



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

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

MCLE Article

I. INTRODUCTION

This article is Part II of a two-part series focusing on e-discovery rules relevant to trust and estate litigators. Part I was published in Volume 27, Issue 2, of the *Trusts and Estates Quarterly*. The goal of the two-part series is to arm the reader with the tools needed to properly conduct and respond to e-discovery in an efficient and effective way. This Part II focuses on responding to requests for electronically stored information (“ESI”), asserting appropriate objections, and compelling production of ESI in trust and estate litigation matters.

At the outset, the authors acknowledge that many federal cases are cited in this two-part series. Federal law is more developed than California law on the topic of e-discovery. Recognizing this reality, California state courts often find federal cases to be persuasive in the e-discovery context.¹ As a result, this two-part series relies heavily, but by no means exclusively, on federal cases.

II. RESPONDING TO REQUESTS FOR PRODUCTION OF ESI

A. Evaluation of ESI Requested

Once discovery requests are received, counsel should work closely with the client and any ESI consultant that has been retained to structure and then facilitate the collection of ESI from the responsive sources. Once that collection has been undertaken, counsel can review the documents for relevance, privacy, and privilege before production to the requesting party. In making this determination, counsel will want to undertake the following steps: (i) identify whether there is ESI responsive to the discovery requests, (ii) identify relevant electronic devices or sources from which the ESI can be harvested, (iii) identify whether the ESI is reasonably accessible from such identified sources, (iv) identify whether the requests require that the responding party translate any ESI into a different or readable format, (v) identify the type of ESI requested and form or forms of production requested, (vi) evaluate whether objections to the scope or form of ESI are appropriate, and (vii)

based upon these answers, develop a collection plan to collect the relevant ESI in a format that allows counsel to review the information and produce it to the requesting party.

Hopefully, prior to receipt of discovery requests, counsel has already implemented the steps identified in Part I of this article to identify relevant sources of ESI, preserved the ESI in the client’s possession, and met and conferred with the requesting party on the preservation of ESI and the form in which ESI will be produced. Upon receipt of discovery requests, counsel should review the potential sources of ESI that are responsive to the requested discovery and either revise the existing ESI preservation plan or develop such an internal plan for the first time. The discovery requests may ask for ESI or identify sources of ESI that counsel did not previously consider. In such an event, counsel will need to inform the client of the need to preserve these new sources of ESI. Counsel will also need to review the discovery requests to determine the form of production that is requested. If native format or metadata is requested and appropriate, counsel will need to undertake collection efforts to preserve the requested metadata.

B. Duty to Undertake Reasonable Search for Responsive ESI

Each party responding to a request for production of ESI has a duty to search each and every source of ESI that is in the responding party’s possession, custody, or control.² This includes information that is not in a party’s physical possession, but that is controlled by or accessible to that party.³ The responding party must affirm that a diligent search and a reasonable inquiry has been made in an effort to comply with the request for production of ESI.⁴

In addition, the duty of candor confers upon counsel the duty to employ only those means that are consistent with truth, and never to seek to mislead the judge or any judicial officer by an artifice or false statement.⁵ In the context of e-discovery, this duty confers upon the attorney a responsibility for ensuring that their clients conduct a comprehensive and appropriate ESI search.⁶ An adequate investigation should include an analysis of the sufficiency of the ESI search and, when electronic documents are involved, an analysis of the sufficiency of the search terms and the locations.⁷ Failure to meet this duty may subject the attorney to sanctions resulting from failure of the client to produce responsive ESI.⁸

In trust and estate litigation, the scope of documents under a party’s possession, custody, or control can vary depending on whether such party is responding in his or



her role as a fiduciary and the type of fiduciary role that is held. A responding party acting as personal representative is in possession, custody, or control of any documents that the decedent could access.⁹ In addition, a trustee, personal representative, or agent under power of attorney has a duty to keep records of their administration.¹⁰ Incumbent with this duty is the fiduciary's obligation to search all such records in responding to requests for production of ESI. Fiduciaries may also have access to the decedent's digital assets under the Revised Fiduciary Digital Assets Act, which was enacted in 2016.¹¹ Careful consideration should be given to the breadth of information that is actually available to the fiduciary before claiming that any ESI is not possessed by the fiduciary or under the fiduciary's custody or control.

C. Considerations in Collection of ESI

Once ESI responsive to the document requests has been identified, counsel will need to develop a plan to collect it from the identified sources. Formulation of this plan will require that counsel consider who is going to collect the ESI and how it will be collected. Manual collection is performed by the client or by the ESI consultant to manually remove the documents responsive to the request from the electronic devices or other sources.¹² Manual collection can be performed by the client by printing, copying the files, or "drag and drop" to another file location or by an ESI consultant using tools to extract the information.¹³ Automated or computer-assisted collection involves using computerized processes to collect ESI meeting certain criteria such as automated searches, predictive coding or other technology-assisted review tools,¹⁴ or de-duplication of multiple copies of the same email.¹⁵ For a detailed discussion of each of these tools, see Part I of this article.

Depending on the sources of ESI and the allegations and circumstances of each case, both manual and automated procedures for collection of ESI may be appropriate.¹⁶ Absent an agreement on the search methods to be used, counsel should be prepared to explain and justify the choice of search methods, especially if counsel expects the requesting party to allege that ESI has not been adequately preserved or searched.¹⁷ If manual collection is performed by the client, counsel should direct the client where to search (e.g., which application and which electronic device) and how to perform each search. Keywords for searching emails or electronic devices linked to the subject matter, names of the parties, and other operative words and phrases should be provided to the client, along with date ranges and specific senders, recipients, and document types that the client should target. In certain circumstances it may be necessary to perform tests or samples using the search methodology to determine if the criteria are appropriate.

