LET'S GET DIGITAL! ESI IN TRUST AND ESTATE LITIGATION, PART 1

By Scott A. Fraser, Esq. and Matthew R. Owens, Esq.***

MCLE Article

I. INTRODUCTION

The time has come to abandon the blurry, barely legible PDF copies of emails and other documents in discovery. Most documents used in trust and estate litigation matters are easily accessible in their native formats, which makes it much more efficient to produce and search through them. No longer should trust and estate practitioners print documents to respond to discovery requests, nor should they have to review paper copies when they receive discovery responses. This is especially true at a time when practitioners find themselves working remotely more than ever before. Indeed, it is time to get digital.

This article is Part I of a two-part series focusing on e-discovery rules relevant to trust and estate litigators. The goal is to arm the reader with the tools needed to conduct and respond to e-discovery properly and in an efficient and effective way. The article addresses common sources of electronically stored information ("ESI") targeted to trust and estate litigation matters, as well as the procedures used to obtain ESI. The article also discusses the importance of advising clients on preserving ESI in order to avoid evidence spoliation and to keep counsel in compliance with ethical rules surrounding e-discovery.

II. INITIAL EVALUATION OF E-DISCOVERY ISSUES

It is rare that a trust and estate litigation case does not involve some form of discovery of ESI. At the beginning of each case, counsel must first determine which e-discovery issues exist, the extent of such issues and anticipated costs, and whether it is necessary to retain an expert to assist.

A. Every Attorney Has a Duty of Competence When Handling E-Discovery Issues

The California State Bar has specifically stated that maintaining learning and skill consistent with an attorney's duty of competence includes keeping abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology and e-discovery.[1]

The scope of an attorney's duty of competence depends upon the nature and complexity of the e-discovery at issue in each case. The California State Bar has provided the following framework: (i) attorneys must assess at the outset of each case what e-discovery issues might arise during the litigation, including the likelihood that e-discovery will or should be sought by either side; (ii) if e-discovery will probably be sought, attorneys must assess their own e-discovery skills and resources that will be needed to meet the demands of the potential e-discovery issues; and (iii) if attorneys lack such skills and/or resources, they must try to acquire sufficient learning and skill, or associate or consult with someone with expertise to assist.[2]

Furthermore, in assessing the scope of e-discovery in the case and their competence to perform the necessary tasks, attorneys handling e-discovery should be able to perform (either by themselves or in association with competent co-counsel or expert consultants) the following: (i) initially assess e-discovery needs and issues, if any; (ii) implement/cause to implement appropriate ESI preservation procedures, (iii) analyze and understand a client's ESI systems and storage; (iv) advise the client on available options for collection and preservation of ESI; (v) identify custodians of potentially relevant ESI; (vi) engage in competent and meaningful meet-and-confer with opposing counsel concerning an e-discovery plan; (vii) perform data searches; (viii) collect responsive ESI in a manner that preserves the integrity of that ESI; and (ix) produce responsive non-privileged ESI in a recognized and appropriate manner.[3]

The e-discovery issues will be different for each case but, in most trust and estate matters, the issues that arise the most often are searches and retrieval of information from personal computers and smartphones and searches and culling of information from emails. Counsel in trust and estate litigation matters should expect that they will need working knowledge of the e-discovery issues concerning these common sources of ESI.

B. Use of Co-Counsel, Experts, and Third-Party Providers

The only way attorneys who are not competent in the law and practice of e-discovery can fulfill their ethical duty is (i) by taking the time and considerable effort needed to become competent, or (ii) by bringing in competent legal counsel to assist.[4] Attorneys may also hire experts, ESI vendors, and

other third-party providers to assist with the matter, and it is often prudent to do so.

If the attorney lacks sufficient skills or resources and associates or consults with someone with expertise, the attorney must still supervise the work of the co-counsel or expert.[5] The duty to supervise and the ultimate responsibility for competence rests with the supervising attorney and is a non-delegable duty.[6] Therefore, in order to competently supervise the co-counsel or expert, the attorney must remain regularly engaged in the e-discovery work and must also educate everyone involved in the e-discovery workup about the legal issues in the case and the factual matters impacting discovery, including witnesses and key evidentiary issues, the obligations around discovery imposed by the law or by the court, and any risks associated with the e-discovery tasks at hand.[7]

C. Initial Evaluation of E-Discovery Issues

Counsel should discuss with their clients early in the representation the topic of evidence they may have in their possession, including ESI. It is critical to identify all sources of ESI through discussions with clients so that evidence may be preserved and requests appropriately targeted. If a lawsuit has already been filed, then there is no question the client must preserve all ESI. Even before a lawsuit is filed, the client may have an obligation to preserve ESI if litigation is reasonably anticipated.

The following is a non-exhaustive list of sources of ESI to consider when evaluating the potential e-discovery issues in a case:

- What electronic devices were used by the decedent—computer (desktop or laptop), smartphone, personal digital assistant (PDA), tablet?
- What operating system does each electronic device use—Mac, Windows, Android?
- Are any of these devices password protected and, if so, who knows the password?
- What applications did decedent use? Examples include:
  - Accounting—QuickBooks
  - Calendaring—iCalendar, Outlook, Google
  - Eating/diet—MyFitnessPal
  - Finance—Venmo, Paypal, cryptocurrencies
  - Medication manager—Medisafe (medication manager)
  - Messaging—text, iMessage, WhatsApp
  - Social media—Facebook, Instagram, Twitter
  - Spreadsheet—Microsoft Excel, Google sheets
  - Web browser—Chrome, Firefox, Safari, Internet Explorer, Bing
  - Word-processing—Microsoft Word, Notes, Google Docs
- What email provider did decedent use—Gmail, Yahoo, Outlook?
- Did the decedent use any wearable electronic devices—Apple Watch, Fitbit, Garmin?
- Did the decedent use any internet of things (IOT) home devices or home security electronic devices—Nest or Ring security camera?
- What electronic storage devices were used by decedent? Examples include:
  - Hard drive, flash drives, CD-ROM, DVD, external hard drives
  - Cloud storage (Box, Dropbox, Google Drive, iCloud)

Other sources of ESI might be important depending on the type of proceeding. For a long-term trust administration, counsel may want to determine how the trust records are stored (e.g., paper, electronic storage device, or in the cloud). In an action involving a contested accounting, counsel may also wish to determine whether the fiduciary used any accounting software, such as QuickBooks. The scope of the questions on which the attorney will need to focus will depend on the facts and legal issues in dispute in the litigation.

