the main phases in electronic discovery and investigations:

1. Litigation Holds and Preservation;
2. Identification, Collection, and Processing; and
3. Document Review.

Businesses that fail to understand these issues may find themselves at a tactical disadvantage in litigation or face heightened regulatory risk. Some have become cautionary tales for their industry peers.

See e.g., Apple, Inc. v. Samsung Elecs. Co. Ltd. (litigation hold and preservation);[i]

National Day Laborer Organizing Network et al. v. United States Immigration and Customs Enforcement Agency, et al. (collection and processing);[ii] and

In re Delta/Airtran Baggage Fee Antitrust Litig. (document review).[iii]

101: Litigation Holds and Preservation

Duty to Preserve

The duty to preserve is a frequent battleground of motion practice. Organizations must preserve data once they have actual or constructive notice that the evidence is or may be relevant to future litigation.[iv]

It is now well-established that courts have the inherent and statutory[v] authority to sanction a party for the loss of evidence where there has been a failure to preserve.vi Indeed, a 2010 survey found that nearly half of all e-discovery sanctions result from a failure to preserve.[vii]

Recent cases bear witness to the criticality of proper preservation in mitigating sanctions risk. For example, a recent 2013 Ohio state case involving a suit by a nursing-home owner against its former CEO illustrates how a failure to preserve can dramatically affect litigation.[viii] The Court dismissed Plaintiff's complaint because Plaintiff failed to preserve Defendant's hard drive (even after Defendant's counsel advised Plaintiff of its preservation obligation by letter). This dismissal was affirmed on appeal.

Scope of Preservation Duty

Once the duty to preserve attaches, an organization should try to determine the scope of preservation. This scope must include potentially relevant data, i.e. all data that could support claims or defenses in the dispute. Determining the scope of preservation almost always requires identifying custodians and repositories of relevant data. Analyzing communication patterns is one way to identify custodians in a potential dispute. This could involve interviews, understanding terms of art, and knowing the technology that potential custodians use to communicate. Of course, an organization should also endeavor to understand what the relevant sources of data may be (i.e., network shares, severs, proprietary data sources, cloud data, laptops, desktops, personal devices, removable media, etc.). One useful tool for eliciting this information is a litigation-hold questionnaire.

Corporate counsel should issue written litigation-hold notices to potential custodians when the organization reasonably anticipates litigation to ensure preservation of relevant evidence. A litigation-hold letter or notice should inform a potential custodian of his or her duty to prevent the deletion or destruction of any potentially relevant information. Depending on the case, a litigation-hold notice may also include a questionnaire to elicit information that could aid counsel in reasonably and defensibly narrowing the collection of evidence to those custodians and sources likely to contain relevant evidence.

Timely Issuance of Litigation Hold

A written notice should be considered a baseline best practice for a defensible process and should issue as soon as an organization reasonably anticipates litigation. This is a crucial step in establishing and recording reasonable efforts to preserve. Indeed, courts increasingly focus on whether written litigation hold notice was timely in a considering the good faith and defensibility of a discovery process. For example, in the recent case of Sekisui American Corp. v. Hart,[ix] the court sanctioned a Plaintiff who failed to issue a pre-complaint preservation notice because it should have reasonably anticipated litigation at that time. Failure to issue a written notice may result in a finding of negligence or worse.[x]

"Philip Morris received a $2.75 million sanction for failing to comply with document preservation order"

Although courts apply a case-by-case analysis on whether failure to issue a written hold merits sanctions, it is still best practice to issue a written hold to key players and potential custodians early in the discovery process.xi Issuing a written litigation hold should be standard practice for any size matter.[xii]

Litigation-Hold Compliance

Issuing a written hold notice is important, but not sufficient. The purpose of a litigation hold is to prevent destruction of evidence, and the hold must be enforced. The seminal case of In re Prudential Ins. Co. of Am. Sales Practices Litig. illustrates the importance of ensuring the hold notice is followed after being issued. [xiii] There the court sanctioned Prudential in the amount of one million dollars, noting that after issuing a hold, "Prudential top management . . . [did not take] an active role in formulating, implementing, communicating, or conducting a document retention policy." [xiv] Thus, the court ordered sanctions despite no finding of intentional destruction of evidence because of Prudential's "haphazard and uncoordinated approach to document retention." [xv]