If collection of metadata is important to the particular facts of the case, use of an ESI consultant to collect the ESI and produce it will be important to avoid claims that the data has been altered. The act of merely accessing or moving electronic data can change the relevant metadata.¹⁸ For example, moving a word processing file from one electronic device to another changes the creation and modification dates found in the metadata.¹⁹ In such instances, ESI consultants can use specific tools designed for forensically-sound collection of ESI, which does not alter or change the metadata.²⁰ In instances where metadata is important it may even be necessary to obtain a forensic image of the electronic device, such as the decedent's phone or computer. A forensic image is a duplicate copy of the subject electronic device—a replication of each bit and sector, including all allocated and unallocated space on the device.²¹ A forensic image also contains all of the embedded, residual metadata.²²

In addition, even when not essential, collection of ESI with metadata intact in trust and estate litigation will make it easier for counsel to cull, search, and analyze the data internally. For example, collecting emails in native format from the client will allow counsel to sort and search the data set in many different ways (e.g., date, sender, recipient, attachments, keyword searches) that would be impossible if the client simply provided a printed copy of each email. Therefore, even if the requesting party has only requested that the information be produced in PDF, it may be advantageous for counsel to collect the ESI in native format so that the information can be analyzed and sorted prior to production, especially if there is a large volume of responsive emails. Manual review of documents prior to production for privilege or responsiveness can be one of the most expensive components of a production. The added efficiency of reviewing emails and other documents in native format for relevancy and privilege and the use of search terms and computer assistance (such as de-duplication) should not be understated and can save counsel an immense amount of time.

In trust and estate litigation, the relevant ESI will depend on the facts and legal issues in dispute, but the most common sources of ESI are emails and data stored on personal computers and smartphones (whether belonging to a decedent or to a fiduciary). Ordinarily, the attorney or third-party provider formulating a discovery response plan would have the creator of the ESI available to answer questions about how the data was created, stored, and the naming convention used for the different files. For certain types of trust and estate litigation this will still be an option (such as claims of breach of duty against a fiduciary), but for other types of litigation (such as a will or trust contest), the creator of the ESI (the decedent) will not be available to provide this information. In



such instances, it might be easy to understand how a layperson reviewing a decedent's personal computer or phone that the layperson is unfamiliar with might not adequately search and retrieve all necessary information from the device. In such instances, search tools used by third-party providers can be invaluable—for both the party responsible for producing the information and the party requesting the information—to search and retrieve information from the decedent's electronic device. Indeed, in certain instances it may be essential to use a third-party provider to retrieve the data to ensure that the data is collected without inadvertently changing the metadata.

Where the ESI and related metadata stored on a decedent's electronic device are at issue in the litigation, obtaining a forensic image of the electronic device should be strongly considered by counsel. The responding party should understand that agreeing to a forensic image is only the first step in the production of ESI and does not result in a complete disclosure of all information obtained from the decedent's electronic device. Once the forensic image is obtained and uploaded to any one or more of the third-party evidence review platforms, the responding party can review and sort the information prior to production to the requesting party, thereby removing all private, privileged, and irrelevant information.

D. Attorney's Duty of Confidentiality in Responding to ESI Requests

1. Protection of Privileged Information

In the context of e-discovery, because of the volume of digitally stored information and the complexities and cost of the screening process, a lawyer must take special precautions that confidential information is not inadvertently disclosed.²³ An attorney has a duty to assert the attorney-client privilege to protect confidential communications between the attorney and the client as well as other privileged material.²⁴ The duty to protect confidential information extends not only to the message itself, but also to its metadata.²⁵ The duty to protect a client's confidential information necessarily involves insuring that such information in metadata is not produced.²⁶ Where appropriate, metadata can be scrubbed through commercially available software and an ESI consultant can assist in that effort if needed.

The attorney also has a duty to act reasonably to protect against inadvertent disclosure.²⁷ The attorney-client privilege will protect confidential communications between the attorney and client in cases of inadvertent disclosure *only if* the attorney and client act reasonably to protect that privilege.²⁸ A lack of reasonable care to protect against disclosing privileged and

protected information when producing ESI can be deemed a waiver of the attorney-client privilege.²⁹

2. Handling Inadvertently-Produced ESI

Given the volume of data that is produced in e-discovery, there is a heightened risk of inadvertent production of privileged material. Fortunately, California law provides a statutory claw-back, enabling parties to address inadvertent production.³⁰

In the event of an inadvertent production of ESI, the producing party may notify any recipient of the inadvertently produced ESI and assert a claim of privilege or attorney work product.³¹ The party in possession of the inadvertent production must then sequester the ESI and either return it or present it to the court conditionally under seal for a determination of the claim.³² If the receiving party wishes to seek a determination from the court on the claim, that party must file a motion with the court within 30 days of being put on notice of the producing party's claim of inadvertent production.³³ The inadvertently produced ESI may not be used while the parties await the court's determination on the claim of privilege or attorney work product.³⁴

E. Form of ESI in Production

If a demand for production specifies the form or forms of production, the responding party should produce the information in the form or forms specified, absent a reason for objection.³⁵ The common forms of production of ESI are native format, TIFF, and PDF. Native format refers to the file type and structure of the electronic document defined by the original creating application.³⁶ For Microsoft Word documents, these are .doc or .docx files; for Excel spreadsheets, these are .xls or .xlsx files.

If a demand for production does not specify a form or forms for producing a type of ESI, then 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.³⁷ If the responding party objects to a specified form of production, or if no form is specified in the demand, then the responding party shall state in its response the form in which it intends to produce each type of information.³⁸ A party need not produce the same electronically stored information in more than one form.³⁹

Therefore, if the responding party is able to produce the ESI in the form or forms requested, the responding party must ordinarily produce the information in that form absent reason for objection.⁴⁰ Furthermore, if the responding party



ordinarily maintains the information it is producing in a way that makes it searchable by electronic means, then the information should not be produced in a form that removes or significantly degrades this feature.⁴¹ Indeed, courts have held that production of ESI in PDF format may not be sufficient if the requesting party can show that the format is not reasonably usable and that the native format, with accompanying metadata, meet the criteria of reasonably usable whereas the PDF format does not.⁴²

This does not mean, however, that every party requesting ESI in native format is entitled to it. Typically, a requesting party does not need ESI produced in its native format in order to access, cull, analyze, search, and display the information.⁴³ The most common way to produce ESI is to create a static electronic image in TIFF or PDF, and place any extracted metadata into one or more separate load files.⁴⁴ The load file enables the requesting party to review the metadata associated with each TIFF or PDF file, without the need for the native format file. Indeed, it is often excessive for a party to demand ESI be produced in native format when the evidence needed to prove the claims and defenses of the parties is found on the face of the documents, and the information contained in the text will allow the requesting party to organize and search the documents.⁴⁵

F. ESI That Is in an Unusable Format or Not Reasonably Accessible

In some cases, the requested ESI is no longer in its original format and may be archived in a less usable format that is not reasonably accessible or usable. In such instances counsel must consider under what circumstances the ESI must be converted back to a more usable format, and who should pay for the conversion.

