What Every In-House Attorney Needs to Know About E-Discovery

June 23, 2022

ReedSmith
Driving progress
through partnership

ACC Association of Corporate Counsel

Contents

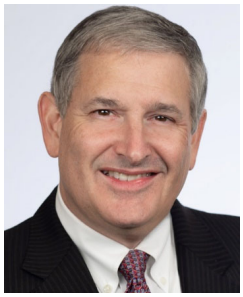
What Every In-House Attorney Needs to Know About E-Discovery

June 23, 2022

ACC Association of Corporate Counsel

ReedSmith
Driving progress through partnership

Today's Speakers



David Cohen
Partner
Reed Smith

Michelle Mantine
Partner
Reed Smith

Disclaimer

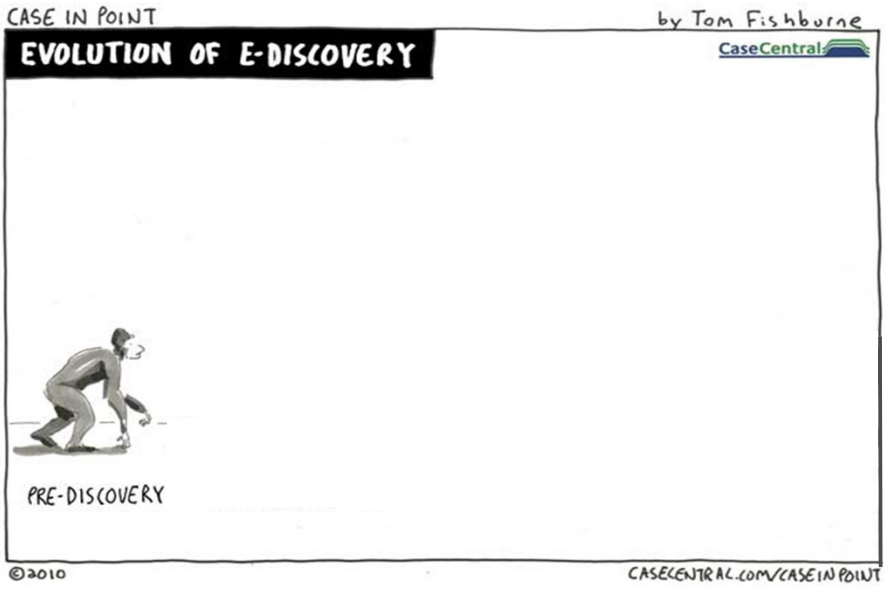
- This presentation is informational in nature and may not be relied upon as legal advice.

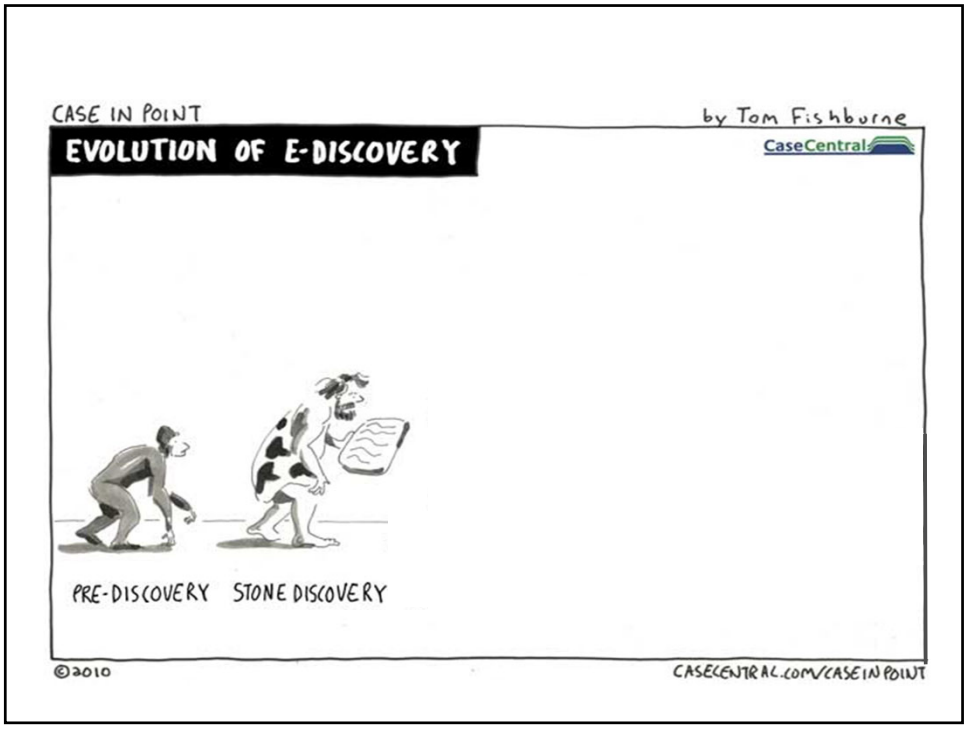
Disclaimer

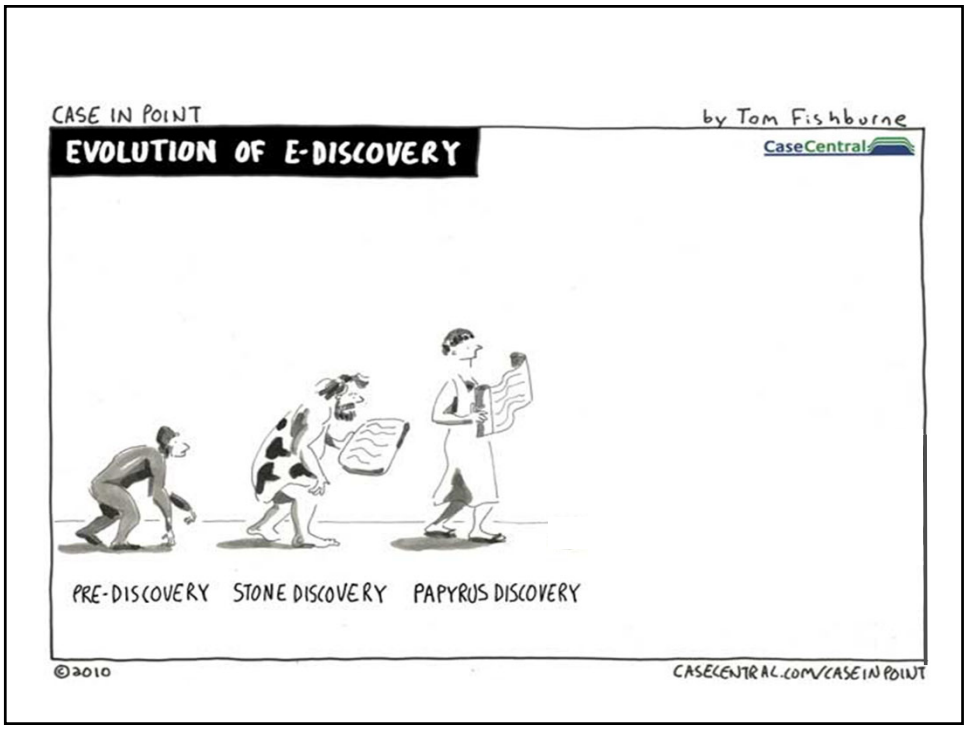
- This presentation is informational in nature and may not be relied upon as legal advice.
- This presentation is not age appropriate for children, senior citizens, or those with high blood pressure or a history of heart conditions. All stunts are performed by professionals. Do not try these at home.

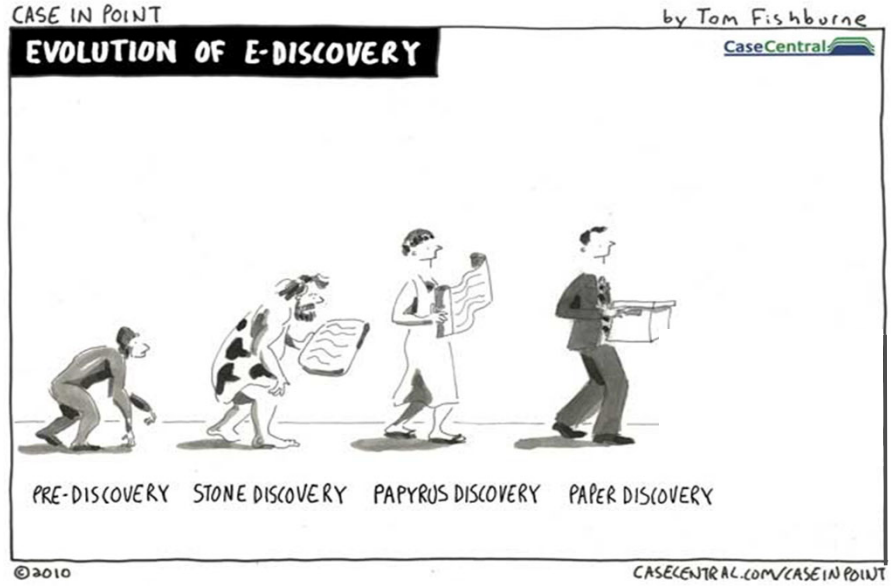
What We Will Cover

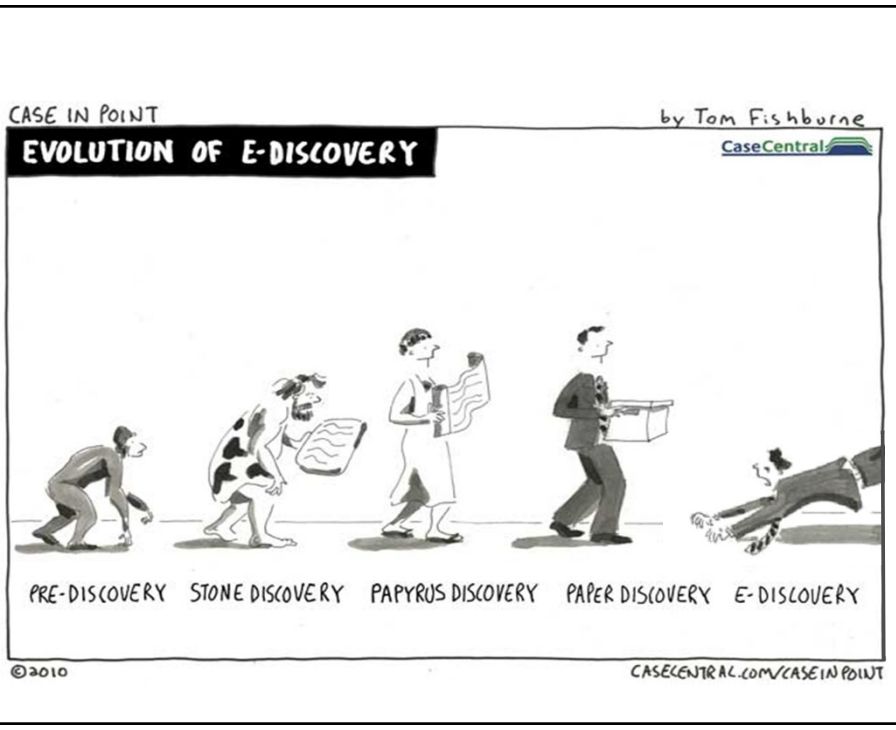
1. Basics About E-Discovery
2. The "Dirty Dozen": Pitfalls to Avoid in Working with E-Discovery Service Providers
3. Available E-Discovery Resources




CASE IN POINT
by Tom Fishburne
EVOLUTION OF E-DISCOVERY
CaseCentral
PRE-DISCOVERY
STONE DISCOVERY
©2010
CASECENTRAL.COM/CASEINPOINT


CASE IN POINT
by Tom Fishburne
EVOLUTION OF E-DISCOVERY
CaseCentral
PRE-DISCOVERY
STONE DISCOVERY
PAPYRUS DISCOVERY
©2010
CASECENTRAL.COM/CASEINPOINT

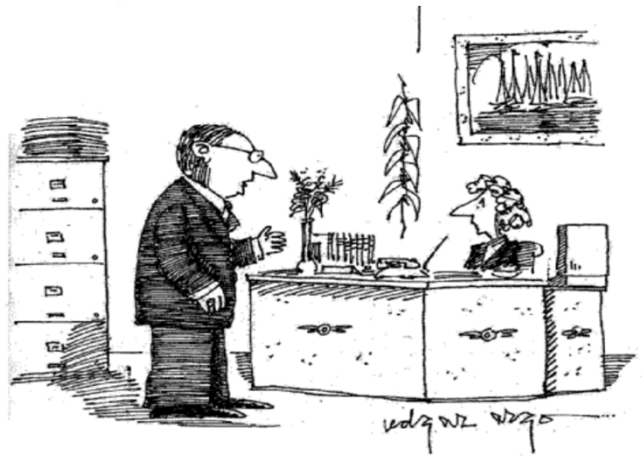

CASE IN POINT
by Tom Fishburne
EVOLUTION OF E-DISCOVERY
CaseCentral
PRE-DISCOVERY
STONE DISCOVERY
PAPYRUS DISCOVERY
PAPER DISCOVERY
©2010
CASECENTRAL.COM/CASEINPOINT


CASE IN POINT
by Tom Fishburne
EVOLUTION OF E-DISCOVERY
CaseCentral
PRE-DISCOVERY
STONE DISCOVERY
PAPYRUS DISCOVERY
PAPER DISCOVERY
E-DISCOVERY
©2010
CASECENTRAL.COM/CASEINPOINT

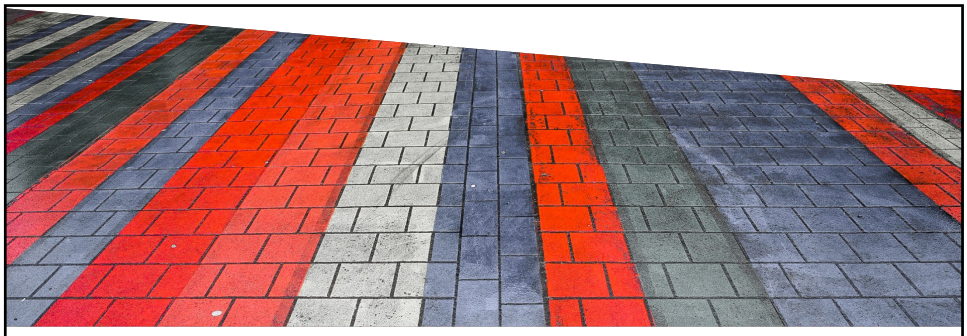
Why E-Discovery is a "Big Deal"

1. Data is Proliferating
2. Everything is Discoverable
3. E-Discovery is Evolving
4. E-Discovery Can Be Complicated
5. E-Discovery Can Be Expensive
6. E-Discovery Mistakes Lead to Sanctions

The Proliferation of Data



"Go through the files and image everything over 10 years old…but make copies first!"