Similarly, in United States v. Philip Morris USA, Inc., the court sanctioned Philip Morris $2.75 million for failing to comply with a document preservation order.[xvi] These cases demonstrate the risk to businesses of failing to take steps to ensure preservation after issuance of a written litigation hold. They serve as a warning that a written notice alone may be insufficient where an organization fails to take further steps to ensure compliance and evidence is subsequently lost or destroyed.

Accordingly, counsel should encourage processes that identify key players early on and make contemporaneous records regarding such decisions.[xvii] In addition, it is a best practice to reiterate to a client that using personal devices such as thumb drives or personal laptops for work may subject such personal devices to discovery. In general, counsel should encourage clients to adopt processes that are planned, repeatable, and auditable rather than ad-hoc.

Spoliation Sanctions

"Spoliation is the destruction or significant alteration of evidence, or failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation."[xviii] The Second Circuit has articulated a widely adopted three-factor analysis regarding granting a motion for spoliation sanctions (an adverse inference). Such a motion may be granted when:

1. The respondent was obligated to preserve evidence when the spoliation occurred
2. The respondent destroyed evidence with a "culpable state of mind," i.e. it knew or should have known that it was obligated to preserve the evidence
3. The movant suffered prejudice, i.e. the spoliated evidence was relevant to claims or defenses such that a reasonable trier of fact could find that it could support that claim or defense.[xix]

Real-World Case: Hart v. Dillon Cos., 2013 U.S. Dist. LEXIS 95441 (D. Colo. July 9, 2013)

This case involved allegations of wrongful termination:

- Defendants terminated a long-time employee in August 2011 and secretly recorded an interview with the employee by Defendants' investigator prior to termination.
- The former employee filed an EEOC discrimination complaint around November 2011 alleging her termination was retaliation for prior testimony in a different matter.
- Defendants failed to issue a litigation hold until March 2012, during which time the investigator recorded over the interview and irretrievably deleted it.

The Court found the defendant "highly culpable" for the delay in issuing a litigation hold. It further held that Defendants' conduct rose to willfulness or at best was grossly negligent. Accordingly, the Magistrate Judge granted Plaintiff's sanctions motion.

Real-World Case: Sekisui American Corp. v. Hart, No. 12-Civ-3479 (SAS) (FM) (S.D.N.Y. Aug. 15, 2013)

This case involved an action against former executives for breach of contract:

- Plaintiff sent a Notice of Claim to Defendant dated October 14, 2010.
- Plaintiff initiated a litigation hold around January of 2012, nearly two years later.
- During the intervening period, Plaintiff lost evidence, including the e-mail boxes of the former executives sued in the action.
- Plaintiff then commenced an action on May 2, 2012, five months after issuing a hold.

Judge Scheindlin reversed Magistrate Judge Maas' prior recommendation that no sanctions should issue absent a finding of bad faith. In granting the motion for sanctions, Judge Schiendlin focused on the failure to issue a timely hold and the likely relevance of the evidence that had been destroyed.

Other circuits follow similar tests. For example, the District Court of Colorado recently framed the factors as: (1) relevance of the evidence to an issue at trial; (2) existence of a duty to preserve because a party knew, or should have known, that litigation was imminent; and (3) prejudice resulting from the destruction of the evidence.[xx] To mitigate risk of spoliation sanctions, business organizations should be vigilant in ensuring their preservation practices do not run afoul of these factors.

101: Identification, Collection, and Processing

To reduce risks and costs, potentially relevant electronically stored information (ESI) and its associated metadata should be collected in a manner that is legally defensible, targeted, proportionate to the matter, auditable, and efficient. The FRCP govern aspects of the identification and collection of ESI, and counsel should become familiar with these rules. Here, we provide the reader with a high-level overview of the relevant FRCP rules and related best practices.