III. PLANNING FOR E-DISCOVERY

Once counsel has initially ascertained the scope of the ESI issues in the case, counsel must take appropriate steps to preserve that data so that it can be appropriately and accurately analyzed in the discovery process.

A. Preservation of E-Discovery

1. When the Duty to Preserve is Triggered

Steps must be taken to preserve ESI as soon as litigation is filed or reasonably anticipated. "[A] litigant is under a duty to preserve evidence which it knows or reasonably should know is relevant to the action."[8] The duty attaches "from the moment that litigation is reasonably anticipated."[9] Destruction of evidence "in anticipation of a discovery request" is a misuse of the discovery process, potentially warranting terminating sanctions.[10] "Spoliation [of evidence] is the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence, in pending or future litigation."[11] A litigant has a duty to preserve evidence, even if the evidence belongs to them.[12] If a litigant destroys evidence, even inadvertently, terminating sanctions may be imposed in the form of a court order striking the defendant's answer and entering a default judgment.[13] In cases of intentional spoliation, terminating sanctions are appropriate in the first instance even without any violation of a prior court order.[14]

As soon as the duty to preserve is triggered, counsel should provide clear instructions to clients on identifying ESI and the method for preserving it. This usually means sending an evidence-preservation letter (also known as a litigation hold letter) to your own client. It is often best to notify clients in advance that they will be receiving such a letter so it does not come as a surprise. The letter can be perceived as harsh when sent to clients, so discussing it in advance provides an opportunity to discuss the importance of evidence preservation so the letter is better received. Below is sample language for an evidence-preservation letter in a case where a litigant may seek the decedent's devices and ESI stored on them.

> You must preserve all documents, evidence, writings, written and recorded information, and electronically stored information (ESI), including metadata, that may relate to the trust, the estate, the decedent, or to any of the related allegations, claims, causes of action, potential defenses, or counterclaims (collectively, the "Claims"). This includes, without limitation, all electronic data such as emails, text messages, images, sound, or video recordings, WhatsApp or similar communications, social media posts, word processing files, spreadsheets, PDFs, QuickBooks, calendars, PowerPoints, video surveillance footage, and the like.
>
> All such materials are to be carefully preserved in their original format. The destruction, alteration, or deletion of documents or electronic data, even if unintentional or even if done in the normal course of business, is prohibited and could have significant adverse consequences. This means that any such documents created or maintained by you, your employees, or your agents at any time must be preserved. Accordingly, all records management or destruction policies impacting records related to the subject matter of the Claims should be suspended.
>
> This preservation directive extends not only to electronic data on your computers, but also extends to electronic data contained on devices such as smartphones, tablets, PDAs, Blackberry devices, disks, CDs, DVDs, flash drives, thumb drives, Jaz drives, external hard drives, and all other forms of electronic data storage devices, regardless of whether such devices are still in use or have been or will be replaced by newer devices.
>
> The documents, information, and communications to be preserved include the following categories, which are to be construed as broadly as possible, and in every instance of doubt or ambiguity, construed in favor of preservation:
>
> a. all ESI concerning the trust;
> b. all ESI concerning the estate;
> c. all ESI concerning the decedent;
> d. all ESI concerning the decedent's assets; and
> e. all ESI concerning, in any other way, the Claims.

When your client intends to seek ESI, it is important to provide notice of that intent as early as possible. Parties may have emails set to automatically delete or may simply decide to delete voicemails, photos, or other ESI unless they are put on notice not to do so. Where possible, it is often prudent to send an evidence-preservation letter to opposing counsel even before a lawsuit is filed. That will eliminate or at least impair the other side's ability to claim they did not reasonably anticipate litigation at the moment in time when they deleted the ESI being targeted.

2. Additional Preservation Duties for Fiduciaries

In trust and estate litigation, there is often a litigant with additional duties separate and apart from discovery obligations: the fiduciary. The duty to preserve ESI is arguably imposed on fiduciaries even in the absence of litigation, because they must

preserve the trust assets[15] or the estate assets[16] as the case may be. Further, a party may be held liable for a loss resulting from the breach of an obligation to preserve evidence.[17] As a result, counsel should inform their fiduciary clients not to throw out the decedent's computers, smartphones, or other devices until it is clear there is no need for the devices either for the administration or for the defense or prosecution of claims concerning the decedent's trust or estate. Sometimes, by the time a fiduciary engages counsel, it is already too late. Perhaps the decedent's spouse or other family member threw out or donated the iPhone and laptop when clearing out other personal property items. Such premature disposal of electronic devices could cause serious problems if litigation ensues and there are claims of intentional spoliation of evidence, especially when the alleged spoliation was done by a fiduciary charged with protecting the decedent's assets.

Fiduciaries may also have access to the decedent's digital assets under the Revised Fiduciary Digital Assets Act, which was enacted in 2016.[18] A digital asset is "an electronic record in which an individual has a right or interest."[19] This broad definition covers a wide range of assets such as cryptocurrencies, social media accounts, and digital music catalogues. Although fiduciaries may have access to such digital assets under the Revised Fiduciary Digital Assets Act, such rights are separate from discovery rights under the Code of Civil Procedure and, therefore, are outside the scope of this article. However, it is noted here because practitioners may grapple with the interplay between discovery rights and a fiduciary's right to digital assets or when considering a fiduciary's duty to collect assets from custodians within their control when responding to an adversary's discovery requests. In many cases, the custodian of a decedent's digital assets must comply with a personal representative's request for disclosure of digital assets where disclosure is reasonably necessary for the estate administration.[20] Since discovery requests to the fiduciary would capture the digital assets in their possession, custody, or control, the fiduciary would arguably be required to produce information concerning digital assets that the fiduciary could obtain upon demand from the various custodians of such digital assets.[21] After all, a litigant "cannot plead ignorance to information which can be obtained from sources under his control."[22]

3. Meet and Confer Process

Just like any other discovery, counsel are required to meet and confer with respect to e-discovery.[23] There is even a separate rule outlining the e-discovery issues counsel must cover, which includes preservation of electronically stored information, the form in which it will be produced, and allocation of costs associated with production.[24]

Before meeting and conferring to request e-discovery, counsel should consider whether the case justifies the extra cost of e-discovery from a cost-benefit standpoint. When requesting e-discovery from the other side, counsel must recognize there is a high likelihood that request will become reciprocal. Clients should be consulted on the cost of e-discovery before it is proposed so they can decide whether they wish to seek e-discovery and incur the additional cost it carries.