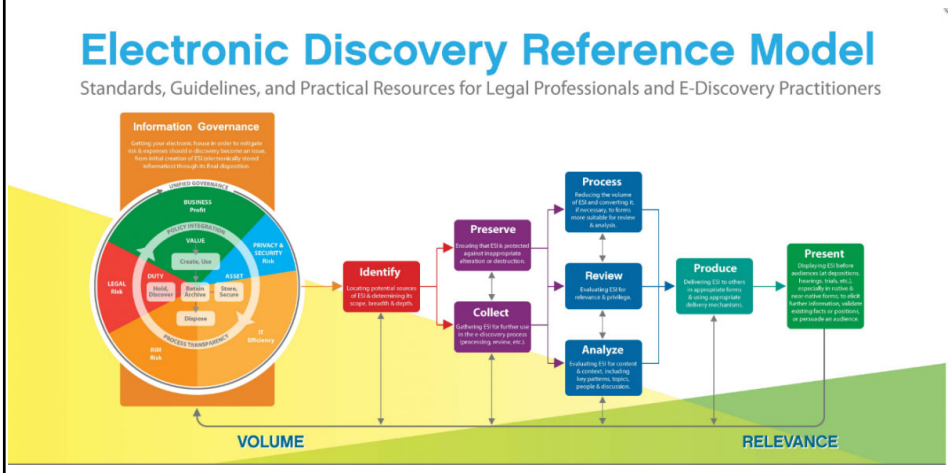


Basics About E-Discovery

8 Basics That In-House Counsel Should Know

1. Basic Stages of E-Discovery
2. Rules of Thumb
3. Legal Hold Best Practices
4. New Data Sources and Collections
5. Non-Waiver Orders
6. Predictive Coding and Other Technology
7. Production Considerations
8. Cross-Border Discovery and GDPR

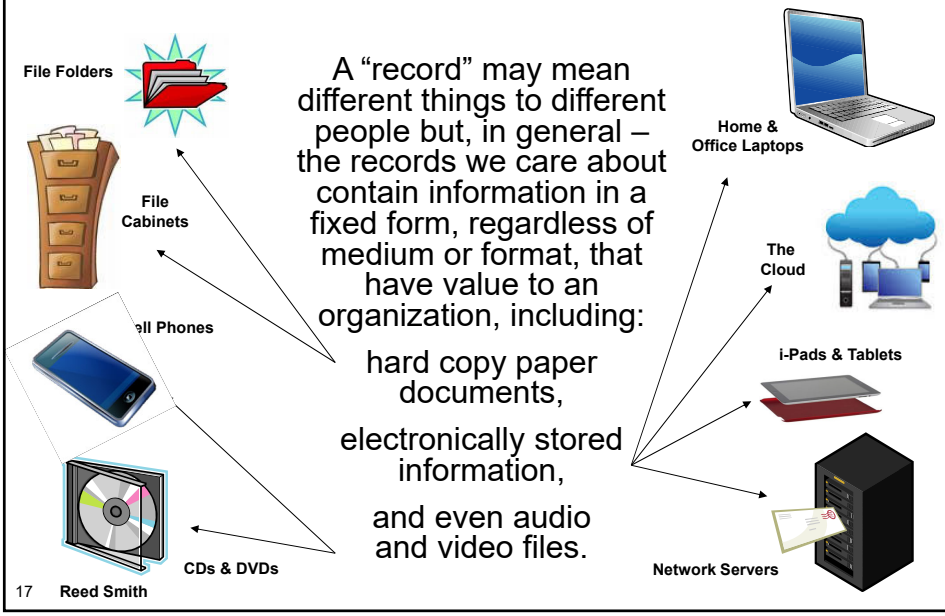
Basic Stages of E-Discovery



Rules of Thumb

- One Gigabyte averages about 35,000 pages (about 100 banker's boxes)
- Not unusual for a single custodian to have 50 Gbs of emails and other ESI
- If you have to collect from 10 custodians, you could have 500 Gb = 17.5 million pages
- One Terabyte = 1,024 Gb = 35+ million pages

Everything is Discoverable



Translation…

The Discovery process can be one of the most expensive and risky phases of a litigation or investigation!

The Scope of Discovery

Rule 26(b)(1):

Scope in General. Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible in evidence to be discoverable.

Preservation

- Give attention immediately to preserving all potential relevant ESI and paper documents – issue a Legal Hold!
- Preservation in place used increasingly instead of preservation through collection
  - Turning off automatic deletion for custodians
- Proportionality comes to preservation
  - See FRCP 26(b)(1) and comments to 37(e)
- Special care required for ephemeral data sources
  - Texts, other cell data, VMs, Slack, Yammer, etc.
- Cast the preservation net broadly
  - *Ronnie Van Zant* opinion and others…

Rule 37(e)

FAILURE TO PRESERVE ELECTRONICALLY STORED INFORMATION.

If ESI that **should have been preserved** in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve the information, and the information cannot be restored or replaced through additional discovery, the court may:

(1) Upon a finding of prejudice to another party from loss of the information, order measures no greater than necessary to cure the prejudice;

(2) Only upon a finding that the party acted with the intent to deprive another party of the information's use in the litigation,

(a) presume that the lost information was unfavorable to the party;

(b) instruct the jury that it may or must presume the information was unfavorable to the party; or

(c) dismiss the action or enter a default judgment.

Rule 37(e) Advisory Committee Notes

"Another factor in evaluating the reasonableness of preservation efforts is proportionality. The court should be sensitive to party resources; aggressive preservation efforts can be extremely costly, and parties (including governmental parties) may have limited staff and resources to devote to those efforts. … A party urging that preservation requests are disproportionate may need to provide specifics about these matters in order to enable meaningful discussion of the appropriate preservation regime."

The Daily Standard

June 23, 2022 $1.50

High 87
Low 73

Classified	E1-5
Crossword	B2
Dear Abby	C4
Comics	B7
Lotteries	A3
Movies	B9
Obituaries	A7
Local	C8-10
World	C1-7
Stocks	B2
Sports	D1

D1
Pirates take series from Cubs!

23

JUDGE IMPOSES HEAVY SANCTIONS FOR LEGAL HOLD FAILURES

ANYTOWN, USA Yesterday a local judge handed down the largest sanction ever imposed in this county for failure to adequately preserve, process and produce electronic records potentially relevant to their pending litigation. The Judge explained that preservation and production of records potentially relevant to pending or anticipated litigation is the duty of every party in a dispute, and outside law firms have an independent duty to take reasonable steps to ensure compliance by their clients.

See Sanctions A3

"They did not seem to understand their duties with regard to electronic evidence."

When is a Legal Hold Required?

A	B	C	D
Litigation is "Foreseeable"	Litigation is "Reasonably Anticipated"	Litigation is "Likely"	Litigation is "Pending or Probable"

The **Correct** Answer is… ?

24 **Reed Smith**

When is a Legal Hold Required?

Litigation is "Foreseeable"	Litigation is "Reasonably Anticipated"	Litigation is "Likely"	Litigation is "Pending or Probable"
A	B	C	D

The **Correct** Answer is… ?

D. *Cianci v. Phoenixville Area Sch. Dist.,* No. 20-4749, 2022 BL 92338, at *8 (E.D. Pa. Mar. 18, 2022)

When is a Legal Hold Required?

Litigation is "Foreseeable"	Litigation is "Reasonably Anticipated"	Litigation is "Likely"	Litigation is "Pending or Probable"
A	B	C	D

The **Correct** Answer is… ?

D. *Cianci v. Phoenixville Area Sch. Dist.,* No. 20-4749, 2022 BL 92338, at *8 (E.D. Pa. Mar. 18, 2022)

C. 2015 Advisory Committee Notes to Fed. R. Civ. P. 37(e)

When is a Legal Hold Required?

Litigation is "Foreseeable"	Litigation is "Reasonably Anticipated"	Litigation is "Likely"	Litigation is "Pending or Probable"
A	B	C	D

The **Correct** Answer is… ?

D. *Cianci v. Phoenixville Area Sch. Dist.,* No. 20-4749, 2022 BL 92338, at *8 (E.D. Pa. Mar. 18, 2022)

C. 2015 Advisory Committee Notes to Fed. R. Civ. P. 37(e)

B. *Bistrian v. Levi,* 448 F. Supp. 3d 454, 473 (E.D. Pa. 2020)

When is a Legal Hold Required?

Litigation is "Foreseeable"	Litigation is "Reasonably Anticipated"	Litigation is "Likely"	Litigation is "Pending or Probable"
A	B	C	D

The **Correct** Answer is… ?

D. *Cianci v. Phoenixville Area Sch. Dist.,* No. 20-4749, 2022 BL 92338, at *8 (E.D. Pa. Mar. 18, 2022)

C. 2015 Advisory Committee Notes to Fed. R. Civ. P. 37(e)

B. *Bistrian v. Levi,* 448 F. Supp. 3d 454, 473 (E.D. Pa. 2020)

A. *Victor v. Moss,* No. 1:20-CV-425, 2021 BL 208403, at *7 (M.D. Pa. June 4, 2021)

When is a Legal Hold Required?

A	B	C	D
Litigation is "Foreseeable"	Litigation is "Reasonably Anticipated"	Litigation is "Likely"	Litigation is "Pending or Probable"

The **Correct** Answer is… ?

E. All of the Above!

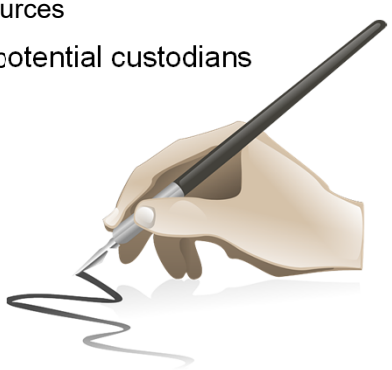
Legal Hold Basics

- Adopt legal hold policies and procedures **before** litigation hits!
- Initiate a legal hold notice as soon as practicable
- Don't over-preserve

  - Don't follow a "fear-based" strategy
  - Track all legal holds
    - Use a consistent process
    - Software or spreadsheet system
- Promptly lift legal holds when matters end
- Return to existing practices for retaining/deleting data

Adopt Best Practices for Legal Holds

- Have a plan – preferably in a written policy!
  - Standard hold notice templates are drafted and ready to go
  - Process in place for notifying IT staff to stop Auto-Delete
  - Be aware of non-custodial data sources
- Issue prompt written notices to all potential custodians
  - Sufficiently broad distribution
- Include all relevant data sources
  - Current employees
  - Former and departing employees
  - Third parties
  - Non-custodial data sources
- Include all relevant data types
  - Don't forget text and Teams messages



Custodian Interviews

- Document all steps
- Use fully developed collection templates to help act as a guide
- Consult with IT to ensure that you are aware of all potential ESI sources in which to discuss with custodians
- If a vendor is collecting, ensure they are aware of all types of data that will need to be collected and introduce them to custodians
- In the age of remote work, were private devices/accounts used?

New Data Sources: Texts/Teams/Zoom

Rise in velocity, variety, and volume

- Greater volumes of email and chat data and videoconference recordings
- New collaboration tools increase the types and amount of discoverable data
  - Courts may require the production of data from collaboration tools such as Slack (***Benebone LLC v. Pet Qwerks, Inc., et al.,*** WL 831025, at 3 (C.D. Cal. 2021))
  - Regulatory attention: Recent FINRA guidance specifically recognizes Teams Polling, Whiteboards, and other interactive features as charts which can be considered correspondence/communications and subject to retention/supervision and subject to the regulations

Collections – Forensic vs Active Data

- When is a forensic collection needed?
  - Chance of deleted/altered data
  - Is cost a factor?
- Who is best situated to make collections?
  - Vendor
  - In-house IT
  - Custodian
  - Law Firm
- Can a custodian self collect?
  - Will anything be lost?
  - Will original metadata be preserved?

Federal Rule of Evidence 502(d)

(d) CONTROLLING EFFECT OF A COURT ORDER.
A federal court may order that the privilege or protection is not waived by disclosure connected with the litigation pending before the court—in which event the disclosure is also not a waiver in any other federal or state proceeding.

Rule 502(d) Order

- Explicitly incorporate Rule 502(d) language into any case-specific protective order regarding non-waiver
- Explicitly remove inadvertence and reasonableness analysis under Rule 502(b) – ***Irth Solutions, LLC v. Windstream Commc'ns LLC***, No. 2:16-cv-219 (S.D. Ohio Aug. 2, 2017)
- Use broad non-waiver language to include any production of documents, not just an "inadvertent" production – incorporate "quick peek" reviews if appropriate
- Also prepare clawback provisions to instruct as to procedures if a privileged document has been produced, inadvertently or otherwise

Leveraging Advanced Technology

- Early Case Assessment (ECA): using advanced technology to cull documents and identify key evidence
- Email Threading
- Predictive Coding a.k.a. Technology Assisted Review a.k.a. TAR
  - TAR 1.0: Seed Sets and Training the System
  - TAR 2.0: Continuous Active Learning
- Automated Privilege Detection
- Automated Redaction Tools
- This Technology Saves Substantial Time and Money

Why Predictive Coding?

- Cost savings
- Time savings
- Reduced risk of errors (?)
- Greater objectivity in classifications
- Sometimes volume of documents and/or value of case makes 100% human review impractical

Production Considerations

- Production specifications may be negotiated or even included in a formal protocol discussed and agreed to with the opponent
- Important information found in the specifications includes:
  - Format of production
  - Bates numbering
  - Acceptable production media
  - Required metadata
  - Non-waiver order

Cross-Border Discovery and GDPR

- The European General Data Protection Regulation (GDPR) prohibits “processing” or “transfer” of “personal data” of European data subjects
- Penalties for violations are severe: up to the greater of 20 million Euro or 4% of worldwide annual revenue
- Accordingly, do not transfer documents from Europe to the U.S. for discovery without first discussing these issues with us
- We are also seeing increased attention to privacy in other jurisdictions outside the U.S., including jurisdictions in Asia and Australia

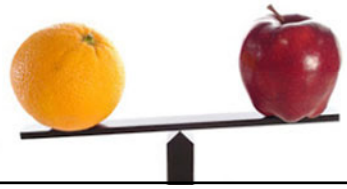
The “Dirty Dozen”: Pitfalls to Avoid in Working with E-Discovery Service Providers

The “Dirty Dozen”: Pitfalls to Avoid in Working With E-Discovery Service Providers

1. When comparing provider *processing and hosting* pricing, be sure to compare “apples-to-apples”
2. When comparing provider *review* pricing, be sure to compare “apples-to-apples”
3. Not all ECA/culling is alike
4. When contracting with providers, be sure to adequately consider data security issues
5. When contracting with providers, be sure that the contract covers all applicable charges (including data export charges) and that there are no reviewer charges during supplier database downtime
6. Not all deduping is alike
7. Not all email threading is alike
8. Avoid use of too many issue tags (preferably 10 or fewer)
9. Not all predictive coding is alike
10. Drill down on your provider’s primary review process
11. Drill down on your provider’s quality control (QC) process
12. Ensure that knowledgeable outside counsel oversees the document review and performs quality assurance

The "Dirty Dozen": Pitfalls to Avoid in Working With E-Discovery Service Providers

1. **When comparing provider *processing and hosting* pricing, be sure to compare "apples-to-apples"**
   - Beware of "free" processing or hosting offers – the vendor will need to make up those costs with other charges (e.g. data export)
   - If the provider is charging by the gigabyte, find out if they are charging based on the original volume or the "unpacked" volume where compressed data has been decompressed
   - The decompressed volume can increase the total volume by **1.2-2.0 times** – and therefore the cost by a corresponding percentage
   - Many providers include hourly personnel charges in their per-GB processing quotes, but others charge hourly ***in addition to*** the per-GB charges



The "Dirty Dozen": Pitfalls to Avoid in Working With E-Discovery Service Providers

2. **When comparing provider *review* pricing, be sure to compare "apples-to-apples"**
   - In addition to comparing primary reviewer hourly pricing, be sure to also account for the charges of quality control and project management personnel
   - Per document pricing can be advantageous to making "apples-to-apples" comparisons, incentivizing providers to be efficient in reviews, and offering greater certainty in budgeting
3. **Not all ECA/culling is alike**
   - All service providers say that they offer early case assessment and culling, but few are proactive about its use – When applied properly, these techniques can substantially reduce review volumes, time, and costs
   - Rely on knowledgeable discovery counsel to cull databases with ECA/analytics tools
   - Rely on knowledgeable discovery counsel to help devise search terms, including multiple iterations informed by "hit-by-term" reports and sampling

The "Dirty Dozen": Pitfalls to Avoid in Working With E-Discovery Service Providers

4. **When contracting with providers, be sure to adequately consider data security issues**
   - Consider background checks and conflict checks for all reviewers
   - Consider requiring all reviewers to sign confidentiality agreements
   - Conduct due diligence on provider's data security – major providers (and law firms) have recently been victims of data breaches and/or ransomware attacks
   - If permitting remote review, what extra data security measures and/or security software are being implemented?
5. **When contracting with providers, be sure that the contract covers all applicable charges (including data export charges) and that there are no reviewer charges during supplier database downtime**
   - Include provisions that hosting/license charges will not continue when databases become inactive – the provider should be required check back with you after any significant period of inactivity

The "Dirty Dozen": Pitfalls to Avoid in Working With E-Discovery Service Providers

6. **Not all deduping is alike**
   - Be sure that deduping occurs not just within custodians but also across custodians
   - Be careful – once deduping occurs, custodians cannot be removed
7. **Not all email threading is alike**
   - Ensure that your provider is using threading to remove duplicative emails from repetitive review
   - Some providers only use threading to group the emails together (while still charging you hourly or per document to review the duplicates) or, even worse, some only use for QC to ensure consistent coding
8. **Avoid use of too many issue tags (preferably 10 or fewer)**
   - Issue tags slow down the review
   - Most provider reviewers are very inconsistent in using them (especially if there are many)
   - Automated tagging (through targeted searching) is a much less costly (and more consistent/reliable) substitute for many issue tags

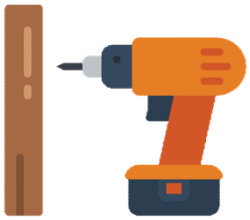
The "Dirty Dozen": Pitfalls to Avoid in Working With E-Discovery Service Providers