Federal Rules of Civil Procedure and ESI

Amendments to the FRCP in 2006 formally brought ESI into the scope of the pre-existing discovery rules. For example, Rule 34 was expanded in 2006 to explicitly include "any designated documents or electronically stored information" within the scope of a request for production.[xxi] The Advisory Committee Notes emphasize that Rule 34 now applies to a broad scope of information: "The change clarifies that Rule 34 applies to information that is fixed in a tangible form and to information that is stored in a medium from which it can be retrieved and examined." Similarly, 2006 also saw amendments to Rule 26 to ensure that part of the meet-and-confer process specifically addresses ESI.[xxii] In turn, amendments to Rule 16 expressly indicate that a court's scheduling order may include "provisions for disclosure or discovery of electronically stored information." [xxiii] Current proposals for amending may affect issues concerning identification and collection, as noted below.

The FRCP establishes a default timeline regarding discovery absent a stipulation or court order:

Within 14 days - Parties must make their initial disclosures either at or within 14 days of their Rule 26(f) meet and confer. A different time may be determined by stipulation or court order.iii Fed. R. Civ. P. 26(a)(1)(C).

At least 21 days before - The Rule 26(f) meet and confer must be "as soon as practicable" and at least 21 days before a Rule 16 scheduling conference and order. FRCP Rule 26(f)(1). A court can order a different schedule pursuant to the Rules.

Within 120 days - The judge must issue the scheduling order as soon as practicable, but in any event within the earlier of 120 days after any defendant has been served with the complaint or 90 days after any defendant has appeared. FRCP Rule 16(b). Note that under amendments currently under consideration, this time period would be shortened to the lesser of 60 days after service of the Complaint or 90 days after any defendant has appeared.

Identification

FRCP Rule 26 specifically requires a party to identify all ESI within its possession, custody, or control to support any of its claims or defenses in a lawsuit.[xxiv] Accordingly, counsel should work to understand the sources and amounts of potentially relevant ESI from the onset of the case.

Effective Client Meetings - It is a best practice for attorneys to discuss sources and types of ESI with their clients before making representations to the Court based on "reasonably available" information as required by FRCP Rule 26(a). Indeed, FRCP Rule 26 specifically states that a party is not excused from its obligation to make these disclosures merely because it has "...not fully investigated the case[,] . . . challenge[s] the sufficiency of another party's disclosures or . . . another party has not made its disclosures."[xxv] Failure to meet this obligation to identify ESI that supports a claim or defense can result in the discovery being excluded from a case.[xxvi]

Effective Early Case Assessment - Early case assessment (ECA) software tools can be used by litigants to identify custodians, date ranges, topics, and types of ESI likely to be relevant to a dispute. The use of ECA software empowers attorneys to determine which ESI may support their claims or defenses, thereby assisting with the initial disclosures required by FRCP Rule 26. Early case assessment can also reduce downstream costs and risks by giving counsel greater ability to intelligently and appropriately tailor a collection to the issues in the case.

Effective Conferences with an Adversary - FRCP Rule 26(f) requires parties to meet; "discuss any issues about preserving discoverable information; develop a proposed discovery plan"; "agree on the proposed discovery plan; and submit to the court within 14 days." This Rule 26(f) conference is vital to developing a discovery plan, which should include the scope of preservation and agreed-upon collection methodologies. Appropriate care should be taken to communicate clearly with an adversary so that issues can be identified and resolved at an early stage.

Collection

Since the 2006 amendments to the FRCP, ESI collection tools have dramatically evolved to facilitate automated targeted collections of ESI from multiple data sources. Instead of employing manual collections and forensic images of every custodian hard drive or server, automated solutions facilitate efficient collections from multiple custodians and data sources within an organization. This efficient methodology saves organizations time and money without sacrificing legal defensibility or forensic soundness.