The meet and confer process on e-discovery should include identification of sources from which the parties will search for ESI. All device types and account types should be identified so everyone knows the target sources and counsel can appropriately tailor their e-discovery requests. Are the parties going to search for data and metadata on all computers, smartphones, tablets, security cameras, wearables, internet-of-things (IOT) home appliances, and the like? Or are the parties really just seeking emails in native format? Having that discussion with opposing counsel early in the case will help set expectations in terms of scope of e-discovery and expected cost.

The next step is to discuss key search terms for emails and other communications such as text messages and social media posts. Terms such as "trust" and "will" are obvious targets, but if those terms are not made part of a Boolean search, then the responses will undoubtedly include mountains of emails the requesting party did not actually want. Counsel may also wish to limit email searches to a specified subset of senders and recipients and limit the date range. Once counsel agree on the key terms, senders/recipients, and date range, those guidelines can be turned over to an ESI vendor (or an ESI expert at counsel's law firm) to run the searches on an e-discovery platform.

4. Preservation of Common Sources of ESI

In trust and estate matters, there are some common sources of ESI that tend to arise when litigants seek e-discovery. A few of the most common are computers, smartphones, and email accounts. These sources become important in a wide variety of case types and impact parties and nonparties alike. For example, in a breach of fiduciary duty case against a trustee, there may be records on the trustee's computer that are more than seven years old that parties could not otherwise obtain via subpoena and must be able to get from the trustee's computer. In a dispute over a bank account, there may be

voicemails or text messages on the decedent's smartphone evidencing the decedent's intent with respect to disposition of the bank account. In a trust contest, the estate planner who is subpoenaed to produce the estate planning file in native format may need to take steps to preserve the ESI in the estate planner's email account. Discussed below are typical methods of preserving these common sources of ESI for use in e-discovery.

a. Avoid Destruction of Computers

Like any physical evidence, the computer's chain of custody should be tightly controlled and tracked. If litigation has commenced or is reasonably anticipated, the computer should be imaged by a third party vendor so it is preserved in its original state before anyone starts searching it. Although there is a cost associated with that step, it is often well worth it to avoid claims of spoliation of evidence or improper tampering.

In order to have it imaged, the party in possession of the computer should hand it over to an ESI vendor without accessing it or conducting any searches. Once the ESI vendor images the computer, it can be held in a locker with the ESI vendor pending expert witness examination or trial. The imaged data can be uploaded to an e-discovery platform so that parties, counsel, and experts can search the data. Once it has been imaged, the computer can even be made available to the parties or their experts for inspection without fear of tampering, because the image mirrors the data that existed on the computer before it was made available to the parties for inspection.

Accessing a decedent's computer can be a challenge. If no one has the password to unlock the computer, then the hard drive can sometimes still be pulled from the computer and imaged. If, on the other hand, the computer is a locked Mac, it may not be accessible unless someone has the decedent's iCloud login credentials and can obtain the password that way. Counsel should, of course, be careful not to violate the decedent's privacy rights or the terms of service for any particular account or device when exploring such options.

There is often a temptation to throw out the decedent's personal property items, including computers, smartphones, tablets, and the like. Family members sometimes assume the decedent would not want their private information searched following death. While this sentiment is understandable, such devices contain evidence that is often highly probative in trust and estate disputes, so they should be preserved until it is clear they will not be needed in the litigation.

One of the co-authors has litigated a case where a fiduciary burned the decedent's laptop in a bonfire after the decedent's death out of concern for the decedent's privacy. If such conduct occurs after litigation is initiated or reasonably anticipated, it can have catastrophic consequences, including issue, evidence, or terminating sanctions. Short of sanctions, such spoliation of evidence could also result in a negative inference at trial.[25]

b. Avoid Destruction of Smartphones

Smartphones may also contain important ESI such as text messages, voicemails, videos, and photos. Like a computer, a smartphone can be imaged for preservation and search purposes. Although many iPhones are locked and often no one has the passcode to unlock a decedent's iPhone, much of the content stored on an iPhone is backed up to the iCloud, so if the iCloud account can be accessed then much of the iPhone's content can be obtained without ever unlocking the physical device.

c. Avoid Deletion of Emails

Email accounts are fertile ground for communications concerning intent with respect to estate planning, the nature of the decedent's relationship with competing heirs, and the decedent's assets. It also may provide useful information on the existence and location of assets. If the computer is accessible, then email accounts may be accessed directly and searched on the computer itself or uploaded to a search platform. But if the computer is locked and no one has the password, then a party with authority to log into the decedent's email account could still do so from a separate computer or device if the party has the decedent's login credentials. Once the email account has been accessed, the party can search for relevant emails or provide access to an ESI vendor to load the emails onto a search platform.

It is important to immediately suspend any auto-delete feature that may be in place for relevant email accounts. Many email accounts automatically delete emails after specified periods of time, which can be as short as a few months in some cases. After a party is in litigation or should reasonably anticipate litigation, auto-deletion of emails can potentially be considered spoliation of evidence and, therefore, must be avoided.[26] Further, there may be useful evidence in the emails that the email account's owner would not want to lose to an auto-delete feature.