1. Duty to Search and Convert Data

There are limits to the requesting party's entitlement to ESI. A common objection in the ESI context is undue burden or expense based on the grounds the requested ESI is not reasonably accessible.⁴⁶ In such cases, the responding party would have to specifically identify the types or categories of ESI that it asserts are not reasonably accessible.⁴⁷ The responding party then bears the burden of demonstrating such inaccessibility.⁴⁸

To evaluate these disputes over whether ESI is reasonably accessible, the court considers such factors as the amount of data that would need to be searched, the time it would take to search that data, and the cost to the responding party in terms of attorney review and potentially retention of an ESI

consultant to assist with the search. The court then balances the responding party's burden against the requesting party's need for the ESI in the case. Even if the responding party establishes that the ESI is not reasonably accessible because of undue burden or expense, the court may still order its production if the court finds good cause for doing so.⁴⁹ In such cases, the court may limit the discovery or impose conditions, including allocation of the expense of the requested discovery.⁵⁰

Even if required to conduct an extensive search, responding parties are often able to successfully argue they are not required to convert data into a different format in order to comply with the ESI request. For example, parties typically are not required to restore ESI on backup tapes in order to produce it in native format.⁵¹

In the federal court case of *United States ex. rel. Cater v. Bridgepoint Education, Inc.*⁵², the Southern District of California held that the responding party did not have to convert data stored on backup tapes to native format for production.⁵³ The court recognized that the backup tapes were discoverable and that the responding party was responsible for preservation of the data maintained on them, but that was only the beginning of the analysis.⁵⁴ The court determined that the ESI sought, including native format emails, had been converted to backup tapes as part of the responding party's standard data retention policy, and that the data was therefore practically inaccessible.⁵⁵ After balancing the need for the ESI against the burden associated with gathering and producing it, the court determined the requesting party was not entitled to the backup tapes, emails in native format, or metadata.⁵⁶

In the California state court case of *Vasquez v. California School of Culinary Arts, Inc.*⁵⁷, however, the outcome in a dispute over requested data conversion was different. There, a party issued a subpoena seeking business records in an electronically searchable and storable format.⁵⁸ The requesting party agreed to pay the costs associated with extracting and producing the ESI, and made clear it sought the ESI in digital format only, not paper copies.⁵⁹ The records custodian filed a motion to quash the subpoena based on numerous objections, including its contention that compliance would be unduly burdensome.⁶⁰ The court denied the motion, ordered the custodian to comply with the request, and awarded the requesting party approximately \$11,000 in attorney's fees incurred in connection with opposing the motion to quash.⁶¹ The Second District Court of Appeal affirmed, noting that the provisions of Code of Civil Procedure section 1985.8 in effect at the time of the motion required production of the requested ESI.⁶² The court further noted that the requested documents existed in paper



format did not excuse the custodian from its obligation to convert them to an electronic format and produce them in an electronic format and in a reasonably usable form.⁶³

There is also statutory authority in California requiring responding parties to convert data into a reasonably usable form.⁶⁴ If the circumstances warrant data conversion, then the responding party may be entitled to have the requesting party pay for the associated costs.⁶⁵

2. *Inaccessible ESI*

Before deciding the format in which the ESI should be produced and which party should pay the costs, courts must carefully consider the degree to which the requested ESI has become legally inaccessible. Consideration of ESI's accessibility involves analysis of: (i) the extent to which the data at issue is actually inaccessible, and (ii) the apparent reasons for this status.⁶⁶ ESI is inaccessible when it is not readily usable and must be restored to an accessible state before the data is usable.⁶⁷ Backup tapes are generally considered to be inaccessible.⁶⁸ The court must also consider the circumstances under which the data was moved from its native state to backup tapes.⁶⁹ If, for example, data is converted to a less useful format during litigation or after litigation was probable, then the responding party may have to bear the cost associated with converting it back to native format since that party had a duty to preserve evidence.⁷⁰ If, on the other hand, it was an innocent conversion as part of ordinary business practices, then the requesting party will be responsible for the cost of production in the format requested, if production is required at all.⁷¹

3. *Cost Shifting*

Given the significant costs associated with e-discovery, a common point of contention is cost shifting. In one case where a requesting party asked that data be converted from the responding party's backup computer tapes to a more usable format, the estimated cost of that conversion was \$1.9 million.⁷² If the parties cannot agree on cost allocation, the court will have to determine which party pays for the various costs associated with e-discovery, including extracting the data, searching the data, and producing the data.⁷³

Many courts have adopted a seven-factor test to guide this decision that weighs the following factors: (i) the extent to which the request is specifically tailored to discover relevant information, (ii) the availability of such information from other sources, (iii) the total costs of production, compared to the amount in controversy, (iv) the total costs of production, compared to the resources available to each party, (v) the

relative ability of each party to control costs and its incentive to do so, (vi) the importance of the issues at stake in the litigation, and (vii) the relative benefits to the parties of obtaining the information.⁷⁴ Several of these factors have now been codified in California law governing e-discovery.⁷⁵

After weighing these factors, the court determines which party bears the cost.⁷⁶ In some cases, the court may determine that one side must pay some of the costs, such as costs associated with searching and recovering the requested ESI, while the other party must pay other costs, such as production and redaction.⁷⁷ Redaction is a cost that is typically borne by the responding party.⁷⁸

G. **Objections to Production of ESI**

Due to the pervasive and expansive nature of ESI, requests for production of ESI frequently implicate issues of overbreadth, relevance, privacy, and privilege. For example, a request to review the entire contents of a decedent's personal computer or smartphone might implicate each of these objections. As a result, courts have repeatedly recognized the need to protect private, privileged, and irrelevant information in ESI requests.⁷⁹ Claims for privacy may relate not only to the decedent, but also to third parties and other beneficiaries.