9. Not all predictive coding is alike

- Every vendor says they offer predictive coding
- Few are proactive about suggesting it and using it to substantially reduce review volumes and costs
- Experienced legal judgment, and often negotiations with opposing parties/courts, can be required as part of the process, so rely on knowledgeable legal counsel to advise on use of predictive coding
- Consideration of predictive coding starts at the very outset of the case: it impacts the language of discovery protocols, the breadth of search terms, and other issues, so be sure that you are avoiding barriers from the start

10. Drill down on your provider's primary review process

- Ensure that privilege terms are pre-highlighted to improve accuracy of privilege determinations
- Reviewers do not need to make privilege determinations on non-responsive documents



The "Dirty Dozen": Pitfalls to Avoid in Working With E-Discovery Service Providers

11. Drill down on your provider's quality control (QC) process

- QC should occur promptly after primary review so that ongoing mistakes can be corrected before they are repeated on numerous additional documents
- In addition to some random sampling, QC should be targeted to the most likely mistakes, e.g. with the benefit of TAR scoring
- Make sure that all of the combined QC does not exceed what is reasonable and necessary

12. Ensure that knowledgeable outside counsel oversees the document review and performs quality assurance

- This is not just an ethical requirement – it is important for quality
- Competent counsel will almost always catch significant provider errors
- Improve quality and reduce cost of counsel oversight by relying on e-discovery lawyers who are more experienced, at lower rates than associates

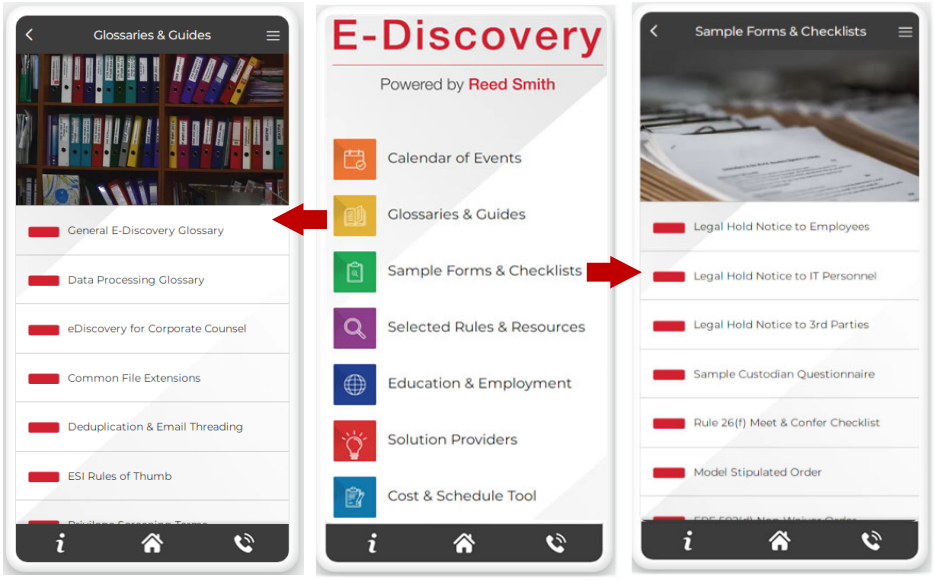
Optimize Communication with Discovery Providers

- Have designated points of contact for the provider, your company, and your outside counsel
- Schedule regular calls/meetings at least weekly to address ongoing issues and decisions
- Keep detailed agendas/to-do lists, including assignments of responsibility, to ensure that required tasks are accomplished
- Arrange to obtain a progress report, at least weekly, to keep track of overall progress and compare to any applicable deadlines
  - Ensure that progress tracking goes beyond primary review to also cover QC, productions, etc.
  - Always allow extra time for unanticipated complications, newly discovery data sources, etc.

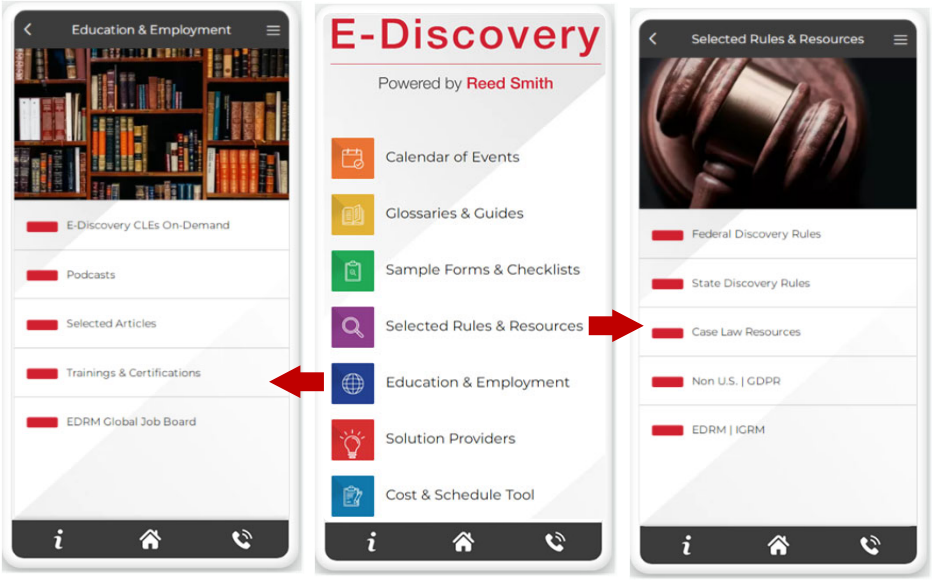
Available E-Discovery Resources

Get the App!

51 **Reed Smith**



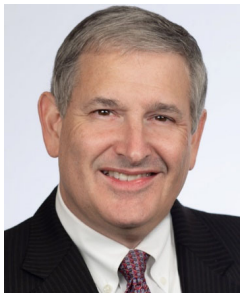
52 **Reed Smith**



National/Special E-Discovery Counsel

- Consistent and defensible processes across cases
- Cost minimization through reduced pricing
- Advance attention to litigation readiness, including data minimization and optimizing legal holds
- Implementing streamlined and efficient identification, collection, processing, review, and production procedures
- Focused attention on e-discovery issues
- Minimizing risks and maximizing clout in e-discovery battles
- Developing and maintaining credibility with judges and regulators
- Encompass e-discovery practice as part of a cost-effective and winning discovery and litigation strategy

Thank You!



David Cohen
drcohen@reedsmith.com
412-288-1098

Michelle Mantine
mmantine@reedsmith.com
412-288-4268

Please feel free to reach out with any questions!

The Legal Intelligencer

Traditional Legal Hold Post-COVID: A Discussion on Best Practices

Beyond these basics, business changes surrounding the COVID-19 pandemic should motivate companies to update their legal hold policies and practices to ensure that they properly address remote work scenarios, including data repositories outside the office and the increased use of collaboration tools beyond email.

February 03, 2022 at 12:23 PM

By David Cohen and Kristen Pologruto

The COVID-19 pandemic has forced companies to adapt to significant changes in the business environment. In March 2020, many companies instituted office closings, sending most of their employees' home to work remotely. In turn, this led to the increased use of home computer systems, and new collaboration and communication platforms, such as Microsoft Teams, Slack and Zoom. Nearly two years later, it is apparent that at least some remote work, and the increased use of home systems and collaboration and messaging applications, is not going away.

Optimal legal hold management begins with the adoption of "best practices" including: issuing legal holds as soon as practicable; scoping notices to avoid under-retention or over-retention; properly documenting and tracking legal holds; sending periodic reminder notices to hold custodians; and promptly lifting legal holds once the underlying matters are resolved. Beyond these basics, business changes surrounding the COVID-19 pandemic should

motivate companies to update their legal hold policies and practices to ensure that they properly address remote work scenarios, including data repositories outside the office and the increased use of collaboration tools beyond email. This article addresses traditional legal hold best practices and recommends consideration of updates post-COVID.

Legal Hold Best Practices

- **Prompt implementation of legal holds**. A legal hold should be implemented promptly, as soon as a party is on notice of, or reasonably anticipates, litigation or an investigation See *Nupson v. Schnader Harrison Segal & Lewis,* No. 18-cv-2505 (E.D. Pa. Apr. 07, 2021). The failure to implement timely legal holds, including the suspension of automatic deletion protocols, and sending legal hold notices to custodians of relevant information, can lead to the loss or deletion of evidence and result in costly remedies, or even spoliation allegations and sanctions. See Fed. R. Civ. P. 37(e) (setting forth potential remedies for the improper loss or deletion of relevant electronic evidence); *DR Distributions v. 21 Century Smoking,* 513 F. Supp. 3d 839 (N.D. Ill. 2021) (court imposed sanctions where evidence was lost as a result of the responding party's failure to issue written litigation holds and failure to disable autodelete functions.)

- **Properly scoping legal holds**. This requires a "balancing act." On one side, it is important to make sure that the list of hold notice recipients, and identification of relevant information sources, are sufficiently broad and comprehensive to preserve identifiable discoverable information. See Fed. R. Civ. P. 26(b) (defining the scope of discovery to include all information relevant and proportional to the claims and defenses of the parties); *Mahboob v. Education Credit Management,* No. 15-cv-0628-TWR-AGS (S.D. Cal. March 1, 2021) (court awarded attorney fees to requesting party after deletion of cellphone data, that should have been placed on hold).

On the other side, the list of custodians and scope of the hold should not be so overbroad as to create burdens, costs, and business disruption beyond what is reasonable and proportional for the investigation or litigation at hand. Since what is reasonable may ultimately be assessed in hindsight, when in doubt about the appropriate breadth of a hold, the safer course is to implement

broader rather than narrower holds in the first instance, and then adjust holds as appropriate as further information becomes available about the matter and relevant data sources.

- **Documentation and tracking**. Legal hold information to track generally includes identification of the matter, the custodians put on hold, when legal hold notices were issued to those custodians, acknowledgements and followups to those notices (including periodic reminders), copies of the hold notices and reminders, records of subsequent additions or modifications to the holds, and information about the termination of any holds. For companies with only one or only a few holds, tracking may be accomplished manually, *e.g.* on a spreadsheet. Companies that have more than a few holds should consider using one of the software products or systems that have automated legal hold tracking capabilities.

- **Notice reminders**. Some courts have held that it is not enough to send litigation hold notices—litigation parties should also follow up with key custodians to ensure compliance. See *Hyundai Motor America v. North American Automobile Services*, No. 20-82102-Civ-Middlebrooks/Matthewman at *5 (S.D. Fla. July 22, 2021) ("in-house and outside counsel not only owe a duty to advise their clients to preserve relevant evidence, they also owe an independent duty to monitor and supervise or participate in a corporation's effort to comply with its duty to preserve evidence."). Most legal holds stay in force for months to years. Where potentially relevant information remains in the control of custodians (i.e. it is not all collected at the outset) or where relevant information may continue to be generated, it is important periodically to remind custodians of holds in place, and their associated preservation duties, to reduce the risk that discoverable information will be lost or deleted.

- **Timely releasing legal holds**. Once a legal hold is no longer justified, the hold should be released and custodians who were subject to the hold should be notified. This helps reduce over-retention of information, and returns control of retention to the company's underlying retention policies and ordinary practices. Generally. holds may be released when matters are settled or resolved (including running of the time period for appeal of any disposition) or, for matters that have never resulted in litigation or an investigation, when circumstances (including the passage of time) suggest that a future litigation or investigation no longer appears likely.

Modernizing Legal Hold Policies and Practices

The prompt implementation of legal holds is no less important post-COVID than it was pre-COVID—but it has gotten more challenging. Work from home, and the increased use of non-traditional collaboration platforms, translates to having more information sources requiring preservation. Accordingly, companies should check their standard legal hold notices templates, and update as necessary, in order to:

- Notify custodians of data sources that must be preserved, include any personal devices or cloud locations where they may have stored relevant information;
- Alert custodians that relevant communications, including messages and call recordings on Teams, Slack, Zoom, and other collaboration platforms, are discoverable and must be preserved. See, e.g. *Benebone v. Pet Qwerks,* 8:20-cv-00850-AB-AFMx (C.D. Cal. Feb 18, 2021) (parties ordered to meet and confer about data to be searched, including defendant's Slack messages);
- Request custodians to contact the legal team or discovery team if they have relevant texts, voicemails, call recordings, social media posts, or collaborative platform communications, to help to ensure proper preservation; and
- Instruct custodians to discontinue use of ephemeral communication systems when communicating about anything potentially relevant to the legal hold.

In addition, legal hold practices and procedures should also be updated to account for the increased number of remote employees and the possibility of higher than historical turnover, including:

- Providing instructions to hold custodians not to dispose of or replace a home computer or other personal device that may hold relevant information, without first contacting the legal team or discovery team for instructions;
- Adopting procedures to identify departing hold custodians and to ensure that their potentially responsive data is preserved; and
- Developing effective communication strategies with remote employees to reduce the chance that relevant information will be lost. See *Sanz v. Wells Fargo Bank, N.A.*, No. 19-23122-CIV-COOKE/GOODMAN (S.D. Fla. June 21, 2021) (plaintiff's request for an adverse inference instruction was denied when plaintiff failed to establish any loss of evidence or bad faith conduct).

Finally, adjust and update retention and production practices in light of the rise in use of "modern attachment" in applications like Google Drive and OneDrive in Microsoft 365. These applications allow users to create links to documents in emails instead of attaching documents. The links found in these emails are not attachments and should not be treated as such, but if they independently are relevant then they must be preserved, searched and produced as needed. See *Nichols v. Noom*, No. 20-cv-3677 (S.D.N.Y. Mar. 11, 2021) (rejecting plaintiff's argument that hyperlinks found in a number of the produced emails were the same as attachments and automatically should be produced with the emails, but confirming that relevant information should be produced). By updating your company's or clients' hold policies and practices to account for post-COVID business realities, you can help to achieve legal compliance and reduce risks of costly sanctions or other remedies that can result from any loss of evidence after a legal hold should be in place.

E-Discovery associate Craig Chaney aided in the preparation of this article.

David Cohen *is a partner and* **Kristen Pologruto** *is e-discovery counsel in the global law firm Reed Smith.*

TAR Frequently Asked Questions

1. What is TAR?

In the litigation and e-discovery arena, “TAR” stands for “Technology Assisted Review.” This term is often used interchangeably with “Predictive Coding.” It refers to a process in e-discovery whereby computer programs or technology are used to facilitate, accelerate, or substitute for, human document review based on how documents are grouped, presented, categorized, analyzed, highlighted, etc. The use of TAR includes both instances in which the computer program or technology is relied upon to make responsiveness determinations, and those instances where the technology is used to prioritize review or help with quality control, but all responsiveness determinations are made by human reviewers.

2. How many documents do you need to have before it is worth considering using TAR?

There is no “magic number” for the minimum volume of documents that are appropriate for the use of TAR, but the potential cost savings increase substantially with larger volumes. It generally is not worth using TAR for fewer than 10,000-20,000 electronic documents because the set-up and transaction costs may exceed the savings. For any review population of more than 10,000 - 20,000 documents, you should consider using TAR.

3. How much does TAR cost, and how much does it save?

Your e-discovery providers should be able to advise you on the costs of using TAR. With some providers, TAR technology costs may already be covered by your processing and/or hosting fees. Other providers may follow “a la carte” pricing strategies, where the TAR is charged separately, and only when used, but in any event, TAR technology charges generally should not exceed 2-3 cents per document. Beyond the technology charges, there are generally hourly charges to cover the lawyers and technologists who are assisting and supporting you with using TAR.

4. Do I need permission of the adverse party or the court in order to use TAR?

Case law continues to support the position that you do not need permission from the adverse party or the court in order to use TAR. However, this is limited by anything you may agree to in an ESI agreement or order. Care needs to be taken to ensure that your use of TAR does not conflict with anything you or your counsel may have agreed to, and care needs to be taken to not commit to a course of action via an ESI agreement that will limit your use of TAR—for example, don't agree to negotiate a TAR protocol that will give your adversary veto power over using TAR effectively for your case.

5. Is it acceptable to use TAR after applying search terms to filter the documents?

There is mixed case law on this question, but the majority (and better) view is that search terms **may** be applied prior to TAR. When contemplating the use of TAR, however, you should err on the side of using broader search terms rather than narrower search terms, to minimize the risk of eliminating any significant number of relevant documents before the TAR technology can "fine tune" screening for relevance.

6. What pitfalls do I need to avoid when using TAR?

Avoid moving forward without e-discovery attorneys AND technology experts who understand TAR enough, and have enough experience with TAR, to help you identify and execute the optimal use of TAR in each particular matter. Not all use of TAR is the same—for example, some technology providers may use TAR to prioritize review and/or assist with QC, but may not be in the best position to advise case teams about how to maximize cost and time savings by using TAR in place of some human review.