B. Use of Traditional Discovery Tools to Identify ESI

All other discovery tools remain available to help counsel identify sources of ESI that can then be targeted in a subsequent round of discovery. For example, in a set of written interrogatories, a party may request that the other side identify all of the decedent's electronic devices, email addresses, and social media accounts. When those items are identified, the party may serve a more narrowly tailored set of discovery seeking specified ESI from those electronic devices, email addresses, and social media accounts. In deposition, counsel should ask the deponent what efforts were undertaken to locate ESI, including what search terms were used, what devices were searched, and where the device is now located. In deposition of a fiduciary, counsel should ask the fiduciary about recordkeeping methods and ascertain what kinds of ESI are created and how the ESI is stored.

IV. REQUESTING PRODUCTION OF ESI

A. Right to Request Production of ESI

Any party to litigation in California is expressly authorized to obtain discovery by inspecting, copying, testing, or sampling ESI in the possession, custody, or control of any other party to the action.[27] ESI is defined as any information that is stored in an electronic medium.[28] "Electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.[29]

Using the common sources of ESI that the authors have identified—computers, smartphones, and email accounts—there is virtually no limit to the amount of ESI that could potentially be relevant to a trust and estate litigation case. In a matter involving claims of incapacity and undue influence, in which the decedent's health, relationships with others, finances, communications, and written expressions of intent are all relevant, these various sources of ESI are critical evidence that may not be available from any other source. In addition, as people perform more basic functions online or through their smartphone or internet-of-things (IOT) devices, the different types of information created and, therefore, potentially relevant is immense and constantly expanding.

In addition to the ESI that a party may request, there is also ancillary data and information associated with that ESI—metadata.[30] This includes a file's name, a location (e.g., directory structure or pathname), file format or file type, file size, file dates (e.g., creation date, date of last data modification, date of last data access, and date of last metadata modification), and file permissions (e.g., who can read the data, who can write to it, and who can run it), as well as hidden text, formatting codes, formulae, and other information associated with the file.[31] Metadata also includes tracked changes and editorial comments.[32]

In some instances, metadata may itself be important evidence. For example, metadata may be relevant if the authenticity of a document is in question or if establishing "who received what information and when" is important to the claims or defenses of a party.[33] In other instances, metadata may be useful in managing and using ESI that has been produced.[34] The metadata may allow for efficient sorting of files by virtue of the dates or file type.[35] Other types of metadata can be utilized by third party provider technology platforms to search, cull, and analyze the data in other ways.[36] In addition, certain types of application metadata may also be crucial for the actual usability of the ESI.[37]

B. Right to Request the Form or Forms of ESI Production

In addition to requesting the production of ESI, counsel may also specify the form or forms in which each type of ESI is to be produced.[38] In determining what ESI form or format to request, the primary goal should be to receive the information in the format that best provides counsel with the ability to cull, analyze, search, and display the information requested.[39] The specific circumstances of each case and the type of ESI requested will guide this determination.

1. Different Forms of Production of Common ESI

The common forms of production of ESI are native format, TIFF, and PDF. Each of these forms has different benefits and drawbacks. Native format refers to the file type and structure of the electronic document defined by the original creating application.[40] Documents produced in native format include all metadata associated with the ESI.[41] For Microsoft Word documents, this would be .doc or .docx files; for Excel spreadsheets, this is .xls or .xlsx.

TIFF (Tagged Image File Format) is a graphic file format in which the ESI is produced in a static image. Essentially, a TIFF (or PDF) is a screenshot of ESI that cannot be edited and in which the metadata is not visible.[42] In the conversion to static image format, some of the metadata can be processed, preserved, and electronically associated with the static image in an associated "load file."[43] TIFF is also compatible with many document review software programs and platforms.

Production in native format gives the receiving party access to the same information and functionality available to the producing party and requires minimal processing time before production.[44] However, production in native form is difficult to redact or "bates" number and in some instances the receiving party may not have the software necessary to open the document.[45] Requests for ESI in native format also present the highest likelihood that irrelevant, privileged, or other objectionable information will be included in the request. Types of documents that most commonly benefit from production in native or near-native format are spreadsheet files, presentation files, or documents with tracked changes.[46] For spreadsheets, metadata is often necessary for display of the formulas and other information, as well as information regarding the changes to spreadsheets, dates of the changes, and identification of the individuals who made the changes.[47]

By comparison, production in a static image format, such as TIFF or PDF, can be bates-numbered and redacted, but there is a loss of metadata.[48] In addition and not insignificantly, production in TIFF or PDF also entails significant processing time and cost. The most common way to produce ESI has been to create a static electronic image in TIFF or PDF, to place the extracted text from the document into a text file, and to place the selected metadata and other non-apparent data into one or more separate load files.[49] The type of ESI and metadata to be placed into the load file should be requested up front by the requesting party.

2. Requesting Form of ESI in Trust and Estate Litigation

The most common document types that arise in trust and estate litigation—PDF files, Microsoft Word documents, and emails—are document types that lend themselves to production in PDF or TIFF. The documents can then be easily bates numbered and redacted and produced in a searchable text format. This will allow counsel quickly to sort the different categories of documents and to then search each document category to identify those documents of evidentiary value. If the requesting party intends to use document review software then that party should consider requesting the information in TIFF format. If TIFF format is used, consider requesting basic metadata fields in associated load files such as: file name, date created, last date modified, created by, edited by, custodian, starting production number, ending production number, document type or file extension, original file path, and, for emails in particular, details such as from, to, cc, bcc, and subject line. Consideration must be given, of course, to the costs associated with requesting production in this manner.

In trust and estate litigation matters involving the authenticity of documents and issues regarding when a document was authored, when changes were made, and by whom the changes were made—such as disputes over the decedent's intent or undue influence claims—it may be appropriate to request production of those documents in native format with metadata. This is especially important if changes to estate planning documents were made over time and prior versions can be tracked through inspection of native format files. In addition, in disputed trust administration cases involving accounting and complex spreadsheets, counsel should consider requesting the spreadsheets in native format. Receipt of the spreadsheets in this manner will allow the requesting party to more easily analyze and use the data, as well as ascertain the formulas used to create the spreadsheet.

C. Requesting Inspection, Copying, and Sampling of Electronic Devices

In addition to requesting production of documents in a particular electronic format, a party may request to inspect, test, or sample ESI in the possession, custody, or control of the responding party.[50] For example, counsel may request to inspect a decedent's computer, smartphone, tablet, or external hard drive.