1. *Requirements for Objection to Production of ESI*

If the responding party objects to a demand for production, the response must: (i) identify with particularity any ESI falling within any category of item in the demand to which an objection is being made, and (ii) set forth clearly the extent of, and the specific ground for, the objection.⁸⁰

If an objection is based on a claim of privilege, the particular privilege invoked shall be stated.⁸¹ If an objection is based on a claim that the information sought is protected work product, that claim shall be expressly asserted.⁸² If an objection is based on a claim of privilege or a claim that the information sought is protected work product, the response shall provide sufficient factual information for other parties to evaluate the merits of that claim, including, if necessary, a privilege log.⁸³ Courts have held that when counsel for a party objects to production of documents, counsel has implied that the documents exist and counsel has reviewed them.⁸⁴

In trust and estate litigation, counsel should be aware of the effect of the death of the creator of the data on potential claims of privacy and privilege relating to the ESI.⁸⁵ There is no attorney-client privilege for communications relevant to an issue concerning claims through a deceased client, intention



of the decedent with respect to a writing affecting an interest in property, or validity of a writing affecting an interest in property.⁸⁶ In addition, there is authority that the personal right to privacy dies with the person, leading some practitioners to conclude that no privacy objection can be made on behalf of the decedent.⁸⁷ This does not, however, prevent other parties to the litigation, such as the decedent's children who were involved in transactions and engaged in personal communications with the decedent, from asserting their own privacy rights to certain ESI.

2. *Specific Objections to ESI Production*

Objections on the basis of relevance,⁸⁸ privilege, or privacy⁸⁹ should be carefully considered with respect to each ESI request. In addition to these common categories, the court must limit the frequency or extent of discovery of ESI, even from a source that is reasonably accessible, if the court determines that any of the following conditions exist: (i) it is possible to obtain the information from some other source that is more convenient, less burdensome, or less expensive, (ii) the discovery sought is unreasonably cumulative or duplicative, (iii) the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought, or (iv) the likely burden or expense of the proposed discovery outweighs the likely benefit, taking into account the amount in controversy, the resources of the parties, the importance of the issues in the litigation, and the importance of the requested discovery in resolving the issues.⁹⁰

3. *Sample Objections to Requests for Production of ESI*

Below is sample language to consider when objecting to a request for production of ESI.

Responding party objects to this request for production on the basis that it is possible to obtain the information from some other source that is more convenient, less burdensome, or less expensive in that [e.g., *requesting party has not shown a particularized need for the form of production requested OR requesting party has not shown a sufficient basis for production electronically stored information in native format*]. Code of Civil Procedure section 2031.060, subdivision (f)(1).

Responding party objects to this request for production on the basis that the discovery sought is unreasonably cumulative or duplicative in that [e.g., *responding party previously produced the responsive documents in searchable PDF*]. Code

of Civil Procedure section 2031.060, subdivision (f)(2).

Responding party objects to this request for production on the basis that requesting party has had ample opportunity by discovery in the action to obtain the information sought in that [e.g., *propounding party previously requested the ESI and failed to request that such information be produced with the requested metadata*]. Code of Civil Procedure section 2031.060, subdivision (f)(3).

Responding party objects to this request for production on the basis that the likely burden or expense of the proposed discovery outweighs the likely benefit, taking into account the amount in controversy, the resources of the parties, the importance of the issues in the litigation, and the importance of the requested discovery in resolving the issues in that [e.g., *the cost of collecting and producing the documents in native format with metadata intact without a showing of a particularized need for such metadata outweighs the burden on requesting party to sort and search the number of documents requested*]. Code of Civil Procedure section 2031.060, subdivision (f)(4).

III. PROTECTIVE ORDER

Given the sensitive nature of data often included within an ESI production, parties occasionally need to seek protective orders to either prevent production altogether or to ensure the ESI that is produced is only used for appropriate purposes. California law sets forth clear statutory guidelines for seeking and obtaining such protective orders.

A. Obtaining a Protective Order

If a responding party wishes to prevent or limit the ESI production, then that party must promptly file a motion for a protective order.⁹¹ Consistent with other discovery motions, a motion for a protective order concerning ESI must be accompanied by a meet and confer declaration.⁹² The grounds on which a protective order may be sought include annoyance, embarrassment, oppression, or, perhaps the most common of them all, undue burden and expense.⁹³ As with other discovery motions, the losing party involved in a motion for a protective order in the ESI context must pay the prevailing party's attorney's fees, unless the court determines the losing party acted with substantial justification.⁹⁴



B. Protective Order Based on Lack of Accessibility

A common objection to the production of ESI is that the requested data is not reasonably accessible because of undue burden or expense.⁹⁵ It is the objecting party's burden to demonstrate the undue burden.⁹⁶ Even if the objecting party establishes undue burden or expense, the court may nonetheless order discovery if the requesting party shows good cause.⁹⁷ In that event, however, the requesting party may be ordered to pay the cost associated with the production.⁹⁸

C. Scope of Protective Order

If the court finds good cause to enter the protective order, the court can enter a whole range of orders including prevention of the production altogether, extension of the production deadline, or the sealing of the production absent court order.⁹⁹ In some circumstances, the court may even order a party to preserve ESI pending adjudication of the case.¹⁰⁰

The court's power to limit the use of ESI produced in litigation is particularly important where proprietary business information and trade secrets are involved.¹⁰¹ In many trust litigation matters, the trust may own interests in ongoing businesses that will not want their financial performance numbers, client contact information, and the like to be produced without adequate protections in place. If counsel can negotiate a stipulated protective order that ensures such safeguards are in place, courts are typically receptive to entering such an order if there is good cause to do so.

IV. MOTION TO COMPEL PRODUCTION OF ESI

In some instances, and despite the best efforts of all parties to meet and confer, a motion to compel will be necessary to resolve issues related to the production of ESI. A motion to compel the production of ESI, or to compel the inspecting, copying, testing, or sampling of ESI, is subject to the same requirements as other motions to compel, with additional requirements specific to the discovery of ESI.