However, counsel may still not be attuned to the nuances of collection terminology, leading to unintentionally ambiguous instructions to a service provider, such as to "forensically copy" a hard drive and "MD5 hash it." Understanding such nuances, e.g., the difference between a forensic image or collection and a forensically sound process can be critical to appropriately tailoring collection to the matter in dispute and ensuring reasonable cost allocations. Here, we provide a guide to some key collection concepts to clarify these issues.

Defensible Forensic Process - ESI must be copied with a defensible forensic process. Such a process can take several forms, including a "targeted" or "logical" collection, where specific information is copied from media, or a "full disk image," where the entire contents of a hard drive are copied. Note that a full disk image may result in over-collection of data, leading to cost overruns or potential errors later in the discovery process.

Full Disk Imaging and Targeted or Logical Collection - Often, counsel assume that a forensically defensible process requires full disk imaging. However this procedure is excessive and unnecessary for the majority of civil litigation matters. Nonetheless, in a desire to mitigate the risk of overlooking potentially relevant evidence, service providers may advise business organizations to employ full disk imaging. This advice may be very costly given both the upfront costs of full disk imaging and the downstream costs of processing, hosting, and reviewing far greater data than necessary. Counsel should consider these costs and more efficient options with today's available technology to do a targeted or logical collection.

There may be instances when a full disk image is advisable, particularly where privacy concerns are lessened or there is a possibility of fraud or custodian non-cooperation. Such instances include:

- Suspected criminal activity
- Suspected fraud by custodians
- Certain types of internal investigations
- Certain regulatory inquiries.

However, even in these instances, a well-scoped logical or targeted collection may achieve the same results at a lower cost.

Forensically Sound Collection - Ultimately, what matters more than method of collection is its forensic soundness. The essence of a forensically sound process is a defensible collection—one that will stand up to rigorous questioning in court. Many collection tools, such as EnCase® Forensic, EnCase® Enterprise, and EnCase® eDiscovery, can run a defensible collection by ensuring that all files and associated metadata are kept intact and unchanged in the collection process. This process can be verified via a digital fingerprint called a "hash code." An MD5 hash code is one type of industry standard hash code for identifying and authenticating ESI. This code can be used, inter alia to authenticate ESI in court as admissible evidence.

Processing

Data that has been collected in a forensically defensible manner generally must be processed before review. This usually involves "ingesting" the data into a software program designed to extract the text and relevant metadata, and in some instances create native, PDF, or image (TIFF) files in a format that facilitates review.[xxvii]

If done intelligently, processing can also reduce data for upload into a review platform, because processing can also involve narrowing data, e.g., by file types, date ranges, and de-duplication. E-mail messages can also be "threaded" using software tools such as EnCase eDiscovery, so that messages appear grouped in conversation threads, allowing quick review of groups of e-mails and attachments that is more efficient than individual review of each e-mail.

101: Document Review and Production

Document Review

It goes without saying that review is imperative prior to disclosure of documents to preserve privilege, ensure that only relevant evidence is produced, protect a client and counsel's litigation strategy, and more generally to protect a client's interests in privacy and confidentiality. In the electronic environment in which we live and conduct business there is absolutely no way to start, defend, or litigate a case without conducting a review of ESI. Of course, from a process-efficiency and risk-mitigation perspective, "[t]he objective of review in ediscovery is to identify as many relevant documents as possible, while reviewing as few non-relevant documents as possible."[xxviii]

As noted above, efficient review begins before the review even starts—with an intelligently scoped collection (and even before that, with well-planned information governance policies and procedures). However, technologies exist and continue to develop to further reduce and tailor the review process to minimize cost and time. Concept clustering, analytics, e-mail threading, and other intelligent organization of data can greatly assist with efficient review. Moreover, software designed for multi-matter management, such as EnCase eDiscovery, can reduce review time by identifying documents previously reviewed in other matters and preserving the results of prior review. This saves counsel from re-inventing the wheel every time an ESI review is undertaken.

Multi-matter management features can also assist in-house counsel in getting a bird's-eye view of review costs by firm and hours spent on review over multiple cases. This type of data may assist with intelligent cost allocations and dialogue with outside counsel.