7. What can I expect in terms of the effectiveness and cost-savings resulting from using TAR?

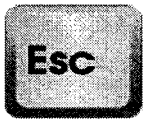
The effectiveness and savings depends on multiple factors, including (i) the "richness" of your starting population (the proportion of documents that are relevant/responsive); (ii) how well the TAR technology can pick up attributes that separate relevant documents vs. irrelevant documents – this can vary by matter and by issue; (iii) whether all documents that are relevant are being reviewed anyway before being produced (e.g. for privilege, issues, hot content, or confidentiality designations or redactions); and (iv) whether you can retain control of the TAR process, and avoid undue interference by adversaries. In cases where the starting population is not very rich (i.e. below 50%), **or** where not all responsive or produced documents need to be reviewed (e.g. the other side's production to you), and you retain control of the process, litigation parties have sometimes achieved time and cost savings of 50% or more—saving some clients $1 million or more in large-scale reviews. Because of the case-by-case variations and uncertainties, however, it is important to manage expectations, and to avoid agreeing to difficult protocols or surrendering control of the process to adverse parties.

8. Any other disadvantages to using TAR?

TAR may not be applicable to the specifics of your project. General lack of experience with managing a TAR project can lead to costly delays or mediocre performance. Discovery disputes around TAR can eat up the cost and time savings that otherwise may be achieved.

9. What steps should I take to explore/start using TAR for my matter?

Seek the advice of experienced discovery counsel and TAR technology experts early in the discovery process to educate you on the various uses of TAR, and the benefits and risks, and to help negotiate appropriate language in case management orders and/or discovery protocols.



Chapter Six

eDiscovery Collection, Processing, and Review

David R. Cohen
Emily J. Dimond[1]

6-1 OVERVIEW

A sound approach to e-discovery must take into account multiple overarching goals, including meeting preservation and production obligations, avoiding spoliation, protecting privileged information, finding evidence helpful or harmful to one's own case, addressing client confidentiality concerns, minimizing the risk of other discovery disputes, and avoiding unnecessary expenses in discovery. For all steps in the process, remember that the Federal Rules of Civil Procedure,[2]

1. David R. Cohen is a partner at Reed Smith LLP, where he leads the Records & E-Discovery (RED) Practice Group, and Emily J. Dimond is an associate with the RED group. They gratefully acknowledge the contributions of Lynn Reilly and Bree Kelly, who co-authored the earlier versions of this chapter.
2. Amendments to the Federal Rules of Civil Procedure that became effective in December 2015 emphasize the concept of proportionality, and contain other revisions designed to help streamline the discovery process. "Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense *and proportional to the needs of the case*, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit." Fed.R.Civ.P. 26(b)(1) (emphasis added).

as well as the Pennsylvania Rules of Civil Procedure[3] and some other states' rules, limit discovery to what is proportional. "Whether preservation or discovery conduct is acceptable in a case depends on what is *reasonable,* and that in turn depends on whether what was done—or not done—was *proportional* to that case and consistent with clearly established applicable standards."[4]

6-2 eDISCOVERY BASICS

Throughout the process, be aware that your preservation and discovery efforts may become the subject of a discovery dispute or collateral "discovery about discovery." Track your efforts in detail, including litigation hold notices, responses, reminders, collections, search terms, and review rules. Many judges expect counsel to be in a position to discuss their client's electronic information systems and preservation and production efforts.

Practice Tip: At the outset of the process, consider identifying and involving a company representative qualified to help oversee the company's efforts, and potentially to attend conferences with the court or among counsel to discuss discovery issues.

Even if you feel that you are well-versed in the rules and case law surrounding e-discovery, it is also important to be familiar with the relevant processes and technology. In fact, Pennsylvania and at least 23 other

3. "As with all other discovery, electronically stored information is governed by a proportionality standard in order that discovery obligations are consistent with the just, speedy and inexpensive determination and resolution of litigation disputes. The proportionality standard requires the court, within the framework of the purpose of discovery of giving each party the opportunity to prepare its case, to consider: (i) the nature and scope of the litigation, including the importance and complexity of the issues and the amounts at stake; (ii) the relevance of electronically stored information and its importance to the court's adjudication in the given case; (iii) the cost, burden, and delay that may be imposed on the parties to deal with electronically stored information; (iv) the ease of producing electronically stored information and whether substantially similar information is available with less burden; and (v) any other factors relevant under the circumstances." Pa.R.C.P. 4009.1, Production of Documents and Things. General Provisions, Editor's Notes—Explanatory Comment—Electronically Stored Information.

4. *Rimkus Consulting Group, Inc. v. Cammarata,* 688 F.Supp.2d 598, 613 (S.D. Tex. 2010). See *First Niagara Risk Mgmt., Inc. v. Folino,* Civil Action No. 16-1779 (E.D. Pa. August 11, 2016) (conducting an analysis of discovery requests under each of the Fed.R.Civ.P. 26(b)(1) factors to determine that they were proportional).

states now consider it an ethical obligation for attorneys to stay abreast of changes in technology relating to law practice.[5] If you do not personally have that knowledge or expertise, consider obtaining assistance from experienced discovery counsel and/or expert consultants. Reasonable, well-documented processes and a demonstrated understanding of your client's electronic information systems can be essential to establishing and maintaining credibility with judges, discovery masters, regulatory officials, or other decision makers.

E-discovery costs can escalate unnecessarily unless attorneys take a proactive and cooperative approach. The federal rules contemplate early conferences between counsel on e-discovery issues,[6] and many questions that could otherwise escalate into disputes may be easily resolved with up-front discussions. For example, even where large volumes of electronically stored information (ESI) technically fall within discovery requests, requesting parties may be amenable to reasonable steps to narrow production and focus on the most likely sources of relevant information—saving themselves burdens and costs as well.

Keep in mind that, in large part, you will get what you give. Be wary of complaining about an opponent's practices when you are vulnerable to counter-charges in the same vein. For example, you should generally be prepared to comply with the same preservation and production requirements you demand from party opponents, so avoid making unreasonable or unduly broad requests that may rebound to you.

The basic steps in any e-discovery project are usually the same: preservation, collection, filtering, processing, review, and production. It is important, however, that you not approach the process with a single template to apply to all cases. Effective cost containment often requires a creative, flexible, or phased approach not only within each case, but also in regard to particular sources or types of ESI.

---

5. Doug Austin, "Less Than Half the States Have a Technology Competence Requirement for Attorneys: eDiscovery Trends," *eDiscovery Daily Blog* (July 29, 2016), available at http://www.ediscovery.co/ediscoverydaily/electronic-discovery/less-than-half-the-states-have-technology-competence-requirements/. In Pennsylvania, "[t]o maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology," Pa.R.P.C. 1.1. See also The State Bar of California Standing Committee on Professional Responsibility and Conduct, *Formal Opinion No. 2015-193* (June 30, 2015), available at http://ethics.calbar.ca.gov/Portals/9/documents/Opinions/CAL%202015-193%20%5B11-0004%5D%20(06-30-15)%20-%20FINAL1.pdf.

6. Fed.R.Civ.P. 26(f).

6-3 PRESERVATION AND COLLECTION

Practice Tip: Give immediate attention to preservation obligations as soon as litigation (or the equivalent) is reasonably anticipated. Storage protocols, automated deletion mechanisms, or individuals' practices may put potentially relevant information in immediate jeopardy of destruction. Allowing spoliation to occur can be an irreparable and costly error. Once effective holds are in place, you have greater flexibility to investigate from whom to collect or whose documents to review, but you must first attend to preservation.

The preservation and collection of ESI raises unique issues and considerations not applicable to hard-copy documents. In particular, ESI requires affirmative steps to be sure that documents are not destroyed or materially altered through routine automatic deletion protocols or inadvertence.

6-3.1 Preservation

As a preliminary step, you must ensure that information potentially to be collected is being properly preserved. Discuss with your client the scope of relevant information and help identify employees to be placed under a "legal hold." Hold notices should be prepared that describe in sufficient detail the relevant subject matter and data to be preserved, as well as instructions for how preservation should be undertaken. You should coordinate distribution and tracking of hold notices, consider obtaining acknowledgments from the recipients, and follow up as necessary to ensure compliance. Immediately at the outset, coordinate with your client's information technology (IT) personnel to be sure that data is not inadvertently lost through, for example, automated deletion protocols or overwriting.

Practice Tip: Where potentially relevant information is not being collected immediately, but will remain in the possession of company employees, discuss mechanisms for continued preservation should a custodian leave the company. Some company IT departments maintain a list of company employees that are on "hold," and may place a notice sticker on the personal computers and/or other devices of those employees subject to holds, so that they can cross-check for holds before any custodian mailboxes, personal com-

puters, or other devices containing potentially relevant ESI are "wiped," deleted, or recycled. Companies may also use legal hold tracking software that can be synched to an HR department's system and provide automated notification about the departure of employees who are on legal hold.

Throughout the process of preservation and collection, be sure internal messages come from a person with sufficient authority to credibly convey the importance of compliance. Have template hold notices ready to tailor and distribute, issue notices promptly when litigation is anticipated, issue periodic hold reminders as appropriate, and track the preservation measures put in place and your client's compliance with them.

6-3.2 Identify Sources

Finding sources of data to be collected means considering both individual employees who may have relevant information and other locations where relevant information is stored. Consider employees' local drives and portable storage, as well as central storage locations such as file servers, e-mail servers, websites, document management systems, SharePoint, cloud storage locations, backup media, and databases. Confer with your client, key custodians, and your client's IT personnel to help ensure that no relevant sources are overlooked. Learn about your client's computer systems, including the hardware and software used, how files are saved, what e-mail system is used, and what backup protocols are in place, if any.

Effective communication with your client's IT personnel is critical to properly identify sources and plan collections. Courts have imposed sanctions, not only for intentional spoliation of evidence, but also when inadequate communication and coordination resulted in the loss or late production of relevant information.[7]

6-3.3 Identify Custodians

Determine the custodians whose data should be preserved and collected for processing and review. While you should err on the side of inclusion when issuing litigation hold notices, at the collection step, consider options for reasonably narrowing the scope. The number of custodians whose data is collected and reviewed is a key cost driver. As long as you have implemented effective preservation measures and are reminding people of that obligation, you may not need to collect at the outset from every per-

7. See, e.g., *In re Delta/Airtran Baggage Fee Antitrust Litig.*, Civil Action No. 1:09-md-2089-TCB (N.D. Ga. August 3, 2015).

son subject to the legal hold. It is often reasonable to start with a narrower set of custodians most likely to have relevant information and to negotiate with the requesting party a narrowed or phased collection process focusing on the key custodians first.

Ask whether particular employees, such as supervisors or secretaries, may have documents likely to be merely duplicative of those maintained by key custodians. Consider surveying potential custodians to determine whether collection is necessary and to identify any centralized sources, such as department-level file server locations or databases, or cloud-based data, that might obviate the need for some individual collections.

One important consideration in any preservation or collection effort is whether new ESI is likely to be generated that will require supplementary collection. Many cases address circumstances in which the relevant time frame is historical; that is, where no new relevant documents are likely to be generated or received after initial collection efforts ("historical discovery" cases). However, if you are in a situation where new discoverable information may be generated or received ("ongoing discovery" or "evergreen discovery" cases), it is important to segregate previously collected documents and ESI from new material. Tracking of initial collections can help to avoid duplication when performing later supplemental collections.

Even for historical discovery cases, however, it is periodically necessary to consider supplemental discovery steps. For example, new issues may arise, new custodians may be identified, or the allowable scope of discovery may be expanded by agreement or by court order. At a minimum, you should consider the potential impact on your prior efforts whenever you receive new or amended pleadings or new discovery requests.

6-3.4 Collection Interviews

During individual custodian collections, conduct interviews of custodians with these goals in mind:

1. finding all locations where the custodian may have stored relevant information;
2. limiting the scope of collection to where relevant or responsive materials are reasonably likely to exist;
3. identifying any other custodians or document sources that should be added to the list; and
4. gathering background information to inform document review and further case preparations.

Interview topics may include, for example, the custodian's relationship to the relevant subject matter, any electronic repositories or date ranges that can appropriately be eliminated from collection, interaction the custodian may have had with attorneys, any sensitive or highly confidential content, and any relevant acronyms, aliases, initials, or e-mail groups that might appear in potentially relevant records.

Remember that some courts have held that counsel has a duty not only to send litigation hold notices, but also to follow up with key custodians to ensure compliance.[8] In addition to sending written reminders, use custodian interviews to reconfirm that each custodian has identified and taken appropriate steps to preserve all potentially responsive documents and ESI, and will continue to preserve potentially discoverable information that is not being collected initially.

6-3.5 Planning

Practice Tip: Consider the various methods for collection to determine a strategy that ensures legal compliance while minimizing costs. Some circumstances may be appropriate for guided custodian self-collection, while others may require more third-party investment and involvement to ensure that all potentially responsive data is properly captured, to meet court expectations, or to provide third-party verification of the efforts undertaken.

There are different methods and approaches to collections, and you should aim to determine the most effective approach to collecting ESI from each source. A number of factors affect how collections should be conducted and by whom.

Usually search terms, date ranges, de-duplication, e-mail threading and/or other analytics (including predictive coding) can be used to filter initial collections down to a subset requiring review for responsiveness and/or privilege. In planning the filtering, a fundamental question is what filtering can be done in-house, and what should be delegated to law firms or e-discovery vendors. Iterative searching and narrowing can be powerful tools for reducing volumes, so select a provider that can perform multiple

8. *Zubulake v. UBS Warburg LLC,* 229 F.R.D. 422, 431–34 (S.D.N.Y. 2004); see also *Browder v. City of Albuquerque,* No. CIV 13-0599 RB/KBM (D.N.M. May 9, 2016) (citing *Zubulake,* 229 F.R.D. at 432, 436).

iterations of the search terms, with "hit-by-term" reports and sampling to refine searches so that potentially relevant documents will be captured and irrelevant documents will be excluded to the extent practical.

Other considerations include impositions on client resources, disruption of client's operations, and, in some cases, the potential need for later forensic testimony in regard to collection steps and methods. In conducting individual collections, remember to balance the need to refine collection volume against the imposition on custodians' work time. Some collections—for example, from Exchange servers or user directories—may best be accomplished by client IT administrators, if resources permit. Taking into account the sophistication and resources of the client's IT group, consider whether it is appropriate to outsource collections to discovery counsel or a vendor. Also, where you may later need to provide witness testimony to support collection steps and methods, or where recovery or preservation of ESI requires advanced forensic methods, it can behoove you to enlist the help of outside e-discovery specialists rather than relying solely on in-house resources.

6-3.6 Collection Methods

Collection methods may include taking full collections from custodian-specific storage repositories, targeting collection of centrally stored information, and assisting custodians in self-selecting relevant information. Whatever the collection method, ensure that procedures are forensically sound and do not inadvertently alter potentially relevant electronic documents or their metadata. Recall, too, the overarching considerations of reasonableness and proportionality when making a decision regarding which collection method is best suited to the circumstances of each case.

6-3.6.1 Forensic Versus Active Data Collections

A threshold question is the type of data you need. In the majority of cases, collection of active data will suffice. Active data generally means currently available ESI, including e-mail, text files, spreadsheets, presentations, and databases. This type of ESI is typically stored on hard drives, servers, cloud repositories, or other source locations in a way that keeps it readily accessible for day-to-day use. Its collection is usually straightforward and less expensive than collection of inactive data.

Under certain circumstances, you may need to consider additional measures beyond the collection of active data. A forensic collection can capture all data stored on a physical hard drive, including data that has been deleted or is otherwise not readily available to the average user. In most cases, capture of such data is not necessary. The main reason to consider the additional step of forensic copying is the need to capture deleted information. In typical commercial disputes, there is no reason to believe that

employees, properly instructed, will fail to comply with litigation hold obligations. Forensic copying may be appropriate if, however, there is reason to believe one or more employee(s) may have deleted relevant information, or a judge or discovery master expects you to search for deleted data. This process should be accomplished with the help of qualified forensic experts.

6-3.6.2 Full versus Targeted Collections

Another decision you have to make is whether to engage in full or targeted collections for each identified custodian, and when you can rely on employees to play a significant role in self-collection. Each approach presents costs and benefits, as outlined in more detail below.

6-3.6.2.1 Full Collections

In collecting from custodians' individual storage repositories, it is sometimes most efficient to start by collecting all active files. In full collections of hard drives, for example, files are collected from each custodian's local drive by file type, meaning that essentially all active document and data files are collected. (Program and system files, such as the operating system and computer programs running on a PC, are almost never relevant or responsive so typically need not be collected.)