A. Information from a Source that Is Not Reasonably Accessible

There is a specific framework if a party is opposing the motion to compel on the basis that the ESI is from a source that is not reasonably accessible because of undue burden or expense.¹⁰² First, the party opposing the motion to compel on this basis has the burden of demonstrating that the information is from a source that is not reasonably accessible because of undue burden or expense.¹⁰³ Second, even if the party opposing

the motion to compel establishes that the information is from a source that is not reasonably accessible because of the undue burden or expense, the court may nonetheless order discovery if the demanding party shows good cause.¹⁰⁴ Finally, if the court finds good cause, the court may set conditions for the discovery of the ESI, including cost allocation.¹⁰⁵

B. Factors Specific to Production of ESI in a Motion to Compel

Even if ESI is reasonably accessible, the court must limit the extent of discovery if it determines that the factors under Code of Civil Procedure section 2031.060, subdivision (f), exist (the "ESI Discovery Factors"): (i) it is possible to obtain the information from some other source that is more convenient, less burdensome, or less expensive, (ii) the discovery sought is unreasonably cumulative or duplicative, (iii) the party seeking discovery has had ample opportunity by discovery in the action to obtain the information sought, and (iv) the likely burden or expense of the proposed discovery outweighs the likely benefit, taking into account the amount in controversy, the resources of the parties, the importance of the issues in the litigation, and the importance of the requested discovery in resolving the issues.¹⁰⁶

A typical fact pattern might involve a combination of one or more of these ESI Discovery Factors. The fact pattern might also encompass multiple different categories or sources of ESI from multiple sources. Federal case law on ESI discovery tends to focus on two issues, each of which is applicable in trust and estate litigation: (i) issues relating to the form of production (such as whether requested metadata should be produced), and (ii) issues related to the forensic examination of a party's electronic device.

1. Motion to Compel Production of Requested Metadata

If a party is requesting the production of metadata, there are generally two requirements that must be met: (i) the requesting party must show a "particularized need" for the metadata that exceeds functional utility, and (ii) the requesting party must ask for the production of metadata with sufficient particularity, preferably in the initial request.¹⁰⁷ These two factors interrelate with factors that the court must consider is evaluating the ESI Discovery Factors.

Whether a particularized need exists for the requested metadata depends on the facts of each case. A particularized need exists when metadata directly relates to the facts and relevant issues in the litigation. There is a particularized need when metadata would allow the requesting party to confirm



or contradict the timing of when the documents were authored, and such timing is a critical issue in the case.¹⁰⁸ In addition, a particularized need exists when the metadata relates to a spreadsheet with mathematical formulas, where such formulas are necessary to understand the spreadsheet.¹⁰⁹ In such circumstances, under the ESI Discovery Factors the ESI is not available from another source that is more convenient, less burdensome, or less expensive and the discovery request is not unreasonably duplicative or cumulative.

In addition, 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, the later request should be denied.¹¹⁰ In such circumstances, the party seeking discovery has already had ample opportunity to obtain the information sought, and the burden and expense of producing the information again with metadata could outweigh the potential benefit under the ESI Discovery Factors.

For example, in *Aguilar v. Immigrant Customs Enf't Div. of U.S. Dept. of Homeland Sec.*¹¹¹ (S.D.N.Y. 2008) 255 F.R.D. 350, the court examined a request for the production of metadata involving three categories of documents: (i) emails, (ii) word processing documents and electronic presentations, and (iii) spreadsheets (document types common in trust and estate litigation). The requesting party demanded all metadata for all electronic documents on grounds that metadata was relevant to their claims and because it would enable them to more efficiently sort and search the data.¹¹² The documents were produced in searchable PDF and the requesting party did not request the metadata until production was almost complete.¹¹³ With respect to the emails, it was alleged that the metadata was relevant because the emails did not contain information about who was blind copied (bcc'd).¹¹⁴ The court held that for the emails the searchable PDF was sufficient on the basis that (i) plaintiff did not request the metadata upfront and delayed in such request by several months, (ii) there was no showing that any bcc documents actually existed, and (iii) since there were only 500 emails, requesting party could not show an express need to search and sort the data.¹¹⁵

With respect to the word processing documents and electronic presentations, the court held that searchable PDF was sufficient on the basis that: (i) the requesting party failed to show a particularized need for the metadata—that the who and when of document creation or modification was relevant to their claims, and (ii) given the limited universe of documents (estimated 5,200 pages), the requesting party was not expected to encounter significant difficulty in searching and sorting the documents received.¹¹⁶ Finally, with respect to

the spreadsheets, the court acknowledged that while metadata was relevant when a spreadsheet relies on mathematic formulas, the spreadsheets at issue in the litigation were lists or data sets that could have also been created in a word processing program and therefore metadata was not necessary to review.¹¹⁷

In the context of ESI requests in trust and estate litigation, counsel should be prepared to show a combination of factors for each specific type of data when seeking to compel the production of metadata or native format.

Production of emails with metadata generally requires consideration of one or more of the following factors: (i) information regarding sender/recipient of the email, (ii) when it was sent, (iii) who was blind copied on the email, (iv) the email's relevance to the subject matter of the litigation (and there is actual evidence of such issues), and (v) whether and to what extent there is a large volume of emails to review such that the costs of production of the metadata are outweighed by the functional utility.

Production of word processing documents with metadata generally requires consideration of one or more of the following factors: (i) whether the creation of the document, author of the document, date of revisions to the document, or date of copying or transfer of the document are at issue in the litigation, (ii) whether there is a risk that the document will be deleted, and (iii) whether documents with tracked changes are important to the litigation.

Production of spreadsheets with metadata often requires that there be mathematical formulas that are necessary to analyze the information presented in the spreadsheet.

2. Motion to Compel Forensic Image of Electronic Device

A forensic image is a duplicate copy of an electronic device that contains all of the embedded, residual metadata.¹¹⁸ While direct access to a responding party's electronic storage device is technically permissible, counsel does not have an automatic right of direct access and such access is only justified in certain instances.¹¹⁹ The privacy, privilege, and relevance concerns in the production of ESI are most prevalent in using a forensic examination as the process necessarily captures *all* of the information on the device, including irrelevant information.¹²⁰ In addition, direct access to the responding party's computer system can also disrupt the responding parties use of the computer system (and any business activity that the computer system is used for) and potentially damage or harm the stability of the data and applications.¹²¹



A request for forensic examination of a responding party's electronic device is strongest when the responding party has withheld or deleted requested information and the forensic image is needed to recover the ESI or to potentially uncover additional concealed ESI.¹²² However, "mere skepticism" that an opposing party has withheld or failed to produce ESI is not enough.¹²³