However, while this procedural mechanism is available under the Code of Civil Procedure, it will not always be available in practice. In the majority of cases, the claims and defenses in litigation relate to the informational content of the data stored on the computer system, not the operation of the computer system itself.[51] Therefore, if the responding party produces all of the relevant informational content of the data stored on the computer system, there is no reason why the requesting party should be allowed to inspect or copy the responding party's computer system.[52] As a result, inspection and copying is usually only available as a remedial measure where the responding party has failed to meet their discovery obligations.

Apart from copying and inspecting ESI, another option for counsel is to test or sample ESI.[53] For example, in one case, the court approved a sampling protocol for the purpose of refining a proposed computer-assisted search by taking a random sample, and running and refining the search in order to eliminate irrelevant documents from the sample and focus the parties' search on relevant documents only.[54] In other instances, this mechanism could be used to determine if relevant information is contained within a specific electronic device before requesting to copy or inspect such electronic device.

Counsel seeking to test or sample an electronic device should be prepared to conceive of and implement a protocol to protect against the disclosure of irrelevant, privileged, private, or otherwise confidential information.[55] For example, in the previously mentioned random sampling case, the court required that (i) responding party be able to review the sample and remove any irrelevant documents from the sample, (ii) only one attorney from each side would have access to the documents, and (iii) the parties agree that irrelevant documents would not be used for any other purpose and that all irrelevant documents and notes regarding the sample be destroyed 14 days after resolution of the sampling process.[56]

D. Requirements to Request ESI

1. Describing ESI with Sufficient Particularity

Requests for ESI are subject to the same particularity requirement and privacy/privilege concerns as ordinary discovery requests.[57] In fact, concerns regarding the invasion of privacy and privilege are heightened in e-discovery because of the pervasive and expansive nature of how electronic information is stored.[58]

Accordingly, each demand must designate the ESI to be inspected, copied, tested, or sampled either by specifically describing each individual item or by reasonably particularizing each category of item.[59] Each demand must also state any inspection, copying, testing, sampling, or related activity that is being demanded, as well as the manner in which that activity will be performed, and whether that activity will permanently alter or destroy the item involved.[60] Similar rules apply to requests for inspection or copying of documents via a subpoena duces tecum.[61]

Care should be taken by the requesting party to identify the correct form in which ESI should be produced. To the extent most practical, counsel should identify each item or category of ESI sought and the location of that information.[62] Counsel should target specific ESI that is relevant to the subject matter of the litigation and meets the proportionality requirement of the production rules.[63] Specific drafting in this regard will require that counsel identify the different types of categories of information and the different forms in which those categories are stored.[64] As much detail as possible should be provided, including whether metadata is sought, whether data stored in the cloud is sought,[65] whether email attachments are sought, and whether emails should be produced in a format that will reveal BCCs.[66] Counsel should clarify these details on the front end through meet and confer efforts instead of litigating them on the back end via motion to compel.

Careful drafting of e-discovery requests serves many functions. If a demand for production does not specify a form or forms for producing a type of ESI, the responding party shall produce the information in the form or forms in which it is ordinarily maintained or in a form that is reasonably usable.[67] In comparison, where the requesting party has specified the format of production, a responding party may not object to production on the ground that such information could be produced in paper form or other format.[68] Even where a particularized need is later shown for production of e-discovery in a specific format, courts have shown reluctance to grant such a request where the form of production was not specified in the initial request.[69] In addition, careful drafting of e-discovery requests will reduce the likelihood of objections from the responding party, the need for judicial intervention, and possibly issuance of protective orders by courts.[70] Whether the requests sufficiently describe each item with reasonable particularity will be determined in each instance,[71] but taking the time to carefully draft questions can avoid later disputes.[72] You will know how to specifically describe the ESI that you are requesting by following the steps outlined in the sections above.

2. Requests for Metadata

Requests for metadata should be tailored to appropriate circumstances. It would be unnecessary for counsel to request that ESI be produced in native format (with all metadata) when the evidence needed to prove the party's claims is found on the face of the documents and the information contained in the text and load files will allow the requesting party to organize and search the documents.[73] In addition, the requesting party who takes custody of documents in native format must take reasonable steps to secure the information and its authenticity.[74] Therefore, counsel should avoid requesting production of ESI in native format unless there is a demonstrable need for receiving the ESI in that format and counsel has the necessary technology and resources available to manage and protect the ESI.[75]

As a result of these concerns, federal courts (where case law concerning e-discovery is more developed than state courts) generally have two requirements. First, a party must show a "particularized need" for the metadata that exceeds functional utility.[76]A particularized need has been shown where many of the paper documents that were produced were missing source, date, and other key background information and where the metadata was relevant to authenticating documents whose creators or authors were unknown.[77] A particularized need was found where metadata would allow the plaintiff to confirm or contradict the timing of when the

documents were authored, and the timing was a critical issue in the plaintiff's case.[78]

Second, the requesting party must ask for the production of metadata with sufficient specificity, preferably in the initial request.[79] Cases have repeatedly stated that "if a party wants metadata, it should ask for it up front."[80] Courts are particularly sensitive to producing metadata where the requesting party has already received documents from the responding party in a different form (i.e., paper or PDF).[81] In those cases, some courts have held that if metadata is not sought in the initial document request, and particularly if the producing party has already produced the documents in another form, courts tend to deny later requests.[82] In other cases, however, courts have held that under the context of the request that the responding party should have expected the need to produce documents with metadata intact.[83]

E. Conducting Searches for ESI

1. Keyword Filtering

Appropriate keyword searches make the e-discovery process much more efficient so the results yielded from the search will be more narrowly tailored to the content and evidence that is actually relevant to the case. By casting too wide a net in the keyword search process, counsel will end up with voluminous, irrelevant emails, text messages, and the like that could have been skipped altogether with properly narrowed keyword searches.