A full collection reduces the risk that relevant evidence will be inadvertently missed: all relevant custodians' documents are captured with the collection. This approach also involves the least imposition on the custodians' time. Brief custodian interviews provide helpful background to frame review of a custodian's documents or limit date ranges, for example, but the time required is essentially only as long as it takes to run a collection script (often half an hour or less per user). If the scope of the relevant subject matter later changes, but the collection was comprehensive, repeat collections are not needed.

The disadvantage of a full collection is simple: with more volume, more material is processed, and potentially more must be reviewed for relevance. With a full collection, it is especially important to use reasonable search terms and/or predictive coding technology to limit the volume requiring human review prior to production. Even if you opt for full collections of custodians' local drives, collecting from file servers or cloud storage locations typically calls for a different approach. Server folders are often much too large to be collected and searched effectively, and there may be technological limitations to how you can search information stored in cloud locations, and how rapidly that information can be retrieved. From server or cloud locations, ask custodians to identify folders in which relevant documents might be found.

6-3.6.2.2 Targeted Collections

In targeted collections, each custodian specifically identifies potentially relevant files or folders to be collected and reviewed. If appropriate, rather than copying all active data from each custodian's drive or cloud storage location and reducing later with search terms, ask custodians to point out individual relevant folders or files for collection. Remind custodians of possible sources of relevant data they may not have considered and ask whether files can be segregated by subject, date range, or otherwise, or whether there are clearly irrelevant materials that can be eliminated. The benefit of this type of collection is reduction of the raw volume collected. This process can take more custodian time than full collections because of the need for more detailed custodian interviews, but engaging in a more targeted collection can be a time-saving and cost-saving measure in the long run. The actual collection of materials, as with full collections, is often accomplished through the use of an external drive or FTP site to capture the identified materials without risk of altering metadata.

The risk of a targeted collection strategy is that relevant information will be missed: for example, a custodian may have incorrectly stored documents or simply may not remember the locations of all potentially relevant documents. Since the custodian's full data set has not been collected, a risk of loss of evidence remains.

In any scenario other than a full collection, you must be aware of the limitations of running search terms against the source media. For example, running word searches in Outlook typically will search only e-mails and not attachments—meaning that a relevant document attached to a transmittal e-mail will not be captured unless a search term appears in the parent e-mail. With targeted or self-selected collections, it is critical that you use sound methods and even more detailed custodian interviews to avoid missing potentially relevant information.

6-3.6.2.3 Self-Selection

The least expensive way to accomplish collections is often simply to request that custodians identify and collect relevant materials from their own files. While this approach can be most cost-effective, it is not without risk.

For example, there is a risk that the method of collection will alter document metadata. Typically, parties accomplish self-selection collections by instructing custodians to copy their relevant files to a shared location or external drive. This runs the risk of altering certain metadata fields; before proceeding, counsel should evaluate whether that is likely to be an issue in a particular case. Another vulnerability in this process is that custodians may not understand the scope of what they should collect. Clear and detailed instructions are critical to successful self-selected collections. Finally,

self-selection is not the best option where there are reasons not to trust the custodians, or where opposing parties or a court reasonably may question the sufficiency of this approach. For example, where an employee is accused of fraud, sexual harassment, or other conduct that could lead to personal liability or significant professional embarrassment, have more objective third parties drive the collection process. It should be noted that self-selection has been subject to criticism in some circumstances. In *Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities, LLC,* for example, the court found fault in counsel's "total reliance" on employees to identify responsive records without supervision.[9] The court acknowledged, though, that "not every employee will require hands-on supervision from an attorney" and that the adequacy of each search must be evaluated on a case-by-case basis.[10]

6-3.6.2.4 Collecting from Central/Non-custodial Sources

It is important to remember that there may be relevant/responsive documents beyond those in the possession of individual custodians. For example, marketing materials, financial statements, and board meeting minutes are likely to be stored together and can most efficiently be collected *en masse* when feasible, rather than reviewing each custodian's individual collection for such documents where they may incidentally appear.

6-3.7 Tracking

Whatever method is used to collect and whoever is in charge of collection efforts, track the procedures used and data collected: what was collected, how, from whom, and when? Track volume and type of information, sources and file paths, etc. Keep copies of questionnaire responses and interview summaries. Record how determinations were made to collect from some recipients of hold notices and not others. This information is useful not only to the specific case for which documents were collected, but sometimes also for future cases if the client elects to maintain a library of collected material.

6-4 CULLING FOR REVIEW

Once you have collected raw data from client sources, culling material prior to attorney review is a critical time- and cost-saving step. Three key means of doing so are through date ranges, search terms, and duplicate suppression.

---

9. *Pension Committee of Univ. of Montreal Pension Plan v. Banc of America Secs., LLC,* 685 F.Supp.2d 456, 473 (S.D.N.Y. 2010).
10. Id. at 473, n.68. See also *Burd v. Ford Motor Co.*, Case No. 3:13-cv-20976 (S.D. W. Va. July 8, 2015) (granting plaintiff's motion for Rule 30(b)(6) witness testimony regarding defendant's search and collection methods, including custodians' "self-selection" of relevant documents).

6-4.1 Establish Case and Custodian Date Ranges

If you have not already excluded date-irrelevant documents at the collection stage, you should do so at the processing stage. Different ranges may be appropriate for different custodians. For example, if a long-term employee only recently joined a relevant work group, you might limit your search of that employee's files to the period during which he or she may have created or received relevant communications. Frequently, requests for production of documents specify beginning and ending dates of the overall responsive time frame. Where they do not, or where the period is not reasonably limited, you should negotiate this with opposing counsel, set date limits in discovery responses, and/or seek relief from the court.

6-4.2 Create and Test Search Terms

Practice Tip: Even under deadline pressure, time invested up front to test search terms or identify anomalies in the collected data will pay off in reduced costs and reduced errors in review and production. Maximize the use of automated tools to filter ESI and minimize more time-consuming and expensive attorney review.

Courts have approved the use of search terms as a method to cull relevant material from a larger universe of documents and control the volume of material to be reviewed. In identifying search terms, be sure to consult the law firm, vendor, and/or IT personnel executing the search about how the terms will function. For example, how a search tool handles punctuation, spaces, "stop words," proximity searches, or "wild card" characters can significantly affect results. It is important to confer with those who understand the search tool to be sure that the terms will function as intended.

Seek expert assistance as appropriate. It has been noted that the creation and implementation of search terms involves "technical, if not scientific knowledge" beyond that of most attorneys and may require input from more qualified persons.[11]

Consultation with opposing counsel is strongly encouraged. Good-faith cooperation to identify agreed-upon search terms may serve to prevent later challenges. Additionally, most courts are reluctant to second-guess agreements between the parties.

11. *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 250 F.R.D. 251, 260 (D. Md. 2008).

Because case- and source-specific search terms are so important to cost containment, you should test, analyze, and revise search terms through multiple iterations to reach a defensible set of terms that also yields a manageable volume for attorney review. Analyze sample data, evaluate how the search terms are functioning, and modify terms that are over-capturing irrelevant information or under-capturing potentially relevant information. This ultimately redounds to the benefit of all parties.

6-4.3 Suppress Duplicate Documents Prior to Review

Apart from reduction with date ranges and search terms, pre-review processing should include duplicate suppression wherever feasible. Through "deduping" processes, available technology can suppress both exact duplicates and lesser-included e-mail threads. This step helps to ensure that, whether or not duplicate documents are eventually produced, they need not be reviewed more than once.

When using duplicate suppression technology, consider whether your software or provider has the capability to dedupe both within an individual custodian's documents and across all custodians' documents. Also, it is helpful for the software or provider to track suppressed versions and produce a log if necessary. Discuss with opposing counsel whether there is any objection to suppressed duplicates being excluded from production—this step can save both sides time and money in review and production.

Be careful not to dedupe across custodians until you determine which custodians' materials will be produced. Otherwise, documents that are required to be produced could inadvertently be suppressed.

6-4.4 Format for Review

Preparing ESI for attorney review often includes conversion from its native format into an image format, such as Tagged Image File Format (TIFF). However, many popular review software packages support review of ESI in its native format. In determining whether to have ESI converted to TIFF format before review, consider the following factors:

1. Does the review software handle native format, TIFF format, or both? If both, does review move faster in one or the other format?
2. Is the ESI (or most of it) ultimately to be produced in TIFF format?
3. Are greater cost and time savings likely to be achieved by TIFFing during initial processing (so the data never has to be re-processed before production), or by TIFFing only those documents identified as responsive after the review has occurred?

6-5 REVIEWS: IDENTIFYING RESPONSIVE AND PRIVILEGED DOCUMENTS

Filtering documents through word searches, date limitations, and other such steps can help to narrow the universe of potentially responsive or privileged documents, but a document-by-document review, undertaken by attorneys or with predictive coding technology, is usually necessary to confirm which records are relevant or responsive, which are "hot," and which qualify for privilege or work-product protection. Attorney review of large quantities of ESI can be time-consuming and expensive, so it is important to narrow the universe as much as reasonably possible before the review is undertaken and then use technology and streamlined processes to optimize the review.

Using best practices in review means meeting your production obligations while properly protecting your client's information and controlling litigation expenses. Best review practices should consider three factors: the people, the technology, and the process.

6-5.1 People

In some cases, the most efficient approach is simply to have the trial team conduct document review. If the volume of records is small and the litigators are already familiar with particularly complex or technical subject matter, the cost of outsourcing and training other lawyers to do document review may outweigh the benefit of lower billing rates.

In most cases with high document volume, however, you should explore options less costly than having high-priced law firm associates or partners reviewing the entire universe of records that have made it through the filtering process. In addition to the cost, experience suggests that law firm partners and associates are often not particularly good at performing large-scale document reviews. Most of them do not have much interest in the work, or much expertise using the technology tools that are available to optimize the process. Frequently, their time is divided between document review and other projects, which can slow down a review and hurt the quality of the result.

Accordingly, for both cost and quality reasons, it is usually wiser to use lower-cost attorneys who have more experience with reviews, and greater facility with review tools. Consider having first-level review work performed by experienced e-discovery attorneys who focus on this work and have much lower billing rates. Alternatively, where an adequate training and supervisory structure is in place, using temporary or contract attorneys can be an effective solution to culling nonresponsive material at reduced rates. With some collections of documents, it can even be worthwhile to have some or all of the filtered records reviewed by paralegals, clerks, or foreign lawyers to

save time and costs. However, be sure to consider the ethical implications and your supervisory and quality control obligations before relying on anyone other than U.S.-licensed law firms or in-house attorneys to make legal judgments or render legal advice.[12]

No matter who is conducting the review, merits counsel should provide detailed guidelines and case background and work closely with the review team throughout the process to ensure the quality of the result. Exporting early review results for trial team feedback can be a worthwhile step to ensure that review guidelines are being communicated effectively and the process is proceeding as intended.

6-5.2 Technology

Practice Tip: E-discovery technology is constantly evolving. To provide superior service to your client, it is critical that you employ the most effective options, including review software that filters nonresponsive information, eliminates duplicative reviews, and maximizes review speed and accuracy.

Using specialized review software can both accelerate and improve the quality of the review process. Virtually all of the available litigation review software can add value over hard-copy review by allowing searching, sorting by date, etc. But a critical jump in review efficiency comes with the use of concept-analyzing software. The various packages now available perform what is known as predictive coding, computer-assisted review (CAR), or technology-assisted review (TAR). This technology is covered in chapter 12 of this book. Although such systems have yet to achieve universal acceptance by all courts, they are gaining ground.[13]

12. See the District of Columbia Bar Ethics Opinion No. 362, "Non-lawyer Ownership of Discovery Service Vendors" (June 2012), stating that "the lawyer seeking to retain a discovery services organization should satisfy herself that the organization will not be engaged in the practice of law with respect to the matter for which the lawyer seeks to hire the organization." Available at https://www.dcbar.org/bar-resources/legal-ethics/opinions/opinion362.cfm.

13. See *Rio Tinto PLC v. Vale S.A.*, 306 F.R.D. 125, 127, 129 (S.D.N.Y. 2015) ("the case law has developed to the point that it is now black letter law that where the producing party wants to utilize TAR for document review, courts will permit it"); *In re Biomet M2a Magnum Hip Implant Products Liab. Litig.*, Cause No. 3:12-MD-2391 (N.D. Ind. April 18, 2013); *Da Silva Moore v. Publicis Groupe*, 287 F.R.D. 182 (S.D.N.Y. 2012); and *Global Aerospace, Inc. v. Landow Aviation, L.P.*, Consolidated Case No. CL 61040 (Cir. Ct. Loudon County, Va. April 23, 2012).

Even short of trying to replace human review with predictive coding, TAR software and other review software may allow like documents to be grouped together to optimize reviewer comprehension, speed, and accuracy. Decisions about review technology can be intertwined with decisions about who will perform the review. If your company or law firm is conducting the review in-house, do you have the necessary infrastructure to use the best tools? In addition to licensing the software, you also need to have, or acquire, the server space required to run the applications and host collected and produced data, sufficient work stations where the review can be conducted (preferably with two monitors per reviewer to maximize the efficient use of review software), training for review personnel, and the necessary technical personnel to support hosting, review, and production. It may not be realistic to expect a company's or law firm's existing IT resources to support this infrastructure without adding support personnel as well as the necessary hardware and software. This is one reason to consider retaining an e-discovery provider or a law firm that already hosts large-scale review operations using advanced review software.

6-5.3 Process

Because attorney review usually constitutes the largest portion of e-discovery costs, you need to strategize to maximize the value you gain from this review. A common mistake is wasting attorney review time looking for types of information that can be captured electronically using combinations of metadata fields, search terms, and file types. For example, you do not need attorney review to capture all e-mails sent by Person A within a particular time period, to find all boilerplate customer contracts, to locate all financial spreadsheets, or to eliminate duplicate documents. A key benefit of electronic documents is the minimal time and work involved in capturing objective information about the data set. Accordingly, you should budget attorney time for determining or confirming responsiveness and privilege, identifying documents that are "hot" or particularly related to key issues in the case, training predictive coding software, or in some cases identifying proprietary documents or levels of confidentiality (such as nonconfidential, confidential, and "attorneys' eyes only"). If you are unfamiliar with what information can be extracted electronically, consult with e-discovery experts to be sure you are not wasting your most costly resource on work that can be done more cheaply and accurately through automated means.

Before commencing a human review, consider the review plan or structure that is best for your project. In a review that is relatively straightforward and/or where you have a high level of trust in the attorneys performing the review, it can be most cost-effective to do a single-pass review for responsiveness, protective order designation, hot documents, and privilege, with quality control audits only on a sampling basis. Where the review is more complicated or the primary reviewers are temporary or contract attorneys,

a second pass through the relevant or potentially privileged records by a smaller group of specially trained reviewers or trial team members may lead to better results. With regard to documents where only some portions are subject to attorney/client privilege or work product protection, you need to consider how and when to redact the protected information.

However you choose to conduct review, you should have quality control and quality assurance measures in place. These measures should include, at a minimum, sufficient training on each case, and frequent review team meetings and updates on any changes or clarifications to review guidelines. Other quality measures should include quality control review or sampling and/or a final review of each production by experienced personnel as a check against inadvertent production of privileged material.

The reasonableness of the chosen review process may have broad implications in the event of inadvertent production of privileged material. Under Federal Rule of Evidence 502, inadvertent production does not necessarily result in the waiver of privilege. Rather, pursuant to F.R.E. 502(b), inadvertent production of privileged material in a federal proceeding does not operate as a waiver (in federal or state court) if: "(1) the disclosure is inadvertent; (2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and (3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26(b)(5)(B)." Accordingly, great care is warranted in the planning stages of any review to ensure the chosen process can be defended as reasonable in the event of inadvertent disclosure. Rule 502(e) non-waiver orders can provide additional protection as discussed below.

Do not underestimate the importance of choosing an appropriate review process. If you have not managed a large-scale review operation before, do not try to undertake one without the assistance of counsel and/or consultants who have prior experience managing large-scale reviews.

6-5.4 Is Production Without Review a Viable Option?

In some cases, it is a viable option to simply run search terms and produce the search hits without further review for responsiveness. If the stakes in the litigation simply do not justify any review expense or the budget is very limited, this option is certainly the least expensive means of effecting document discovery.

The risks of this approach, however, go beyond simply producing non-responsive documents. Employees' e-mail will often hold surprises, including personal information, unflattering remarks about co-workers, or worse. Records that are not responsive, yet were unnecessarily produced, have the potential to expose embarrassing information or even open up new claims or lines of attack against the producing party.