In *Dodge, Warren & Peters Ins. Services, Inc. v. Riley*,¹²⁴ the court discussed the burden required to obtain a forensic image. The requesting party sued defendants for breach of fiduciary duty, misappropriation of trade secrets, unfair business practices, and breach of contract.¹²⁵ After filing the complaint, the requesting party filed a motion for preliminary injunction for the preservation of electronic evidence.¹²⁶ The court first observed that the requesting party could irretrievably lose evidence that otherwise would have been available. In addition, there was no other remedy that could provide the same relief, as this evidence was not available from any other source.¹²⁷ On the other hand, there was no harm to the responding party—the ESI would be copied in their presence and after working hours so as to not interrupt their ability to conduct business and no damage or loss of information would result from the copying.¹²⁸ Furthermore, the requesting party provided a protocol to ensure that any concerns about privacy or privilege were minimized.¹²⁹ The copied material would be unavailable to anyone except upon agreement of the parties or order of the court.¹³⁰ Finally, the reasonable cost to review the copied files for irrelevant and privileged information was to be borne by the requesting party, subject to reallocation by the trial court.¹³¹

Forensic examination may also be available where it is shown that the responding party has in good faith failed to adequately meet its duties in the production of discoverable information and the information is not available from any other source.¹³² In *Wynmoor Community Council, Inc. v. QBE Ins. Corp.*,¹³³ the hardcopy of the information requested had been destroyed in a natural disaster and the information was not available absent access to the ESI stored in the responding party's computer system.¹³⁴ However, the responding party testified that they presently lacked the capability to undertake a search of their computer system for the requested ESI.¹³⁵ The court observed that the responding party's inability to conduct the search of their ESI did not relieve them of their discovery obligations.¹³⁶ Next, the court found that based upon the fact that the information may not be available from any other source, and responding party's representation that it was unable to conduct the search themselves, a forensic examination of responding party's computer was warranted.¹³⁷

These factors interrelate with the factors the court must consider in evaluating the ESI Discovery Factors. When a party has withheld or deleted the requested information, it will not be possible to obtain the information from another source and the discovery cannot be said to be unreasonably cumulative or duplicative. In addition, where the responding party is unable to meet its duties of production, the requesting party has not had ample opportunity to obtain the information sought and the burden or expense is justified.

In trust and estate litigation some of the most common sources of ESI are the decedent's computer, smartphone, or other portable electronic device. Information on one or more of these devices may not be available from any other source and may have significant evidentiary value in the litigation. For example, if there are documents created by the decedent on an electronic device that express the decedent's testamentary intent, and there is a dispute concerning verification of who created the document, when it was created, or when it was edited. Under these circumstances a forensic image may be appropriate if the responding party is unable to collect the metadata themselves. A forensic image also may be available in any circumstances where counsel can show that the responding party has withheld documents, failed to conduct an adequate search themselves, or the information is subject to spoliation or deletion.

3. Examination Protocol

In order to resolve concerns regarding privacy, privilege, and damage to the responding party's computer system that are raised by a forensic examination, counsel should present to the court an examination protocol concurrent with the motion to compel. The protocol should: (i) be documented in an agreed-upon (or court-approved) protocol, (ii) recognize the rights of nonparties such as family members or business partners, (iii) be narrowly restricted to protect confidential and personally identifiable information or provide for a process for the information to be reviewed by the parties or a court-appointed neutral, (iv) provide for an agreement between the parties on inadvertently disclosed confidential information, and (v) provide for the protection of the integrity and security of the electronic device to be examined.¹³⁸ In order to accomplish this, counsel will almost certainly have to retain a qualified consultant or vendor to take custody of the data and manage it.¹³⁹

Consider the following example protocol relating to the forensic examination of a party's computer for emails: (i) the responding party's expert would provide a declaration on the feasibility of the recovery of the emails, (ii) a court-appointed computer expert would create a forensic image



of the responding party's hard drive, (iii) the disclosure of any private or privileged information to the court-appointed expert would not result in a waiver of such privacy right or privilege, (iv) the parties would agree on a date and time to access the computer, (v) upon production of the forensic image, a copy would be provided to the responding party, who would review the ESI and provide any responsive emails to the requesting party (all documents withheld on a claim of privilege would be recorded on a privilege log), and (vi) the responding party would be the sole custodian of the forensic image of its computer system.¹⁴⁰

V. CONCLUSION

Part II of this two-part series provides guidelines for responding to e-discovery requests, asserting appropriate objections, and, where necessary, filing motions with the court concerning ESI requests. Used in conjunction with Part I, the two-part series arms the trust and estate litigator with the tools needed to properly conduct e-discovery and respond to e-discovery requests. Those tools can be used to make the discovery process more efficient and effective, enabling attorneys to search and organize a large volume of data in a fraction of the time it would take in the old days of paper copies, and providing sources of evidence that were previously unavailable to litigants.

Given advances in technology, the e-discovery software platforms available today, and the evolving case law that acknowledges the utility of e-discovery, practitioners who skip e-discovery are losing a competitive advantage. To avoid getting left behind, it is indeed time to get digital.

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

***Withers Bergman LLP, San Diego, California*

This article is available as an
ONLINE SELF-STUDY TEST.



Visit: cla.inreachce.com
for more information.