Keyword filtering is a common method of tailoring ESI searches. When reviewing thousands of documents for responsive ESI, the use of keyword filtering as opposed to manual review of each document is appropriate under certain circumstances.[84] The keywords may be linked to subject matter, names of parties, or other words that will yield responsive documents. By using keyword filtering, the pool of documents that counsel must manually review can be reduced substantially. Counsel must carefully track the keyword search conducted so that if questioned on the methodology counsel can submit a declaration demonstrating exactly which search terms or Boolean search sequences were used.

If there is evidence of an improper or inadequate search, courts may order the party who failed to conduct a thorough search to retain an ESI vendor to conduct the search and submit a declaration demonstrating the terms and process used.[85] To avoid such claims, it is generally preferable to meet and confer with opposing counsel before conducting the search to ensure there is agreement on the search terms to be used. Given the cost associated with running these types of searches, every effort should be made to eliminate claims of an inadequate search because the cost will be doubled if a party is ordered to run the search a second time.

If your client is seeking the ESI, you must ensure you capture all the relevant search terms when meeting and conferring with opposing counsel before the search is conducted. If you determine later that there were additional terms you failed to include for the initial search, you may be unable to compel the opposing party to run a second search. That is precisely what happened in *In Re National Association of Music Merchants, Musical Instruments and Equipment Antitrust Litigation*.[86] There, the plaintiffs neglected to request the abbreviations and acronyms the defendants used in internal communications.[87] After receiving the defendants' document production and learning the defendants commonly used abbreviations and acronyms, the plaintiffs argued the defendants' keyword search did not capture the agreed-upon universe of ESI.[88] The defendants successfully opposed the plaintiffs' request for a second search by pointing out the terms used in the initial search were selected and provided to the plaintiffs before the initial search was conducted.[89] The defendants had also already spent a substantial amount of time and money on the first search and did not wish to repeat their effort due to the plaintiffs' failure to request abbreviations and acronyms before the initial search.[90] Finding the plaintiffs had ample opportunity to request abbreviations and acronyms when the defendants first explained which search terms they intended to use, the court denied plaintiffs' request to compel the defendants to run a second search.[91]

2. Predictive Coding/TAR

Artificial intelligence and machine learning technologies have had a major impact on how larger e-discovery searches are handled. Once a comfort level is established with these technologies, they can save counsel an immense amount of time on document review.

Predictive coding is one form of technology-assisted review ("TAR"), which is a broader term that covers many different uses of technology in the documents review process. Predictive coding helps automate document review through a hybrid approach of human and technology review.

Through predictive coding, instead of manually reading every single document in a collection, reviewing attorneys can use software available through most e-discovery platforms to classify documents according to how they match concepts in sample documents selected by the reviewing attorneys. First, the reviewing attorneys review a relatively small subset of the

documents that need to be reviewed, coding the documents based on relevance and potentially other metrics. Then, once a sufficient sample set has been reviewed, the software completes the search based on the patterns it has learned from the attorney's review of the sample set. In other words, the software learns from the manual coding and then automates that logic to a larger group of documents. The software predicts how the reviewing attorney would code the remaining documents. Once the software generates its proposed set of documents for production, the reviewing attorney can review that final set instead of reviewing the thousands of pages (or tens of thousands of pages) of documents that the software determined to be irrelevant.

Predictive coding is increasingly accepted by courts as a legitimate method of conducting document review, especially in cases with a large volume of ESI. "Predictive coding or TAR has emerged as a far more accurate means of producing responsive ESI in discovery than manual human review of keyword searches."[92] "Studies show it is far more accurate than human review or keyword searches which have their own limitations."[93] Predictive coding review of ESI requires an "unprecedented degree of transparency and cooperation among counsel" in the review and production of ESI responsive to discovery requests and, as a result, courts typically require parties to disclose the technology used, the process, and the methodology, including the documents used to "train" the computer.[94]

3. De-Duplicating and De-NISTing

Counsel should also meet and confer on de-duplicating emails in the ESI production so that the same email does not get produced multiple times every time that particular email received a reply. By de-duplicating, only the last email in an email thread will get produced. ESI vendors can de-duplicate emails fairly easily if requested.

Counsel should also meet and confer on de-NISTing the ESI collected for review. This process removes certain file types that are unlikely to have any evidentiary value so that attorneys do not have to review them. The "NIST" in de-NIST stands for the National Institute of Standards and Technology, which is an agency that maintains a list of millions of file types that are frequently de-NISTed.[95] Although the list of file types is extensive, in general terms the ESI targeted for removal through de-NISTing includes system files, program files, and other non-user created data.

V. CONCLUSION

Although the world of e-discovery is polluted with industry jargon that counsel may wish to ignore, gaining a comfort level with and understanding of e-discovery is ethically required when counsel find themselves handling a case that involves or should involve requests for ESI. After all, you will not be able to get valuable ESI that may help your case if you do not know what to request or how to request it.

Part I of this two-part series should assist counsel with identifying an adversary's ESI and then targeting it through deployment of appropriate e-discovery tools. E-discovery is a cumulative process and the initial steps are critical for properly laying the groundwork to achieve a successful result. Requests for particular types of ESI such as metadata must be made early and counsel must be prepared to show a particularized need for such ESI. Failure to adequately identify such a need in the preliminary meet-and-confer process or to timely request ESI production could seriously harm the likelihood of success. Similarly, counsel who are careless in the drafting of keyword searches and terms who wish to refine their search later will have difficulty obtaining a second bite at the apple. These strategic decisions can only be competently made by counsel who are familiar with e-discovery rules and procedures that commonly arise in trust and estate matters.

Part II of this two-part series will address responding to e-discovery requests and asserting appropriate privacy and privilege objections, discovery of information that is not reasonably accessible, cost allocation among parties, and motions to compel.

** Crist, Biorn, Shepherd & Roskoph APC, Palo Alto, CA*

*** Withers Bergman LLP, San Diego, CA*

1 Cal. Bar Formal Opn. No. 2015-193 (citing ABA Model Rules Prof. Conduct, rule 1.1, com. [8]).

2 Cal. Bar Formal Opn. No. 2015-193 (citing Rules Prof. Conduct, rule 3-110(C)).

3 Cal. Bar Formal Opn. No. 2015-193.

4 San Diego County Bar Assn. Legal Ethics Opn. 2012-1.

5 Cal. Bar Formal Opn. No. 2015-193.

6 Cal. Bar Formal Opn. No. 2015-193 (citing Former Cal. Rules of Prof. Conduct, rule 3-110).

7 Cal. Bar Formal Opn. No. 2015-193.

8 *In re Napster, Inc. Copyright Litigation* (N.D. Cal. 2006) 462 F.Supp.2d 1060, 1067.