Production of documents without human review also significantly increases the risk of inadvertently producing privileged documents. While that risk can be reduced by reviewing documents caught by predictive coding software and/or by screening with privilege search terms (for example, names of known attorneys and words like "lawyer," "attorney," "law," "legal," "counsel," "esq.," "privilege," etc.), such terms will not capture all documents subject to privilege or work-product protection, and such techniques should be accompanied by nonwaiver orders, sampling, and testing to reduce waiver risks. While obtaining nonwaiver agreements and orders in advance provides some additional protection, there is no way to force opposing counsel to forget what they learn from privileged documents. Nonetheless, it is wise to take advantage of any protections that are available, particularly where disclosure of privilege in one case can risk waiver in other situations.

If you are planning to produce search hits without human attorney review, seek agreement with opposing counsel that disclosure of privileged information will not result in waiver and that produced privileged documents will be returned. Then, incorporate that agreement into a court order. Pursuant to F.R.E. 502(e), without such an order, the agreement is only binding on the parties. Where agreement cannot be reached, consider moving for such an order nonetheless, because agreement between the parties is not required under the rule.[14] Even where search hits will be reviewed prior to production, such an order provides an additional safeguard against waiver and should be considered in virtually every case.

The bottom line is that careful consideration is always required when choosing the most appropriate review process. Do not be "penny-wise and pound-foolish" by trying to save some money on initial human review and/or predictive coding if that unacceptably increases downstream risks and exposure.

6-6 PREPARING FOR PRODUCTION

Practice Tip: Engage early with opposing counsel to develop agreed protocols for production of potentially relevant records. It will be more efficient to clarify all requirements up front than to have to redo collections or a production later because you failed to preserve metadata fields or produced documents with the wrong technical specifications. E-discovery

14. See, e.g., *Great-West Life & Annuity Ins. Co. v. American Economy Ins. Co.*, Case No. 2:11-cv-02082-APG-CWH (D. Nev. September 23, 2013); *Rajala v. McGuire Woods, LLP*, Civil Action No. 08-2638-CM-DJW (D. Kan. July 22, 2010).

is one area of practice where you should seek a cooperative rather than adversarial relationship with opposing counsel, as cooperation will usually redound to the benefit of all parties.

Once review is completed, nonprivileged responsive documents must be prepared for production. Ideally, parties will agree on production formats and logistics. Parties can save both time and money where they can reach agreement on issues such as whether records will be produced in native or imaged format, how electronic documents will be numbered, what, if any, metadata or source information will be produced, nonwaiver of privilege, protection of confidential information, load format if parties are using specific review databases, and sharing the cost and results of optical character recognition (OCR) or coding with regard to hard-copy records.

These decisions have important ramifications for the cost and burden of discovery. For example, while production in native format avoids imaging costs and thus may be the least expensive approach in terms of processing charges, dealing with native files presents other issues. Native files can easily be altered (inadvertently as well as intentionally), and numbering and other "branding" presents challenges.

For these reasons, parties commonly agree to a standard image format like Tagged Image File Format (TIFF), notwithstanding the additional expense of converting responsive documents. If your client is asked to produce in more than one format or otherwise to provide more tools or information than applicable rules require, consider seeking equitable cost-sharing with the requesting party.

Practice Tip: It can be expensive to TIFF voluminous spreadsheets, and TIFF images of spreadsheets are rarely very useful for opposing party review. Consider other options for the production of voluminous spreadsheets, such as more selective production and producing truly relevant data in a native format while employing other measures for numbering and control.

A common misconception is that parties must choose between documents produced in native format and non-searchable images without any metadata. In fact, parties can agree to productions that include images (for example, TIFFs or PDFs) with accompanying text files that make the images searchable, along with database load files containing extracted metadata

fields (to, from, author, date, etc.). This approach provides the functionality of native documents but with the added control and protection that imaging and page-level numbering can provide.

Practice Tip: Prior to production, spot-check TIFF images to ensure that documents were imaged in the correct view (for example, with speaker notes showing in PowerPoint documents, or without tracked changes visible in Word documents), to ensure that images are legible and properly endorsed, and as an added check against the production of privileged information.

Some documents contain embedded metadata that is hidden from immediate view, but is easily accessed in the native document. Common examples include hidden or filtered rows or columns in a spreadsheet, formulas used for calculations within spreadsheets, tracked edits in text documents, and comments inserted in text documents or spreadsheets. This information would not be visible on the documents if printed in usual formats, and the need for production of such "hidden" information in electronic format may vary by case. If, however, such data is relevant to issues in the case or necessary to make the document usable, access to native format documents may be warranted. Typically, these issues can be resolved by an agreement or order requiring production of native documents in appropriate circumstances.

6-6.1 Privilege Logs

In large document productions, one of the most time-consuming and expensive, but often least useful, steps can be the preparation and production of privilege logs. With electronic documents, take full advantage of the availability of metadata to pre-populate fields such as document number range, date, "from," "to," etc. Consider having reviewers select privilege codes (for example, specifying the nature and type of privilege) and privilege log descriptions for responsive but privileged documents when documents are first reviewed to avoid subsequent re-review and coding of every privileged document. This can allow generation of an automated draft privilege log that may only require review and editing before production to opposing counsel.

Practice Tip: Agree with opposing counsel that any privileged or work product documents created after the case was filed, such as each party's litigation correspondence with counsel, need not be logged. In cases with large volumes of privileged documents, further negotiate with opposing counsel or obtain court approval for alternatives to full logging of every privileged document. For example, the parties can agree to group logging of privileged documents by category, or to purely automated logs in the first instance, containing the information readily available from metadata. The parties can agree in advance or the court can order that each party may then be allowed to select a sample of the other side's logged documents (for example, 5 percent) for more detailed logging. If that exercise establishes that the privilege determinations were appropriate as to the selected sample, no further detailed logging should be required in regard to the other documents listed on the automated logs.

6-7 TEN KEYS TO SUCCESS

There is no "one size fits all" solution for handling ESI in litigation, but following these key guidelines can reduce risks and avoid many common pitfalls.

1. Give immediate attention to preservation of all potentially relevant records as soon as litigation (or its equivalent) is filed or reasonably anticipated.
2. Follow up with all recipients of legal hold notices to help ensure that they are taking appropriate steps to collect and preserve relevant records.
3. Bring technical expertise to bear on the identification and collection of responsive ESI, including IT personnel, knowledgeable inside and outside counsel, and/or e-discovery consultants.
4. Consider the various collection and review alternatives to determine a strategy that ensures legal compliance while minimizing costs.
5. Engage in early and frequent communications with opposing counsel to attempt to develop agreed protocols for collection, filtering, and production of potentially relevant records.

6. Plan and test to maximize the use of automated tools to filter ESI and minimize the number of records that require more time-consuming and expensive attorney review.
7. Use review software that can eliminate duplicative reviews, limit human review, and maximize review speed and accuracy.
8. Take adequate steps to protect, redact, and log privileged, work product, or proprietary records.
9. Establish credibility with courts, agencies, and opposing counsel by being proactive and diligent in e-discovery compliance, being realistic about the time and effort required to meet e-discovery obligations, and devoting sufficient attention to e-discovery issues at each step along the way. Avoid committing to any tight schedule to "complete production" before you know the document volume and can plan all logistics, and even then build in contingencies to resolve the inevitable snafus or newly discovered records.
10. Employ quality control procedures designed to ensure quality and consistency in all work that is performed, from record preservation and collection through filtering, review, processing, and production. This starts with using well-trained personnel following established procedures, employing adequate supervision, and performing final quality control checks on all produced and withheld document populations. And be sure to document your efforts.

Collecting and processing ESI is more complicated and challenging than many people realize, but through careful planning, adequate attention, and pursuing a sensible approach, parties can achieve optimal outcomes while minimizing the costs incurred in the process.

Cross-Border Discovery Under the GDPR

by David R. Cohen, Reed Smith LLP and Erica Yen, KARL STORZ Endoscopy-America, Inc.

Maintained • USA (National/Federal)

A Practice Note highlighting key considerations and challenges for organizations and their counsel involved in cross-border discovery under the EU General Data Protection Regulation (GDPR), including the tension between the broad scope of the GDPR and the broad scope of US discovery, the GDPR requirements that impact US investigations and litigations, and best practices for navigating cross-border discovery.

The EU General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) governs the processing of individuals' personal data in the European Union (EU). The GDPR was incorporated into the European Economic Area (EEA) Agreement by the EEA Joint Committee, extending application of the GDPR to Iceland, Norway, and Liechtenstein.

The GDPR represents a codified version of the fundamental right to privacy in the EU, which differs significantly from the way US law protects personal data. The GDPR includes several provisions that:

- Protect the rights of individuals in the EU (referred to as data subjects).
- Authorize severe consequences for noncompliance.

GDPR violators are subject to penalties of up to the larger of EUR20 million or 4% of an organization's annual global gross revenue. While maximum fines may rarely be imposed, a penalty of even a fraction of the highest potential amount could have a crippling impact on many organizations.

Any organization that operates in the EU or has EU employees, customers, or clients must protect personal data and comply with the GDPR. However, these efforts may sometimes conflict with US discovery demands. A litigant may face sanctions for either violating the GDPR or failing to fulfill its US discovery obligations. To minimize risk, organizations and their counsel should:

- Understand the tension between the broad scope of the GDPR and the broad scope of US discovery (see GDPR Compliance Versus US Discovery Obligations).
- Review the GDPR requirements impacting US investigations and litigations (see Key GDPR Requirements).
- Implement best practices for navigating cross-border discovery (see Best Practices for Cross-Border Discovery).

GDPR Compliance Versus US Discovery Obligations

The GDPR has a broad territorial reach. It applies to organizations acting as data controllers or data processors that are either:

- Established in the EU.
- Established in a jurisdiction where EU member state law applies through public international law.
- Not established in the EU but either:
    - offer goods or services to data subjects in the EU; or
    - monitor the behavior of data subjects that takes place in the EU.

(GDPR, Article 3.)

The GDPR imposes restrictions on processing, transferring, and retaining personal data, and broadly defines both "personal data" and "processing." Personal data includes "any information relating to an identified or identifiable natural person" (GDPR, Article 4(1)). This definition reflects a significantly broader concept of personal data or personally identifiable information than what is recognized in the US. Any data point that allows a person to be identified (such as an individual's name, an email address, or even a job title and employer's name) constitutes personal data under the GDPR.

The term "processing" includes "any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available … erasure or destruction" (GDPR, Article 4(2)).

Information exchanges in US investigations and litigations typically entail the preservation, collection, filtering, review, and production of voluminous quantities of data, much of which includes processing personal data under the GDPR definition. The frequency and amount of disclosure commonly required in US dispute resolution is unfamiliar to most EU privacy officials given that, outside of the UK, the dispute resolution systems in EU jurisdictions contemplate little (if any) party-driven discovery. Moreover, EU countries tend to give much greater weight to personal privacy because it is a fundamental right in the EU (see Charter of Fundamental Rights of the European Union, Title II, Article 8).

However, US courts often afford little deference to non-US privacy laws when parties object to cross-border discovery. The most pertinent guidance from the US Supreme Court came more than 30 years ago in *Société Nationale Industrielle Aérospatiale v. United States Dist. Court for the S. Dist. of Iowa* (482 U.S. 522 (1987)). In that case, the Court set out factors for lower courts to apply when addressing a request for discovery that implicates foreign law (482 U.S. at 546 & n.30). Most courts applying those factors have held that the US discovery interests outweighed the EU privacy interests (see, for example, *Giorgi Glob. Holdings, Inc. v. Smulski*, 2020 WL 2571177 (E.D. Pa. May 21, 2020); *Knight Capital Partners Corp. v. Henkel Ag & Co., KGaA*, 290 F. Supp. 3d 681, 687 (E.D. Mich. 2017)). Accordingly, it is challenging for organizations with an international reach to comply with US discovery obligations without violating the GDPR.

For more information on typical conflicts that can arise between US discovery laws and non-US data protection laws that limit the collection, processing, and cross-border transfer of personal information, see Practice Note, Conflicts Between US Discovery and Non-US Data Protection Laws.

Key GDPR Requirements

To comply with the GDPR when confronted with US discovery obligations, counsel must understand the GDPR requirements that address how an organization:

- Processes personal data (see Processing Personal Data).
- Transfers personal data (see Transferring Personal Data).
- Retains personal data (see Retaining Personal Data).

Because GDPR compliance is complicated, counsel should consider consulting with knowledgeable local counsel before processing, transferring, or retaining any personal data for a US dispute.

Processing Personal Data

The GDPR restricts the processing of personal data by an organization in several ways. First, an organization must have a lawful basis for processing the data. The most likely lawful bases for processing personal data for US dispute resolution include where either:

- The data subject consents to the processing of her personal data for one or more specific purposes (see Consent).
- Processing the personal data is necessary to:
    - comply with a data controller's legal obligation under EU state law; or
    - serve a data controller's or a third party's legitimate interests, except where a data subject's fundamental rights and freedoms requiring the protection of her personal data override those legitimate interests.

    (See Legitimate Interests.)

(GDPR, Article 6(1)(a)-(f).)

Consent

US counsel seeking personal data for a US dispute may try to obtain a data subject's consent to process data for discovery. Consent under the GDPR is a high threshold to meet and maintain, so it is usually not prudent to rely on that basis.

Valid consent must be:

- **Demonstrable.** A data controller bears the burden of proving that it obtained the data subject's consent to process her personal data, typically through a written statement, a ticked box, or a verbal representation (GDPR, Recital 32 ("Silence, pre-ticked boxes or inactivity should not … constitute consent.")). A data controller's request for consent must be clearly distinguishable from other matters addressed in the request and must be conveyed in clear, plain language.

- **Revocable.** A data subject may freely withdraw consent (GDPR, Article 7(3) ("It shall be as easy to withdraw as to give consent.")). Obtaining revocable consent may be impractical in US disputes because a data controller typically loses control of data once it is produced to another party. However, the GDPR also states that a revocation of consent does not render unlawful any processing performed before the revocation. Organizations that have produced processed personal data based on consent before it was withdrawn may still comply with the GDPR.

- **Voluntary.** A data subject must freely give consent. However, the Article 29 Working Party (now the **European Data Protection Board**) acknowledged the difficulty associated with determining and establishing that an employee's consent is truly voluntary where it was provided in response to an employer's request.

(GDPR, Article 7; Recitals 32, 33, 42, and 43.)

In addition to these requirements, consent-based processing covers only the consenting data subject's personal data. Because any individual custodian's data will include personal data about numerous other data subjects, securing the consent of every data subject identified in every document, communication, or piece of data is unrealistic in most cases.

For a sample consent form that counsel can use to obtain a data subject's consent to process and transfer personal data protected by non-US data protection laws for production in US discovery, see Standard Document, Consent to Process and Transfer Personal Data in US Discovery.

Legitimate Interests

Given the difficulties associated with securing valid consent, parties in US disputes typically rely on the legitimate interests basis to justify processing personal data.

To make the required showing, a litigant must be prepared to demonstrate that the interests or fundamental rights and freedoms of the data subjects do not override the litigant's legitimate interests. Counsel can employ various techniques, including data minimization and protection, to help satisfy that balancing test (see Best Practices for Cross-Border Discovery).

However, a data controller may not invoke the legitimate interests basis to process personal data if the data falls within one of the "special categories" of personal data set by the GDPR, such as:

- Data revealing a data subject's:
  - racial or ethnic origin;
  - political opinions;
  - religious or philosophical beliefs; or
  - trade union membership.
- Genetic data, biometric data, or data concerning health.
- Data concerning a data subject's sex life or sexual orientation.

(GDPR, Article 9(1).)

A data controller may process this type of personal data only if it either:

- Secures the data subject's explicit consent for processing, which is subject to more exacting consent requirements than those identified above (GDPR, Article 9(2)(a); see Consent). Explicit consent requires a data subject to state her consent clearly and in detail, leaving no room for confusion or doubt. Explicit consent can be confirmed expressly through a written statement alone and it can be further bolstered by having the data subject sign the written statement manually or digitally, fill out an electronic form, or send an email (see Article 29 Working Party, WP 259).
- Demonstrates that the processing is necessary to establish, exercise, or defend legal claims, or that a court is acting in its judicial capacity (GDPR, Article 9(2)(f)).

The GDPR does not explicitly state whether the phrase "legal claims" extends to US legal claims. Accordingly, in the context of cross-border discovery, a data controller should attempt to filter out the special categories of personal data from any further processing or transfers. Even if a party establishes a legal basis to process special categories of personal data for a US dispute, it must also conduct a data protection impact assessment (DPIA) if it intends to process the data on a large scale (see GDPR, Article 35(3); Article 29 Working Party, WP 248).