Form of Production

FRCP Rule 34(b)(2)(e) states that, absent other agreement or court order, ESI should be produced in the form in which it is "ordinarily maintained" or a "reasonably usable" form. The Advisory Committee Note reiterates this requirement. Issues regarding the form of production are still litigated today, as a recent 2013 order from Magistrate Judge Ross Walters on the form of production attests.

Industry-standard production formats have developed around this default FRCP rule as repeated litigation tests procedures for ESI production. Three formats comprise the vast majority of productions. These are "native format," "static image files," or a blend of the two. Files may further be provided in a "load file," i.e., in a form that allows files to be quickly ingested by an industry-standard review tool.

Native Files - A "native file" is a file in its original format, for example, a Microsoft Word document produced as a .doc or .docx file or a Microsoft Excel document produced as an .xls or .xlsx file. Native production usually requires minimal processing, saving time and money. Moreover, a native production provides "original" data that may include substantive and embedded metadata. For this reason, native file data can be used to great benefit in litigation support review applications from basic searches to advanced analytics, including data clustering and concept or faceted searching. Indeed, there are some types of files, such as Microsoft Excel spreadsheets, which are difficult or impossible to fully review in an imaged format. It is customary for parties to request native formats for such file types. When agreeing to produce ESI in native format, it is a best practice to try to reach agreement on which attendant metadata will be produced so that counsel can limit production of metadata to only what is agreed upon, and thereby reduce the risk of overproduction or compromising a client's interests.

"It is best practice to try to reach agreement on which attendant metadata will be produced for that counsel can limit production of metadata to only what is agreed upon."

Static Images - Static images may be thought of as most analogous to the paper productions of the pre-electronic discovery era. These files are images of the output of the ESI, for example, an image of a Microsoft Word document will typically be an image of the such document as if the document had been printed on paper. Standard static image file formats include TIFF and PDF files.

Image production may be useful or even necessary if ESI exists in proprietary file formats that cannot be otherwise viewed. Static image files are also often used to mark up documents, for example, to redact, annotate, or Bates-stamp documents. Counsel review in internal investigations or outside counsel review may be facilitated by static image formats.

Some notes of caution should be sounded regarding static-image productions. Often service providers charge fees for converting files to static image formats. These fees may be charged per page and can be very costly: for example, in a sizeable production, a TIFF format production could be triple the cost of a native format production.

Furthermore, static images may make advanced analytic capabilities irrelevant because of lost metadata. Static images do not have the data richness of a native production, and may make review tools like concept clustering or faceted search useless. Accordingly, if files are produced as static images, it is a best practice to also produce extracted text and agreed-upon metadata. Failure to abide by this best practice may result in sanctions, as static images without metadata are more difficult and costly to review.[xxx]

Blended - Blended productions include both native and static image files. Usually these productions are made where counsel have agreed to produce certain files in native file format, such as Microsoft Excel spreadsheets. Other files are then produced as static images, particularly where redaction, annotation, or Bates stamping will be necessary (for example, in an outside counsel review). In some instances, seeking a protective order from the court may reduce the need for annotation and redaction, thereby reducing the cost of converting native files into static image files.xxxi Counsel should note, however that depending on the language in a protective order, it may still be necessary to use static image files to mark them with the appropriate level of confidentiality, e.g., "confidential" or "attorneys' eyes only," etc.

Preservation of Searchable Data - As noted above, absent an agreement or court order, parties should produce ESI in the form "ordinarily maintained" or in a "reasonably usable" form. Practically speaking, this often involves production in native format. Even where a non-native format is used, parties must take care not to degrade or delete searchable metadata. For example, a court held that production had not been made in a "reasonably usable" form where the producing party removed all metadata and searchable text by printing ESI as paper and then scanning the documents as non-searchable PDFs.xxxii In general, such problems can be avoided by producing files in native format, and some courts have expressly stated a preference for this form of production.[xxxiii]

How Do You Review?