- 1 *Liberty Mutual Ins. Co. v. Superior Court* (1992) 10 Cal.App.4th 1282, 1288 ("Because of the similarity of California and federal discovery law, federal decisions have historically been considered persuasive absent contrary California decisions.").
- 2 Code Civ. Proc., section 2031.230.
- 3 *Pardon v. Watchtower Bible and Tract Society of New York, Inc.* (2017) 16 Cal.App.5th 1246, 1266.
- 4 Code Civ. Proc., section 2031.220.
- 5 Bus. & Prof. Code, section 6068, subd. (d); see also Cal. Rules Prof. Conduct, rule 5-200.
- 6 *Qualcomm Inc. v. Broadcom Corp.* (S.D. Cal. 2008, No. 05-CV-1958-B (BLM)) 2008 U.S. Dist. Lexis 911 *31 [2008 WL 66932].
- 7 *Id.* at *37-*38.
- 8 See *Ibid.*
- 9 See Evid. Code, section 953, subd. (a).
- 10 See Prob. Code, section 16060.
- 11 Prob. Code, sections 870-884.
- 12 The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production (2018) 19 Sedona Conf. J. 1, 167 ("Sedona"). A copy of this paper may be accessed at: <<https://thesedonaconference.org/sites/default/files/publications/The%20Sedona%20Principles%20Third%20Edition.19TSCJ1.pdf>>.
- 13 *Id.* at p. 167.
- 14 *Id.* at p. 168.
- 15 *Ibid.*
- 16 Sedona, *supra*, at p. 167.
- 17 *Id.* at p. 165.
- 18 Sedona, *supra*, at p. 209.
- 19 *Ibid.*
- 20 *Id.* at p. 167.
- 21 *In re Am. Med. Sys. Inc. Pelvic Repair Sys. Prod. Liab. Lit.* (2016 S.D. Va.) M.D.L. No. 2325, 9-10; *Wynmoor Community Council, Inc. v. QBE Ins. Corp.* (2012 S.D. Fla.) 280 F.R.D. 681, 686-687.
- 22 *Id.* at pp. 686-687.
- 23 Cal. Bar Formal Opn. No. 2015-193 (citing Comments 16 and 17 to ABA Model Rules Prof. Conduct, rule 1.6).
- 24 Evid. Code, sections 952, 954, 955.
- 25 State Bar Formal Opn. No. 2010-179.
- 26 *Ibid.*
- 27 State Bar Formal Opinion. No. 2010-179.
- 28 See *Regents of University of California v. Superior Court (Aquila Merchant Services, Inc.)* (2008) 165 Cal.App.4th 672, 683.
- 29 See *Kilopass Technology Inc. v. Sidense Corp.* (N.D. Cal. May 1, 2012, No. C 10-02066 SI) 2012 WL 1534065 *2-3 (attorney-client privilege deemed waived as to privileged documents released



- through e-discovery because screening procedures employed were unreasonable).
- 30 Code Civ. Proc., section 2031.285.
 - 31 Code Civ. Proc., section 2031.285, subd. (a).
 - 32 Code Civ. Proc., section 2031.285, subd. (b).
 - 33 Code Civ. Proc., section 2031.285, subd. (d)(1).
 - 34 Code Civ. Proc., section 2031.285, subd. (d)(2).
 - 35 Code Civ. Proc., section 2031.280.
 - 36 Sedona, *supra*, at pp. 340-341 (glossary).
 - 37 Code Civ. Proc., section 2031.280, subd. (d)(1).
 - 38 Code Civ. Proc., section 2031.280, subd. (c).
 - 39 Code Civ. Proc., section 2031.280, subd. (d)(2).
 - 40 *Vasquez v. California School of Culinary Arts, Inc.* (2014) 230 Cal. App.4th 35, 43 (responding party may not object to production of ESI on ground that such information can be produced in paper form if requesting party has specified production in electronic format).
 - 41 *L.H. v. Schwarzenegger* (E.D. Cal. May 14, 2008, No. CIV S-06-2042 LKK GGH) 2008 U.S. Dist. Lexis 86829 *12-13 [2008 WL 2073958].
 - 42 *Ellis v. Toshiba America Information Systems, Inc.* (2013) 218 Cal. App.4th 853, 861.
 - 43 Sedona, *supra*, at p. 172.
 - 44 *Id* at 172; 2 CA Pretrial Civil Procedure: The Waggstaffe Group 43-VI[B][2][a].
 - 45 Sedona, *supra*, at p. 172.
 - 46 Code Civ. Proc., section 2031.210, subd. (d).
 - 47 *Ibid.*
 - 48 *Vasquez v. California School of Culinary Arts, Inc.* (2014) 230 Cal. App.4th 35, 42.
 - 49 *Vasquez v. California School of Culinary Arts, Inc., supra*, 230 Cal. App.4th at p. 42.
 - 50 *Ibid.*
 - 51 *United States ex. rel. Carter v. Bridgepoint Education, Inc.* (S.D. Cal. 2015) 305 F.R.D. 225; *Vasquez v. California School of Culinary Arts, Inc., supra*, 230 Cal.App.4th 35, 43.
 - 52 *United States ex. rel. Carter v. Bridgepoint Education, Inc.* (S.D. Cal. 2015) 305 F.R.D. 225.
 - 53 *Id* at p. 247.
 - 54 *Ibid.*
 - 55 *Id.* at p. 241.
 - 56 *Id.* at p. 247.
 - 57 *Vasquez v. California School of Culinary Arts, Inc.* (2014) 230 Cal. App.4th 35.
 - 58 *Id.* at p. 38.
 - 59 *Id* at p. 39.
 - 60 *Ibid.*
 - 61 *Ibid.*
 - 62 *Id.* at p. 41.
 - 63 *Id.* at p. 43.
 - 64 Code Civ. Proc., section 2031.280, subd. (e).
 - 65 *Ibid.*
 - 66 *United States ex. rel. Carter v. Bridgepoint Education, Inc., supra*, 305 F.R.D. 225, 240.
 - 67 *Ibid.*
 - 68 *Ibid.*
 - 69 *Ibid.*
 - 70 *Ibid.*
 - 71 *Ibid.*
 - 72 *Toshiba America Electronic Components, Inc. v. Super. Ct.* (2004) 124 Cal.App.4th 762.
 - 73 *United States ex. rel. Carter v. Bridgepoint Education, Inc., supra*, 305 F.R.D. 225, 242.
 - 74 *United States ex. rel. Carter v. Bridgepoint Education, Inc., supra*, 305 F.R.D. 225, 242 (quoting *Zubulake v. UBS Warburg LLC* (S.D.N.Y. 2003) 217 F.R.D. 309, 322).
 - 75 Code Civ. Proc., section 2031.060, subd. (f)(4).
 - 76 *United States ex. rel. Carter v. Bridgepoint Education, Inc., supra*, 305 F.R.D. 225, 247.
 - 77 *Ibid.*
 - 78 *National Lawyers Guild v. City of Hayward* (2020) 9 Cal.5th 488.
 - 79 *Landau v. Lamas* (M.D. Penn. Dec. 15, 2017, No. 3:15-CV 1327) 2017 U.S. Dist. LEXIS 206158 *20; *Hespe v. City of Chi* (N.D. Ill. Dec 15, 2016, No. 13 C 7998) 2016 U.S. Dist. Lexis 173357 *7.
 - 80 Code Civ. Proc., section 2031.240, subd. (b).
 - 81 Code Civ. Proc., section 2031.240, subd. (b).
 - 82 *Ibid.*
 - 83 Code Civ. Proc., section 2031.240, subd. (c)(1).
 - 84 *Bihun v. AT&T Information Systems, Inc.* (1993) 13 Cal.App.4th 976, 991, fn. 5.
 - 85 For a detailed discussion on the topic of a decedent's right to privacy, see the article from the California Trusts and Estates Quarterly (2021), Volume 27, Issue 2, entitled "How to Invade Someone's Privacy 101," co-authored by Erin A. Norcia, Esq and Hengameh Kishani, Esq.
 - 86 Evid. Code, sections 957, 960, 961.
 - 87 *Flynn v. Higham* (1983) 149 Cal.App.3d 677, 683.
 - 88 Code Civ. Proc., section 2017.010.
 - 89 Cal. Const., art. I, section 1.
 - 90 Code Civ. Proc., section 2031.060, subd. (f).
 - 91 Code Civ. Proc., section 2031.060, subd. (a).