A DPIA is required where data processing "is likely to result in a high risk to the rights and freedoms of natural persons" (GDPR, Article 35(1); Article 29 Working Party, WP 248 (listing nine criteria to be considered in determining potential "high risk")). A DPIA:

- Describes the nature, scope, context, and purposes of the processing.
- Assesses whether the processing is necessary and proportional.
- Identifies and evaluates risks to data subjects.
- Specifies measures an organization can take to address data risks and demonstrate compliance.

(See GDPR, Article 35(3); Article 29 Working Party, WP 248.) The DPIA must be continuously updated and overseen by the controller in conjunction with the data protection officer. A DPIA is required in any instance where processing involves risks to the rights and freedoms of natural persons.

If the data controller determines that processing is not likely to result in a high risk, the controller should document the reasons for not carrying out a DPIA. Even where the GDPR does not require an organization to conduct a DPIA, the process may help the organization:

- Assess risks before processing data.
- Mitigate risks by demonstrating that it took actions to comply with GDPR requirements.

(See Article 29 Working Party, WP 248.)

Transferring Personal Data

In addition to needing a lawful basis to process personal data, a party must have a lawful basis to transfer data outside of the EU for discovery purposes.

Transfers to the US are particularly problematic because the GDPR permits data controllers to transfer personal data only to those countries that adequately protect personal data (GDPR, Article 45; Recital 103). The European Commission does not consider the US to offer adequate privacy protections, which means that organizations must meet certain GDPR requirements before transferring personal data to the US (GDPR, Article 46).

For purposes of EU-US data transfers for US disputes, the GDPR provisions most likely to be invoked require the transfer to be subject to appropriated safeguards, under either:

- A preapproved transfer mechanism (see Preapproved Transfer Mechanisms).
- Derogations for specific situations as set forth in GDPR Article 49 (see Derogations for Specific Situations).

Preapproved Transfer Mechanisms

Preapproved transfer mechanisms include:

- An approved code of conduct (GDPR Articles 40, and 46(2)(e)). However, no such code of conduct has been approved.
- A legally binding and enforceable instrument between public authorities or bodies (GDPR, Article 46(2)(a)).
- Binding corporate rules (GDPR, Article 46(2)(b), Article 47).
- Standard contractual clauses adopted or approved by the European Commission (GDPR, Article 46(2)(c) and (d)).

Formerly, some parties relied on the EU-US Privacy Shield as an approved certification mechanism for data transfers under GDPR Article 42. However, on July 16, 2020, the European Court of Justice (ECJ) issued a decision in *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems* (Case C-311/18) EU:C:2020:559, 16 July 2020) (*Schrems II*) that invalidated the EU-US Privacy Shield framework as a personal data transfer mechanism under the GDPR. For more on the decision, see Legal update: case report, Schrems II: controller to processor standard contractual clauses valid but EU-US Privacy Shield invalid (ECJ).

The *Schrems II* decision upheld the general validity of standard contractual clauses, but requires case-by-case evaluations on whether a recipient country's laws, such as government surveillance or reporting requirements, interfere with the mechanism's ability to provide the GDPR's required level of adequate protection for the particular transfer. The same problems that led to invalidation of the EU-US Privacy Shield (including US surveillance laws and the lack of remedies for EU data subjects) could result in a finding that standard contractual clauses are equally deficient as a basis for transferring data to the US for litigation discovery.

Moreover, none of the approved transfer mechanisms under GDPR Articles 42 or 46 permit onward or additional transfers to data processors or data controllers, including parties in US litigation.

Derogations for Specific Situations

In light of the inadequacies of preapproved transfer mechanisms in the context of cross-border discovery, litigants must rely on the derogations for specific situations set forth in GDPR Article 49. GDPR Article 49 permits transfers when:

- The transfer is necessary for the establishment, exercise of defense of legal claims (GDPR Article 49(1)(e)). However, it is questionable whether GDPR drafters intended this provision to apply to US legal claims. Moreover, where a party seeks to invoke this exemption, the transfer must be "occasional and necessary" for purposes of:
    - judicial proceedings;
    - administrative or out-of-court proceedings;
    - proceedings before regulatory bodies;
    - criminal or administrative investigations; or
    - formal pretrial discovery proceedings, including to commence a litigation or to seek approval for a merger.

    (GDPR, Recital 111; Article 29 Working Group, WP 262.) The mere possibility that litigation proceedings may arise in the future, is insufficient to justify a data transfer. This can pose challenges where, for example, a party must implement a cross-border litigation hold or perform an early case assessment before litigation arises.
- The transfer is:
    - not repetitive;
    - concerns only a limited number of data subjects;

- is necessary for purposes of compelling legitimate interests that are not overridden by the data subject's interests or rights and freedoms; and
- is subject to suitable safeguards to protect the personal data during and after the transfer.

Where transfers are made under this provision the data controller must inform both the data subjects and the supervisory authority of the transfer and the compelling legitimate interests pursued. (GDPR, Article 49(1); Recital 113.)

For information on crafting a cross-border legal hold policy and implementing a US-style legal hold abroad, see Practice Note, Cross-Border Legal Holds: Challenges and Best Practices.

For information on using early data assessment to search, organize, and cull a collection of **electronically stored information** before it is fully processed, see Practice Note, The Advantages of Early Data Assessment.

For information on how the GDPR affects the transfer of personal data between the UK and other countries outside the EEA, see Practice Note, Cross-Border Transfers of Personal Data Under the GDPR.

Retaining Personal Data

The GDPR restrictions on retaining personal data stem from the principle that personal data should be kept in a form that permits data subjects to be identified only for as long as needed to satisfy the purposes behind the processing of the personal data (GDPR, Article 5(e)).

The importance of this principle has been amplified by the "right of erasure," commonly known as the right to be forgotten. The right of erasure permits a data subject to have an organization delete personal data it possesses or controls that concerns the data subject "without undue delay," including removing personal data that the organization made public, if any of the following circumstances exist:

- The personal data is no longer needed to serve the purposes for which it was collected or otherwise processed.
- The data subject withdraws her consent and there is no other legal ground for the processing.
- The data subject formally objects to the processing and there are no overriding legitimate grounds for the processing.
- The personal data was unlawfully processed.
- The personal data must be erased to comply with a legal obligation in the EU or in an EU jurisdiction to which the data controller is subject.

(GDPR, Article 17.)

The right of erasure is a qualified right rather than an absolute right. A data controller's legitimate interests in the personal data may in some circumstances override the interests of the data subject seeking to exercise the right. Additionally, the right of erasure does not apply to processing personal data to establish, exercise, or defend legal claims. (GDPR, Article 17(3).)

For more information on the right of erasure, see Practice Note, Data Subject Rights Under the GDPR.

Best Practices for Cross-Border Discovery

Despite the uncertainty that remains, there are some practical steps that can help an organization demonstrate its good faith efforts to maximize GDPR compliance when faced with US discovery demands. For example, counsel should:

- Take full advantage of any non-EU based discovery to avoid application of the GDPR (see Non-EU Discovery).
- Analyze potential lawful bases to justify the processing of any personal data (see Lawful Basis Justification).
- Notify any affected data subjects of the potential processing and transfer and consider obtaining informed and voluntary consent where practical (see Notification and Consent).
- Minimize the volume of personal data to be processed or transferred.
- Implement appropriate safeguards to protect personal data both before and after a transfer (see Data Collector Safeguards).
- Document all processes and methods counsel have employed in their efforts to comply with the GDPR (see Recordkeeping).

Non-EU Discovery

Perhaps the most obvious means of ensuring GDPR compliance is to conduct as much discovery as possible within US borders. For example, counsel should:

- Assess whether a litigant can comply with US discovery obligations without seeking foreign discovery.
- Object to cross-border discovery requests, particularly where they are disproportional or duplicative.
- Seek judicial intervention as needed, and be prepared to demonstrate the cost and burden of searching for data abroad and complying with the GDPR.

When a party must obtain data from Europe, counsel should use existing international mechanisms such as the **Hague Evidence Convention** and **letters rogatory**.

Lawful Basis Justification

When no better alternatives exist, identifying a lawful basis under the GDPR to justify processing personal data is perhaps the most labor-intensive but critical step to maximize compliance. To help inform and support this analysis, counsel should:

- Understand the specific rules and protections in each EU jurisdiction where the applicable data resides, including any relevant country-specific rules and practices. Counsel can consult local data privacy counsel about these jurisdictional rules and local best practices, which may involve seeking agreements with works councils in some countries.

- Set out the details of documents that must be reviewed or collected, including email accounts to be searched, persons to being interviewed, relevant time periods, and relevant file types.

- Apply reasonably narrow search parameters to electronically search for only documents that are necessary (rather than merely potentially or tangentially relevant) to resolve contested issues in the dispute.

- Review any search hits within the EU to minimize the scope of a cross-border transfer, or remove any personal information from the data before transferring it to the US for review where practical.

- Immediately delete any collected data as soon as counsel determine that the data is unnecessary.

- Reconsider data needs and delete no longer needed data at key points in the litigation, such as after the dismissal or settlement of particular claims or the dismissal of certain parties.

- Consider potential compliance obligations when additional processing is performed on the preserved data.

- Ensure the data controllers and data processors (typically litigation support vendors) sign an appropriate data processing agreement that provides assurances about adequate privacy protection for personal data. Where possible, use a data processor that:
    - is located in the country where the data resides; and
    - has implemented appropriate privacy safeguards.

(For more information, see Practice Note, Data Processor Obligations Under the GDPR.)

For more information on the lawful bases under the GDPR that can justify processing personal data, see Practice Note, Overview of EU General Data Protection Regulation.

Data Collector Safeguards

Counsel should confirm that the data collector has enacted appropriate safeguards to protect collected personal data both before and after a data transfer. Common safeguards include:

- **Security measures.** Data encryption or other reasonable protections should be in place when handling personal data. This is useful for both the data transfer and the subsequent storage and handling of the data in the US.

- **Confidentiality agreements and protective orders.** These agreements and orders can help shield the confidentiality of personal data that is included in the transferred data. (For more information, see Standard Document, Protective Order for Documents Protected by Non-US Data Protection Laws.)

- **Restricted access to transferred data.** Counsel should permit individuals to view the data only on an as-needed basis, and should document any instances where someone has accessed the data.

- **Pseudonymizing software tools.** Software or service providers that can pseudonymize personal data even before review or transfer of the data can help mitigate the risk that personal data will be improperly processed or transferred. Only a small minority of documents produced for discovery in US litigation are used in **depositions** or at trial. Even pseudonymized versions of documents typically contain enough information for trained reviewers to determine their potential importance for resolving disputed issues in the litigation. Where reviewers determine that an pseudonymized document is highly relevant, an organization might need to produce that document in its original form. Yet, by pseudonymizing documents before the initial review, an organization can filter out most (indeed, all but the most relevant) documents from further processing or transfer, thereby minimizing any necessary processing or transfer of key documents with personal data still intact (see Practice Note, Anonymization and Pseudonymization Under the GDPR).

- **Inspection instead of production.** Counsel should consider requiring the requesting party to examine the data at a secure location (preferably before the data transfer) where possible rather than producing documents containing personal data. After that inspection, counsel can arrange for the transfer of only truly necessary documents, which generally make up a small portion of the original data universe.

- **Deletion of unneeded data as soon as possible.** As noted above, counsel should arrange to delete any collected data as soon as it is no longer needed. Additionally, counsel should ensure, through a case management, confidentiality, or protective order and through agreements with litigation support providers, that all parties must delete any remaining data when the dispute is resolved. To confirm compliance with this obligation and ensure the data is deleted on a timely basis, counsel should follow up with the data controllers, any litigation support vendors, and opposing counsel (who must then follow up with their clients and litigation support vendors).

Notification and Consent

Counsel should notify data subjects when their data is being processed or transferred for a US dispute. This information may also be contained in an organization's privacy policy, but boilerplate notices in a privacy policy generally do not meet notification requirements under the GDPR. Instead, counsel should consider providing specific notices, to the extent practicable, when data is being transferred for a particular dispute.

For more on the GDPR notice requirements, see Practice Note, Overview of EU General Data Protection Regulation: Transparency.

Counsel generally should avoid relying on consent as the primary basis for any data processing or transfers. If counsel must seek consent, they should:

- Take steps to ensure and document that the data subject's consent was truly informed, specific, voluntary, and revocable to the extent possible.

- Put measures in place to address the exercise of data subject rights, including any objections to the processing or transfer and requests to access the personal data, as applicable.

Recordkeeping

In light of the GDPR's new accountability requirement, counsel should maintain detailed documentation of all procedures used in connection with processing or transferring personal data and constantly monitor the data controller's compliance with data protection laws. In general, all technical and organizational procedures and data subject notifications must be recorded. An organization may use this information when demonstrating its compliance during any audits. For more on the GDPR's accountability requirement, see Practice Note, Demonstrating Compliance with the GDPR.

The Sedona Conference Resources

The Sedona Conference provides various resources to help organizations and their counsel navigate cross-border discovery. Key principles from this guidance include the following:

- Counsel and parties should demonstrate due respect for foreign data protection laws.
- Where full compliance presents a conflict of law, a party's conduct should be judged by a standard of good faith and reasonableness.
- Parties should limit the scope of preservation and discovery to limit conflicts of law.
- Where a conflict with GDPR compliance arises, the parties should enter into a stipulation or obtain a court order.
- Data controllers should be prepared to demonstrate that adequate protections have been implemented to safeguard personal data.
- Data controllers should retain protected data only as long as necessary.

(See The Sedona Conference, International Principles on Discovery, Disclosure & Data Protection in Civil Litigation.)

The Legal Intelligencer

'Things Just Couldn't Be the Same' After the 'Lynyrd Skynyrd' Spoliation Decision

Most lawyers know to advise their clients to preserve evidence in their "care, custody or control" relevant to pending or threatened litigation. But exactly how far does "control" go? Can a party be sanctioned for spoliation for failing to issue a legal hold notice to a third party who has no obligation to follow your legal hold instructions?

By **David R. Cohen and Todd R. Fairman** | February 05, 2018

Most lawyers know to advise their clients to preserve evidence in their "care, custody or control" relevant to pending or threatened litigation. But exactly how far does "control" go? Can a party be sanctioned for spoliation for failing to issue a legal hold notice to a third party who has

no obligation to follow your legal hold instructions? A recent case, relating to the late, great rock band Lynyrd Skynyrd, answers that question in the affirmative, see *Ronnie Van Zant v. Pyle*, No. 17 Civ. 3360 (RWS) (https://scholar.google.com/scholar?scidkt=16422730876387523656&as_sdt=2&hl=en) , 98 Fed. R. Serv.3d 719 (S.D.N.Y. 2017).

Rock music fans will recall the Lynyrd Skynyrd band, and its hit songs like "Freebird" and "Gimme Three Steps." Fans may also recall that the band's lead singer and primary songwriter, Ronnie Van Zant, died in a tragic private plane crash in 1977. Other members of the band were also killed or critically injured in the crash. Following the crash, Van Zant's widow, other family members and some surviving members of the band entered into a "blood oath" never to perform again under the Lynyrd Skynyrd name. A commemorative tribute tour 10 years later resulted in a legal dispute which was resolved in 1988, by a consent order signed by multiple parties, including the band's former drummer, Artimus Pyle. The consent order provided that former band members could again perform under the Lynyrd Skynyrd name, if certain conditions were met, but signatories were permanently restrained and enjoined from exploiting the history of the Lynyrd Skynyrd band (including in movies or books) without the advance written approval of the other original band members and the Van Zant estate.

Fast forward to 2016 when Cleopatra Records and its filmmaking affiliate decided to make a movie based on the 1977 plane crash. Cleopatra contracted with screenwriter/director Jared Cohn to write and direct the film, and subsequently hired Pyle to consult and co-produce. Once they learned about plans for the film, other signatories to the 1988 consent order sent a "cease and desist" letter, and ultimately filed suit on May 5, 2017. The suit named Pyle

and Cleopatra, but did not name Cohn as a defendant. Cleopatra's defense included arguing that Pyle's role was limited and that release of the movie should not be enjoined as a result of that limited involvement by Pyle.

Gimme These Texts, Gimme These Texts Mister

Throughout the writing of the film, Cohn frequently consulted with Pyle by telephone and by text messages. Plaintiffs demanded that the text messages from Cohn be produced, so that the extent of Pyle's influence on the film could be illuminated. However, Cohn had switched phone providers and cellphones in mid-May 2017, shortly after filming was completed and the suit was filed. The text messages on Cohn's old phone were not transferred or otherwise preserved. Plaintiffs urged the court to find that the failure to preserve the text messages constituted spoliation of evidence and asked the court to draw an adverse inference against Cleopatra.