9 *Apple Inc. v. Samsung Electronics Co., Ltd.* (N.D. Cal. 2012) 881 F.Supp.2d 1132, 1136.

10 *Cedars-Sinai Medical Center v. Super. Ct.* (1998) 18 Cal.4th 1, 12.

11 *Hernandez v. Garcetti* (1998) 68 Cal.App.4th 675, 680.

12 *Coca-Cola Bottling Co. v. Super. Ct.* (1991) 233 Cal.App.3d 1273, 1294.

13 Code Civ. Proc., section 2023.030, subd. (d)(1), (4); see also *R. S. Creative, Inc. v. Creative Cotton, Ltd.* (1999) 75 Cal.App.4th 486 (affirming terminating sanctions based on discovery abuse, including destruction of evidence); see also *WeRide Corp. v. Kun Huang* (N.D. Cal. Apr. 24, 2020, No. 5:18-CV-07233-EJD) 2020 U.S.Dist. WL 1967209 at *3 (imposing terminating sanctions against defendant and striking answer where emails were automatically deleted after 90 days).

14 *R. S. Creative, Inc. v. Creative Cotton, Ltd.* (1999) 75 Cal.App.4th 486, 497; see also *New Albertsons v. Super. Ct.* (2008) 168 Cal.App.4th 1403, 1426.

15 Prob. Code, section 16006.

16 Prob. Code, section 9650, subd. (a)(1).

17 See, e.g., *Cooper v. State Farm Mutual Automobile Insurance Co.* (2009) 177 Cal.App.4th 876, 892 (insurer disposed of allegedly defective tire after promising to preserve it); *Coprich v. Super. Ct.* (2000) 80 Cal.App.4th 1081, 1091 (persons injured in rented car when tire blew out alleged that they had asked dealer and its insurer to preserve car and tire for use as evidence, but were later told that they no longer existed or had been sold).

18 Prob. Code, sections 870-884.

19 Prob. Code, section 871, subd. (h).

20 Prob. Code, section 877.

21 Code Civ. Proc., section 2031.010, subd. (a).

22 *Deyo v. Kilbourne* (1978) 84 Cal.App.3d 771, 782.

23 Cal. Rules of Court, rule 3.724(1).

24 Cal. Rules of Court, rule 3.724(8).

25 Evid. Code, section 413; *Cedars-Sinai Medical Center v. Super. Ct.* (1998) 18 Cal.4th 1, 16; CACI No. 204 ("You may consider whether one party intentionally concealed or destroyed evidence. If you decide that a party did so, you may decide that the evidence would have been unfavorable to that party.").

26 *WeRide Corp. v. Kun Huang* (N.D. Cal. Apr. 24, 2020, No. 5:18-CV-07233-EJD) 2020 U.S.Dist. WL 1967209 at *3.

27 Code Civ. Proc., section 2031.010, subd. (a).

28 Code Civ. Proc., section 2016.020, subd. (e).

29 See Code Civ. Proc., section 2016.020, subd. (d).

30 The Sedona Principles, *Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production* (2018) 19 Sedona Conf. J. 1 p. 169 ("Sedona").

31 Sedona, *supra,* at p. 169; *Williams v. Sprint/United Management Co.* (D. Kan. 2005) 230 F.R.D. 640, 646; *Aguilar v. Immigration & Customs Enforcement Division of U.S Department of Homeland Security* (S.D.N.Y. 2008) 255 F.R.D. 350, 354.

32 Sedona, *supra,* at p. 169; *Aguilar v. Immigration & Customs Enforcement Division of U.S Department of Homeland Security, supra,* 255 F.R.D. at p. 354.

33 *Aguilar v. Immigration & Customs Enforcement Division of U.S Department of Homeland Security* (S.D.N.Y. 2008) 255 F.R.D. 350, 354; Sedona, *supra,* at p. 211.

34 Sedona, *supra,* at p. 170.

35 Sedona, *supra,* at p. 170; *Aguilar v. Immigration & Customs Enforcement Division of U.S Department of Homeland Security, supra,* 255 F.R.D. at p. 356.

36 Sedona, *supra,* at p. 170.

37 *Ibid.*

38 Code Civ. Proc., section 2031.030, subd. (a)(2).

39 Sedona, *supra,* at p. 174.

40 Sedona, *supra,* at pp. 340-341 (glossary).

41 *Bailey v. Alpha Techs. Inc.* (W.D. Wa. June 1, 2017, No. C16-0727-JCC) 2017 U.S. Dist. WL 2378921 at *4.

42 *Bailey v. Alpha Techs. Inc., supra,* 2017 U.S.Dist. WL 2378921 at *4-5.

43 Sedona, *supra,* at pp. 340-341 (glossary).

44 *Aguilar v. Immigration & Customs Enforcement Division of U.S Department of Homeland Security* (S.D.N.Y. 2008) 255 F.R.D. 350, 356.

45 *Aguilar v. Immigration & Customs Enforcement Division of U.S Department of Homeland Security, supra,* 255 F.R.D. at p. 356.

46 Sedona, *supra,* at p. 180.

47 *Williams v. Sprint/United Management Co.* (D. Kan. 2005) 230 F.R.D. 640, 653.

48 *Aguilar v. Immigration & Customs Enforcement Division of U.S Department of Homeland Security* (S.D.N.Y. 2008) 255 F.R.D. 350, 356.

49 Sedona, *supra,* at p. 172.

50 Code Civ. Proc., section 2031.010, subd. (e).

51 Sedona, *supra,* at p. 128.

52 Sedona, *supra,* at p. 128.

53 Code Civ. Proc., section 2031.010, subd. (e).

54 *In re Lithium Ion Batteries Antitrust Litigation* (N.D. Cal. Feb. 24, 2015, No. 13–MD–02420 YGR [DMR]) 2015 U.S.Dist. WL 833681 at *3.