ESI should not be reviewed as if rummaging through a box of paper, because it is fundamentally different from paper. For example, ESI can be indexed and sorted by dates, custodians, and control numbers (identifying numbers comparable to Bates numbers). Moreover, ESI can be searched and organized using advanced tools that facilitate review. Unlike paper, ESI is usually reviewed by "tagging" documents with specific issues or categories in order to sort documents by relevance to an issue in a case or responsiveness to a request for production. In creating tags, it is useful to consider the claims and defenses in a dispute, the key players, and the relevant timeframes.

In some instances, it may be appropriate to simply tag documents based on responsiveness or privilege. In other instances, tagging documents as "responsive," "relevant," or even "hot" may be too general to provide value. For example, when preparing for a deposition or court appearance, it may be more useful to have documents tagged with issues relevant to a dispute, deponent, or causes of action.

Privilege Review

If a party asserts a privilege as a basis to withhold any documents, FRCP Rule 26(b)(5) requires that party to produce a privilege log, which:

1. Expressly states the privilege for each such document.
2. Describes enough of the nature of the information not being disclosed to enable other parties to assess the privilege claim.

For efficiently drafting a privilege log, you and your team can review ESI and build a privilege log in a database. This may involve the following steps:

- Identify the possible privileges in the case
  - Examples include: Attorney-Client Communications, Attorney Work Product, Marital Communications, Clergy Privilege, etc.
- Create issue tags on the prospective privileges, including sub-issues.
- Prioritize privilege searches by term type.
- Search for names of individuals known to trigger privilege.
  - Examples include: Outside counsel, retained firms, retained vendors, etc.
- Search for explicit privilege markers.
- Search for legal keywords indicating likely privilege.
- Use privilege tagging to generate a privilege log (many review tools, such as EnCase eDiscovery, will generate the log automatically once privilege tagging is complete).

When conducting a privilege review, it is ordinarily necessary to select the relevant privilege tags and also include additional information explaining the privilege in order to complete the log. For example, an e-mail that is a communication from a client to the attorney seeking legal advice would be tagged attorney client privilege with an explanation identifying the sender and recipients as well as the basis for asserting the privilege.

With tools like e-mail threading, the reply e-mail can be automatically privilege coded as an e-mail from an attorney to the client providing legal advice. Again, additional information likely must be added to establish the basis for the privilege and complete the log.

Once privilege review is completed, many review tools will automatically generate a privilege log by exporting the relevant information to an Excel file for production.

Conclusion

Discovery no longer starts when a complaint is filed or a request is made. Discovery now begins with intelligent information policies and procedures. Implementing good processes for managing, preserving, and deleting data is crucial to meeting e-discovery obligations in a defensible and cost-effective manner. Accordingly, counsel must understand their obligations with respect to preservation; identification, collection, and processing; and efficient review of ESI.

FRCP's Rule 1 states that the rules "should be construed and administered to secure the just, speedy, and inexpensive determination of every action and proceeding be litigated." Part of meeting this obligation requires the intelligent practice of e-discovery. Regarding preservation, responsible attorneys should engage in litigation-hold and preservation activities in every case. Lawyers simply cannot forego preservation and the defensible methodology of the litigation hold. Doing so puts clients at risk of sanctions and extensive motion practice. With respect to collection and review, counsel can leverage technology to identify, collect, and process ESI pre- and post-collection. Technology can greatly assist a party with honing in on ESI that is relevant to a case, while at the same time controlling discovery costs. More importantly, these strategies help attorneys focus on the merits of the case and not large amounts of data.

The review and production of e-discovery is the blending of art and science. Attorneys must understand the spirit of the law as well as how to use technology to meet discovery obligations. For example, a discovery request that is overly broad may not only result in motion practice, but it may ensure the nightmare of actually placing years' worth of ESI, e-mail, text messages, and social-media transcripts into a very expensive review and production cycle. Similarly, failure to discuss form of production at a meet and confer can result in a production that renders advanced analytics tools powerless to reduce review time and costs.

The key to success in e-discovery review is simple: implement repeatable, auditable processes early on. Don't rely on ad-hoc responses. Being proactive can reduce your e-discovery costs and risks.