- 92 *Ibid.*
- 93 Code Civ. Proc., section 2031.060, subd. (b).
- 94 Code Civ. Proc., section 2031.060, subd. (h).
- 95 Code Civ. Proc., section 2031.060, subd. (c).
- 96 *Ibid.*
- 97 Code Civ. Proc., section 2031.060, subd. (d).
- 98 Code Civ. Proc., section 2031.060, subd. (e).
- 99 Code Civ. Proc., section 2031.060, subd. (b).
- 100 *Dodge, Warren & Peters Ins. Services, Inc. v. Riley* (2003) 105 Cal. App.4th 1414, 1422.
- 101 See *Children's Hospital Central California v. Blue Cross of California* (2014) 226 Cal.App.4th 1260 (hospital's concerns about trade secrets did not warrant denial of motion to compel as such concerns could be handled through appropriate protective orders).
- 102 Code Civ. Proc., section 2031.310.
- 103 Code Civ. Proc., section 2031.310, subd. (d).
- 104 Code Civ. Proc., section 2031.310, subd. (e).
- 105 Code Civ. Proc., section 2031.310, subd. (f).
- 106 Code Civ. Proc., section 2031.310, subd. (g).
- 107 *United States ex rel. Carter v. Bridgepoint Educ., Inc.* (S.D. Cal. 2015) 305 F.R.D. 225, 246.
- 108 *Chevron Corporation v. Stratus Consulting, Inc.* (D.Colo. Aug. 31, 2010, No. 10-cv-00047-MSK-MEH) 2010 U.S. Dist. WL 3489922 *4.
- 109 *Williams v. Sprint/United Mgmt Co.* (D.Kan. 2005) 230 F.R.D. 640, 647 (the cells containing formulas, which are arguably metadata themselves, often display a value rather than the formula itself; therefore in order to understand the spreadsheet the user must be able to ascertain the formula within the cell).
- 110 *Aguilar v. Immigration & Customs Enforcement Division of U.S. Department of Homeland Security* (S.D.N.Y. 2008) 255 F.R.D. 350, 357.
- 111 *Aguilar v. Immigrant Customs Enf't Div. of U.S. Dept. of Homeland Sec., supra*, 255 F.R.D. 350.
- 112 *Id.* at p. 359.
- 113 *Ibid.*
- 114 *Ibid.*
- 115 *Id.* at p. 360.
- 116 *Aguilar v. Immigrant Customs Enf't Div. of U.S. Dept. of Homeland Sec., supra*, 255 F.R.D. at p. 359.
- 117 *Ibid.*
- 118 *Wynmoor Community Council, Inc. v. QBE Ins. Corp.* (2012 S.D. Fla.) 280 F.R.D. 681, 687.
- 119 *A.M. Castle & Co. v. Byrne* (S.D. Tex. 2015) 123 F.Supp.3d 895, 900; *Marsulex Envtl. Techs. V. Selip S.P.A.* (M.D. Penn. May 21, 2019, No. 1:15-CIV-00269) 2019 U.S. Dist. Lexis 85153 *30-31.
- 120 Sedona, *supra*, at p. 128.
- 121 *Ibid.*
- 122 *Marsulex Envtl. Techs. V. Selip S.P.A.* (M.D. Penn. May 21, 2019, No. 1:15-CIV-00269) 2019 U.S. Dist. Lexis 85153 *30-31; *Wynmoor Community Council, Inc. v. QBE Ins. Corp.* (S.D. Fla. 2012) 280 F.R.D. 681, 687.
- 123 *Midwest Feeders, Inc. v. Bank of Franklin* (S.D. Miss. July 19, 2016, No. 5:14cv78-DCB-MTP) 2016 U.S. Dist. Lexis 93994 *4.
- 124 *Dodge, Warren & Peters Ins. Services, Inc. v. Riley* (2003) 105 Cal. App.4th 1414.
- 125 *Dodge, Warren & Peters Ins. Services, Inc. v. Riley, supra*, 105 Cal. App.4th at pp. 1417-1418.
- 126 *Id.* at p. 1418.
- 127 *Id.* at p. 1421.
- 128 *Ibid.*
- 129 *Ibid.*
- 130 *Ibid.*
- 131 *Ibid.*
- 132 *Crosmun v. Trs. of Fayetteville Tech. Cmty. Coll.* (N.C. Ct. App. 2019) 832 S.E.2d 223, 234.
- 133 *In Wynmoor Community Council, Inc. v. QBE Ins. Corp.* (S.D. Fla. 2012) 280 F.R.D. 681
- 134 *Ibid.*
- 135 *Id.* at p. 686.
- 136 *Ibid.*
- 137 *Id.* at p. 687.
- 138 Sedona, *supra*, at p. 129; *Crosmun v. Trs. of Fayetteville Tech. Cmty. Coll.* (N.C. Ct. App. 2019) 832 S.E.2d 223, 234.
- 139 Sedona, *supra*, at p. 129.
- 140 *Playboy Enters. v. Welles* (S.D. Cal. 1999) 60 F.Supp.2d 1050, 1054-1055.