55 *Dodge, Warren & Peters Insurance Services, Inc. v. Riley* (2003) 105 Cal.App.4th 1414, 1421.

56 *In re Lithium Ion Batteries Antitrust Litigation, supra,* 2015 U.S.Dist. WL 833681 at *3.

57 Code Civ. Proc., section 2031.030, subd. (c)(1).

58 Code Civ. Proc., section 2031.310, subd. (g).

59 Code Civ. Proc., section 2031.030, subd. (c)(1).

60 Code Civ. Proc., section 2031.030, subd. (c)(4).

61 Code Civ. Proc., section 1985.8.

62 Sedona, *supra,* at p. 87.

63 *Ibid.*

64 Sedona, *supra,* at p. 88.

65 *Intermarine, LLC v. Spliethoff Bevrachtingskantoor, B.V.* (N.D. Cal. 2015) 123 F.Supp.3d 1215, 1216 (subpoena targeting ESI held in Dropbox account).

66 Sedona, *supra,* at p. 88.

67 Code Civ. Proc., section 2031.280, subd. (d)(1).

68 *Vasquez v. California School of Culinary Arts, Inc.* (2014) 230 Cal. App.4th 35, 43.

69 *United States ex rel. Carter v. Bridgepoint Educ., Inc.* (S.D. Cal. 2015) 305 F.R.D. 225, 245.

70 Sedona, *supra,* at p. 87

71 *Volkswagenwerk Aktiengesellschaft v. Super. Ct.* (1981) 123 Cal. App.3d 840.

72 See *Flora Crane Service, Inc. v. Super. Ct. of S.F.* (1965) 234 Cal. App.2d 767, 786.

73 Sedona, *supra,* at p. 173.

74 Sedona, *supra*, at p. 179.

75 Sedona, *supra,* at p. 173.

76 *United States ex rel. Carter v. Bridgepoint Educ., Inc.* (S.D. Cal. 2015) 305 F.R.D. 225, 246.

77 *Younes v. 7-Eleven, Inc.* (D.N.J. March 18, 2015, No. 13–3500 [RMB/JS]) 2015 U.S.Dist. WL 1268313 at *6.

78 *Chevron Corp. v. Stratus Consulting, Inc.* (D. Colo. Aug. 31, 2010, No. 10–cv–00047–MSK–MEH) 2010 U.S.Dist. WL 3489922 at *4.

79 *United States ex rel. Carter v. Bridgepoint Educ., Inc.* (S.D. Cal. 2015) 305 F.R.D. 225, 246.

80 *Ibid.*; *Aguilar v. Immigration & Customs Enforcement Division of U.S Department of Homeland Security* (S.D.N.Y. 2008) 255 F.R.D. 350, 357.

81 *Brinckerhoff v. Town of Paradise* (E.D. Cal. 2010, No. CIV. S–10–0023 MCE GGH) 2010 U.S.Dist. WL 4806966 at *10.

82 *Aguilar v. Immigration & Customs Enforcement Division of U.S Department of Homeland Security* (S.D.N.Y. 2008) 255 F.R.D. 350, 357.

83 *Williams v. Sprint/United Management Co.* (D. Kan. 2005) 230 F.R.D. 640, 654.

84 See generally *In re National Association of Music Merchants, Musical Instruments and Equipment Antitrust Litigation* (S.D. Cal. Dec. 19, 2011, MDL No. 2121) 2011 U.S.Dist. WL 6372826 (discussing sufficiency of keyword searches).

85 See, e.g., *Logtale Ltd. v. IKOR, Inc.* (N.D. Cal. July 31, 2013, No. C-11-05452 CW (DMR)) 2013 U.S.Dist. WL 3967750 at *3.

86 *In re Nat. Assn. of Music Merchants, Musical Instruments and Equipment Antitrust Litigation* (S.D. Cal. Dec. 19, 2011, MDL No. 2121) 2011 U.S.Dist. WL 6372826.

87 *Id.* at *2.

88 *Ibid.*

89 *Id.* at *2-3.

90 *Id.* at *3.

91 *The Sedona Conference Best Practices Commentary on the Use of Search & Information Retrieval Methods in E-Discovery* (Fall 2007) 8 Sedona Conf. J. 189, 204.

92 *Youngevity International, Corp. v. Smith* (S.D. Cal. Apr. 9, 2019, No. 16-cv-00704-BTM (JLB)) 2019 U.S.Dist. WL 1542300 at *11 (citing *Progressive Casualty Insurance Co. v. Delaney* (D. Nev. July 18, 2014, No. 2:11–cv–00678–LRH–PAL) 2014 U.S.Dist. WL 3563467 at *8); see also *Hyles v. New York City* (S.D.N.Y. Aug. 1, 2016, No. 10 Civ. 3119 [AT][AJP]) 2016 U.S.Dist. WL 4077114 at *2 ("[I]n general, TAR is cheaper, more efficient and superior to keyword searching.").

93 *Youngevity International, Corp. v. Smith, supra,* 2019 U.S.Dist. WL 1542300 at *11 (citing *Progressive Casualty Insurance Company v. Delaney, supra,* 2014 U.S.Dist. WL 3563467 at *8); see also *In re Lithium Ion Batteries Antitrust Litigation* (N.D. Cal. Feb. 24, 2015, No. 13–MD–02420 YGR [DMR]) 2015 U.S.Dist. WL 833681 at *3 ("[A] problem with keywords is that they often are overinclusive, that is, they find responsive documents but also large numbers of irrelevant documents."); but see *T.D.P. v. City of Oakland* (N.D. Cal. July 17, 2017, No. 16-cv-04132-LB) 2017 U.S.Dist. WL 3026925 at *5 (finding that keyword searches were not necessarily inadequate and such a determination was fact specific).

94 *Youngevity International, Corp. v. Smith, supra,* 2019 U.S.Dist. WL 1542300 at *12.

95 National Institute of Standards and Technology, <www.nist.gov> (as of Apr. 22, 2021).