To learn more about how EnCase eDiscovery can help turn review into a fast, accurate, and repeatable business process, please visit www.encase.com/ediscovery.

Citations

[i] Apple, Inc. v. Samsung Elecs. Co. Ltd., No. C 11-1846 LHK (PSG) (N.D. Cal. July 25, 2012) (sanctioning defendant for use of self-collection).

[ii] National Day Laborer Organizing Network et al. v. United States Immigration and Customs Enforcement Agency, et al., 10-CV-3488 (SAS) (S.D.N.Y. July 13, 2012) (ordering new searches due to failure to follow best practices).

[iii] In re Delta/Airtran Baggage Fee Antitrust Litig., 2012 U.S. Dist. LEXIS 13462 (N.D. Ga. Feb. 3, 2012) (sanctioning defendant where documents not produced were later produced in separate DoJ investigation, showing failure to search and review all evidence sources).

[iv] Distefano v. Law Offices of Barbara H. Katsos, PC., No. CV 11-2893 (JS) (AKT) (E.D.N.Y. March 29, 2013) (attorney's duty to preserve triggered upon receipt of letter from client terminating attorney client relationship and indicating potential litigation).

[v] Fed. R. Civ. P. 26(a)(1), 37(b)(2).

[vi] See e.g., Hart v. Dillon Cos., Inc., 2013 WL 3442555 (D. Colo. July 9, 2013); In re John W. Danforth Group, Inc., 2013 U.S. Dist. LEXIS 92476 (W.D.N.Y. June 30, 2013); Zubulake v. UBS Warburg LLC, 217 F.R.D. 309 (S.D.N.Y. May 23, 2003); Rowe Entertainment, Inc. v. The William Morris Agency, Inc., 205 F.R.D. 421 (S.D.N.Y. 2002); Mosaid Techs. Inc. v. Samsung Elecs. Co., 348 F. Supp 2d 332 (D.N.J. 2004).

[vii] Willoughby Jr., et al., Sanctions For E-Discovery Violations: By The Numbers, 60 DUKE L. J. 789, 803 (2010) (finding that ninety of two-hundred and thirty e-discovery sanctions cases involved a failure to preserve).

[viii] Altercare v. Clark, 2013 Ohio 2785 (9th Dist. Ohio June 28, 2013).

[ix] Sekisui America Corp. v. Hart, No. 12 Civ. 3479 (SAS) (FM), (S.D.N.Y. Aug. 15, 2013), reversing Sekisui America Corp. v. Hart, No. 12 Civ. 3479, (SAS) (FM) (S.D.N.Y. June 10, 2013).

[x] Apple, Inc. v. Samsung Electronics Co., Ltd., F. Supp. 2d. (N.D. Cal. 2012) (sanctions issued for failure to issue timely litigation hold notice).

[xi] Chin v. Port Authority of New York & New Jersey, 685 F.3d 135 (2d Cir. 2012), reversing Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities, 685 F. Supp. 2d 456 (S.D.N.Y. 2010) (sanctioning thirteen plaintiffs for failure to issue a written hold and finding that such failure constitutes negligence per se).

[xii] Voom HD Holdings LLC v. Echostar Satellite LLC, 2010 N.Y. Misc. LEXIS 6306 (N.Y. Sup. Ct. Nov. 3, 2010) (ordering sanctions for plaintiff's failure to issue a pre-complaint litigation hold notice following reasonable anticipation of litigation).

[xiii] In re Prudential Ins. Co. of Am. Sales Practices Litig., 169 F.R.D. 598 (D.N.J. 1997).

[xiv] Id. at 615.

[xv] Id.

[xvi] United States v. Philip Morris USA, Inc., 327 F. Supp. 2d 21, 26 (D.D.C. 2004).

[xvii] Counsel often assert a privilege over documents due to "anticipation of litigation." It should go without mention that the assertion of such a privilege may carry risk if counsel cannot demonstrate preservation during the period when a client allegedly "anticipated" litigation. A process that includes early issuance of a litigation hold and a contemporaneous audit trail as to preservation decisions will help demonstrate preservation and reduce risk in asserting this privilege.