Senior Judge Robert Sweet signed his detailed and well-written opinion on Aug. 23, 2017, less than three months before his 96th birthday. He granted the plaintiffs' request for an adverse inference. Even though Cleopatra did not have any legal right to force Cohn to preserve the messages, Judge Sweet held that the text messages were, "practically speaking," under Cleopatra's control because Cohn had been working closely with Cleopatra for over a year, and stood to gain financially if Cleopatra prevailed in the litigation. Sweet's reliance on the "practical control" test was in line with established law in the Southern District of New York, see *GenOn Mid-Atlantic v. Stone & Webster*, 282 F.R.D. 346 (S.D.N.Y. 2012) (there was "little doubt that [plaintiff's litigation consultant] would have complied with a timely request by the [plaintiff] to preserve its information."); *In re NTL Securities Litigation,* 244 F.R.D. 179 (S.D.N.Y. 2007) ("documents are considered to be under a party's control when that party has the right, authority, or practical ability to obtain the documents from a nonparty to the action.").

Sweet Home Alabama?

Is this same "practical ability" test applied outside of the Southern District of New York? The answer is mixed. If you are in Alabama—or anywhere in the U.S. Court of Appeals for the 11th Circuit—you could cite *Searock v. Stripling*, 736 F.2d 650 (11th Cir.1984) (https://www.bloomberglaw.com/product/blaw/bc/W1siRG9jdW1lbnQiLCIvcHJvZ-bb2af6a3ad3992c0d4ee3ed3eef6f89758eb262a/document/XABO2C?jcsearch=736%20F.2d%20650&summary=yes#jcite), for the proposition that control means "the legal right to obtain documents." Courts in other jurisdictions have split with regard to the construction of "control." Compare *Ricks v. Wood*, No. 13-00264-TLM Chapter 11, 2015 BL 202107 (Bankr. D. Idaho June 24, 2015); *Hill v. Asset Acceptance,* 2014 BL 186028 (S.D. Cal. Jul 3, 2014); and *Tank Connection v. Haight*, No. 13-cv-1392-JTM-TJJ, 2015 BL 177306 (D. Kan. June 4, 2015) (applying "legal right" test) with *Benisek v. Lamone*, 320 F.R.D. 32 (D. Md. 2017); *Duarte v. St. Paul Fire & Marine Insurance,* No. EP-14-CV-305-KC, 2015 BL 395112 (W.D. Tex. Sept. 25, 2015); and *SRAM, v. Hayes Bicycle Group,* No. 12 C 3629, 2013 BL 341173 (N.D. Ill. Dec. 10, 2013) (applying "practical ability" test). No case, however, had gone as far as the *Van Zant* case in finding "control" in the absence of any corporate affiliation, employment or agency relationship.

One could argue that there is a logical gap between a nonparty having a close relationship with a litigant, or even a financial interest in the outcome of litigation, and necessarily complying with a voluntary request to preserve or produce documents absent legal compulsion. Why should the nonparty shoulder that burden absent knowing the documents will be helpful to its allies in the litigation (or worse, if the nonparty knows or suspects that the documents will be unhelpful)?

Perhaps that, and a sense of "frontier justice," is part of what drove the decision in this case and other cases that have looked at nonparty interests in litigation outcomes as a factor in determining the scope of "control," see, e.g., *Costa v. Kerzner International Resorts,* 277 F.R.D. 468 (S.D. Fla. 2011)*; Steele Software Systems v. DataQuick Information Systems,* 237 F.R.D. 561 (D. Md. 2006). It is not really that the nonparty would volunteer to preserve or produce the information if asked, but that a nonparty's decision about whether to do so could be based on the content of the documents. Other factors cited in Judge Sweet's opinion included the failure of defendant Pyle to produce any texts or other documents*,* suspicious timing of Cohn's cellphone upgrade (shortly following filing of the litigation), and the fact that Cohn managed to copy over his pictures from his old phone, but not the texts*.* While the defendants essentially took the position that Cohn and Cleopatra were *free as a bird* not to arrange preservation of those messages, Sweet essentially held *Lord knows they're to blame*.

I Wish You'd Let Me Ask One Favor From You

There are good reasons for courts to show restraint in extending the concept of control beyond legal control and into territory where they have to start speculating about "close relationships" or "shared interests in litigation outcomes." *Implementing* legal holds can be a major burden on litigants, and a challenge to properly scope, even when the holds are limited to litigants' employees and agents. There are other mechanisms available, including subpoenas, for requesting parties to obtain evidence from nonlitigants, without getting on the slippery slope of how far a "practical ability" test extends the preservation obligations of parties.

We have not, as of yet, heard the last of the *Van Zant* case. The case is now on appeal to the Second Circuit Court of Appeals, and a number of leading news media, movie studios and television networks have submitted *amicus* briefs

challenging the injunction decision on the basis that it is an unconstitutional prior restraint of free speech. There is also a strong argument that the court's imposition of an adverse inference sanction was improper under the Federal Rules, in the absence of any finding that "a party acted with the intent to deprive another party of the information's use in the litigation."

Unless or until there is a reversal on the control issue, however, you will be well advised to counsel your clients to extend their circulation of preservation notices, not only to their own employees and agents who might have relevant information, but also to any third parties with which they may have close relationships. Only then will you and they be able to say "*now we all did what we could do*."

David R. Cohen *is a partner in the global law firm, Reed Smith, where he leads the firm's records and e-discovery (RED) practice group.*

Todd R. Fairman *is an e-discovery attorney in the firm's RED group.*

2021 WL 831025
Only the Westlaw citation is currently available.
United States District Court, C.D. California.

BENEBONE LLC

v.

PET QWERKS, INC., et al.

Case No. 8:20-cv-00850-AB-AFMx
|
Filed 02/18/2021

Attorneys and Law Firms

Andrea Levenson, Jason T. Lao, Haynes and Boone LLP, Costa Mesa, CA, Joseph Lawlor, Pro Hac Vice, Richard Rochford, Pro Hac Vice, Haynes and Boone LLP, New York, NY, Kenneth G. Parker, Gibson Dunn and Crutcher LLP, Irvine, CA, for Benebone LLC.

Ali Razai, Adam R. Aquino, Steven J. Nataupsky, Knobbe Martens Olson and Bear LLP, Lewis E. Hudnell, III, Natalya Vasyuk, Rolando Javellana Tong, Manning and Kass Ellrod Ramirez Trester LLP, Irvine, CA, Benjamin B. Anger, Knobbe Martens Olson and Bear LLP, San Diego, CA, Daniel I. Hwang, Pro Hac Vice, Joseph F. Arand, Pro Hac Vice, Michael T. Murphy, Pro Hac Vice, Global IP Counselors LLP, Washington, DC, for Pet Qwerks, Inc., et al.

Proceedings (In Chambers): Order Granting Defendants Pet Qwerks, Inc. and Doskocil Manufacturing Company, Inc. D/B/A Petmate's Motion to Compel Plaintiff Benebone LLC's Production of Slack Communications (ECF No. 88)

The Honorable: ALEXANDER F. MacKINNON, U.S. Magistrate Judge

***1** Defendants Pet Qwerks, Inc. and Doskocil Manufacturing Company, Inc. d/b/a Petmate (collectively, "Defendants"), have filed a motion seeking to compel Plaintiff Benebone LLC ("Benebone") to be required to produce Slack communications responsive to Defendants' document requests. For the reasons provided below, Defendants' motion is **GRANTED** to the extent set out herein.

I. Background

Slack is a cloud-based software system that allows a company to organize its electronic discussions into user-defined categories called "channels." Plaintiff Benebone uses Slack, as well as standard email, for its internal communications.

During the parties' early discussions regarding discovery of electronically stored information, Defendants sought to include Benebone's Slack messages in the parties' Stipulated ESI Order, and Benebone took the position that Slack messages should be excluded from discovery. The parties requested a telephonic discovery conference with the Court to address this, and each side submitted a short brief outlining its position. (*See* ECF Nos. 60-63.) Defendants included a declaration from Michael Gutierrez, Director of Forensic Services at Xact Data Discovery, an e-discovery vendor that Defendants have engaged for this case. During the telephonic discovery conference on November 23, 2020, the Court concluded that Benebone's Slack messages are relevant, but it lacked sufficient information to determine whether Slack discovery would be proportional to the needs of the case. Accordingly, the Court ordered the parties to meet and confer further regarding possible Slack production after Benebone had obtained additional information about its Slack account and what would be required to search and produce responsive Slack messages.

As part of the meet and confer process, Benebone informed Defendants that its Slack account contains approximately 30,000 messages. Benebone also estimated that it would cost $110,000 to $255,000 to extract, process, and review these 30,000 messages. Based on these cost estimates, Benebone maintained that searching and producing documents from Slack would be an undue burden and would not be proportional to the needs of the case. Defendants disagreed and filed the present motion to compel Benebone to produce its responsive Slack messages. (ECF No. 88.) The parties filed a joint stipulation pursuant to L.R. 37-2, as well as supplemental memoranda. (*See* ECF Nos. 89-92, 102-104.)

In connection with the motion to compel, Defendants submitted a second declaration from Mr. Gutierrez. In his declarations, Mr. Gutierrez stated that he has been involved in multiple lawsuits where Slack messages have been produced. He described a number of tools that software vendors have developed to streamline review and production of Slack messages and explained how extracting, processing, and reviewing Slack messages could take place using currently available software tools. He also provided a cost estimate for doing so in this case. Mr. Gutierrez stated that Xact offers

contract review attorneys at a rate of $40 per hour to conduct the first level review of Slack messages, and he provided a cost estimate of $22,000 for Benebone to find and produce its responsive Slack messages. Benebone, on the other hand, stood by its prior estimate of $110,000 to $255,000 based on a blended attorney rate of $400 per hour for Slack review. Benebone did not provide a declaration from an e-discovery expert to support its conclusions or respond to the evidence provided by Mr. Gutierrez.

***2** The Court held a Zoom hearing on February 3, 2021 regarding Defendants' motion to compel. Mr. Gutierrez attended the hearing and answered the parties' and the Court's questions under oath.

II. Discussion

Federal Rule of Civil Procedure 26(b)(1) provides that a party may obtain discovery "regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case[.]" Factors to consider include "the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit." *Id.* Discovery need not be admissible in evidence to be discoverable. *Id.* However, a court "must limit the frequency or extent of discovery otherwise allowed by [the Federal] rules" if "(i) the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive; (ii) the party seeking discovery has had ample opportunity to obtain the information by discovery in the action; or (iii) the proposed discovery is outside the scope permitted by Rule 26(b)(1)." Fed. R. Civ. P. 26(b)(2)(C). Boilerplate or general objections are not appropriate, and a party's objections should be specific to each particular discovery request and be supported by evidence. *See* Fed. R. Civ. P. 34(b)(2). "Upon a motion to compel discovery, the movant has the initial burden of demonstrating relevance. In turn, the party opposing discovery has the burden of showing that discovery should not be allowed, and also has the burden of clarifying, explaining and supporting its objections with competent evidence." *United States v. McGraw-Hill Cos.*, 2014 WL 1647385, at *8 (C.D. Cal. Apr. 15, 2014) (citations and internal quotation marks omitted)). The Federal Rules of Civil Procedure must be "construed, administered, and employed by the court and the parties to secure the just, speedy, and inexpensive determination of every action and proceeding." Fed. R. Civ. P. 1.[1]

Here, because Benebone uses Slack as part of its internal business communications, there is no real dispute that Benebone's Slack messages are likely to contain relevant information. The crucial issue is whether requiring Benebone to search for and produce responsive Slack messages would be unduly burdensome and disproportional to the needs of this case. In this regard, the Court relies on Mr. Gutierrez's testimony regarding the estimated cost and level of effort necessary for producing the Slack messages. Mr. Gutierrez was a knowledgeable and credible witness on this subject, and his declarations and testimony at the hearing were not rebutted by a Benebone witness.

***3** Mr. Gutierrez testified that third-party tools have been developed over the past several years for collecting and reviewing Slack messages and that review and production of Slack messages has become comparable to email document production through use of these tools. Mr. Gutierrez further testified that it likely would not be necessary for Benebone to search all its Slack messages. Instead, searches likely could be limited to certain Slack channels, users, or custodians – which could significantly reduce the volume of Slack messages requiring review. For instance, in this intellectual property case, it may not be necessary to extract and review messages in a Slack channel dealing with human resources issues.

Moreover, Mr. Gutierrez's declarations and testimony indicate that it is possible to conduct first level review of the pertinent Slack messages via contract attorneys for far less than Benebone's estimated blended rate of $400 per hour. Mr. Gutierrez testified that contract reviewers are available who are licensed attorneys at a rate as low as $40 per hour for first-level review. As discussed during the hearing, Mr. Gutierrez did not include any time or expense for second-level review by more experienced counsel. It is also possible that contract attorneys may cost somewhat more than the hourly rate used in his estimate. Thus, the Court finds that Mr. Gutierrez's estimate of $22,000 for Benebone to review and produce Slack messages is on the low side. However, Benebone's cost estimate of $110,000 to $255,000 for producing the Slack messages is substantially inflated due to its assumption of attorney review of all 30,000 Slack messages at a rate of $400 per hour. As noted above, Benebone did not provide an e-discovery declaration or testimony to support its cost estimate or its position that producing the Slack messages represents an undue burden and is disproportional to the needs of this case.

III. Conclusion

Based on the evidence presented in the parties' briefing and at the hearing, the Court finds that requiring review and production of Slack messages by Benebone is generally comparable to requiring search and production of emails and is not unduly burdensome or disproportional to the needs of this case – if the requests and searches are appropriately limited and focused. Defendants' evidence supports this conclusion, and Benebone has responded largely with attorney argument but no witness or declarant on the e-discovery issues. E-discovery tools are available for this process, and the Slack messages to be reviewed can be narrowed based on the channels or users likely to have responsive information given the relevant issues in this case. Although Benebone makes cursory reference to other proportionality factors (*see* ECF No. 89 at 22.), its focus has been on the purported burdens associated with production of Slack documents and the fact that Benebone is a small company compared to Defendants. Nevertheless, Benebone seeks the full range of monetary damages in this case, plus injunctive relief against Defendants' accused products – sales of which are allegedly in the millions of dollars. As discussed herein, a focused search for and production of Slack messages is proportional to the needs of this case where Benebone regularly uses Slack messaging for internal business communications and users of Slack include Benebone's marketing director, COO, and CEO (who is also a named inventor on the three asserted design patents). Thus, the Court agrees with Defendants that e-discovery in this case shall include Benebone's Slack messages.

To be clear, the parties have not fully briefed, and the Court has not resolved by this order, the question of specific request categories and search methodologies to be used for identification, review and production of Benebone's Slack messages. To address what will be searched for and how the search will take place, the parties shall meet and confer no later than **March 5, 2021**. At least seven days before this meet and confer, Benebone shall provide to Defendants a list of its Slack channels, including the title and a brief description of each Slack channel, the number of messages in each Slack channel, the users associated with each Slack channel, and any other data that will assist the parties in tailoring the Slack review and production.

***4 IT IS SO ORDERED.**

All Citations

Slip Copy, 2021 WL 831025

Footnotes

1 Slack is a relatively new communication tool, but a few published cases have addressed production of Slack messages. For example, in *Calendar Research LLC v. Stubhub, Inc.*, 2019 WL 1581406, at *4 (C.D. Cal. Mar. 14, 2019), the court granted the plaintiff's motion to compel production of defendants' remaining relevant Slack messages. Similarly, in *BidPrime, LLC v. SmartProcure, Inc.*, 2018 WL 6588574, at *2 (W.D. Tex. Nov. 13, 2018), the Court ordered production of remaining Slack messages because "they may be relevant and SmartProcure has not provided a specific objection to the contrary." *Id.* In *Milbeck v. Truecar, Inc.*, 2019 WL 4570017 at *3 (C.D. Cal. May 2, 2019), the court denied the plaintiff's motion for Slack production without prejudice, because of an imminent trial date.

End of Document

Reed Smith is a dynamic international law firm, dedicated to helping clients move their businesses forward.

Our long-standing relationships, international outlook, and collaborative structure make us the go-to partner for speedy resolution of complex disputes, transactions, and regulatory matters.

ABU DHABI
ATHENS
AUSTIN
BEIJING
BRUSSELS
CENTURY CITY
CHICAGO
DALLAS
DUBAI
FRANKFURT
HONG KONG
HOUSTON
KAZAKHSTAN
LONDON
LOS ANGELES
MIAMI
MUNICH
NEW YORK
PARIS
PHILADELPHIA
PITTSBURGH
PRINCETON
RICHMOND
SAN FRANCISCO
SHANGHAI
SILICON VALLEY
SINGAPORE
TYSONS
WASHINGTON, D.C.
WILMINGTON

reedsmith.com