[xviii] Allstate Ins. Co. v. Hamilton Beach/Proctor Silex, Inc., 473 F.3d 450, 457 (2nd Cir. 2007).

[xix] Residential Funding Corp. v. DeGeorge Financial Corp., 306 F.3d 99, 107 (2d Cir. 2002) (establishing factors for spoliation sanctions in Second Circuit); see also, In re Pfizer Inc., 288 F.R.D. 297, 316 (S.D.N.Y. 2013) ("a showing – inferential or otherwise – that the movant has suffered prejudice" required to award sanctions).

[xx] EEOC v. Dillon Companies, 839 F.Supp.2d 1141 (D. Colo. 2011).

[xxi] FRCP Rule 34(a).

[xxii] FRCP Rule 26(f).

[xxiii] FRCP Rule 16(b).

[xxiv] FRCP Rule 26(a)(2).

[xxv] Logan v. Gary Cmty. Sch. Corp., 2008 U.S. Dist. LEXIS 95761 (N.D. Ind. Nov. 21, 2008), citing Fed. R. Civ. P. 26(a)(1)(E).

[xxvi] Littlefield v. Dealer Warranty Servs., LLC, 2010 U.S. Dist. LEXIS 101102, at *9-10, (E.D. Mo. Sept. 27, 2010) citing Fed. R. Civ. P. 37(c)(1).

[xxvii] Eichnholtz, Seth, Pricing Processing in E-Discovery: Keep the Invoice from Being a Surprise, 25 A.B.A. IN-HOUSE LITIGATOR 1, 18–21 (2010).

[xxviii] Da Silva Moore v. Publicis Groupe, et al., 2012 U.S. Dist. LEXIS 23350 (SDNY, Feb. 24, 2012).

[xxix] Readlyn Tel. Co. v. Qwest Communs. Corp., 2013 U.S. Dist. LEXIS 45168, 2-3 (N.D. Iowa Mar. 29, 2013).

[xxx] See e.g., Kwan Software Eng'g, Inc. v. Foray Techs., LLC, 2013 U.S. Dist. LEXIS 144882, *2-5 (N.D. Cal. Oct. 1, 2013) (ordering Defendant who produced TIFF files without metadata to re-produce files in native format).

[xxxi] In re Coventry Healthcare, Inc., 2013 U.S. Dist. LEXIS 39050, at *14-15, n. 6 (D. Md. Mar. 21, 2013) (holding that entry of a protective order would eliminate Defendant's burden of review: "the more practical approach is to avoid the necessity of an expensive and time-consuming privilege review by entry of a court order with a clawback provision that protects against a claim of waiver by production of a privileged document"), citing Hopson v. Mayor & City Council of Baltimore, 232 F.R.D. 228 (D. Md. 2005).

[xxxii] Independent Marketing Group, Inc. v. Keen, 2012 U.S. Dist. LEXIS 7702 (M.D. Fla. Jan. 24, 2012).

[xxxiii] See e.g., In re Porsche Cars N. Am., Inc. Plastic Coolant Tubes Prods. Liab. Litig., 279 F.R.D. 447, 449 (S.D. Ohio 2012) (stating that "[t]his Court has expressed a preference for the production of electronically stored information in its native format.").

About Guidance Software

At Guidance, we exist to turn chaos and the unknown into order and the known—so that companies and their customers can go about their daily lives as usual without worry or disruption, knowing their most valuable information is safe and secure. Makers of EnCase®, the gold standard in digital investigations and endpoint data security, Guidance provides a mission-critical foundation of applications that have been deployed on an estimated 25 million endpoints and work in concert with other leading enterprise technologies from companies such as Cisco, Intel, Box, Dropbox, Blue Coat Systems, and LogRhythm. Our field-tested and court-proven solutions are used with confidence by more than 70 of the Fortune 100 and hundreds of agencies worldwide. Get to know us at guidancesoftware.com.