TABLE OF CONTENTS

CASE NOTES (prepared by Larimer Law)

1. **Federal Rule of Civil Procedure 37 (e): Sanctions for Destruction of ESI.**
    - *GN Netcom v. Plantronics*, No. CV 12-1318-LPS, 2016 WL 3792833 (D. Del. July 12, 2016).
    - *Klipsch* Group*, Inc. v. ePRO E-Commerce Limited*, 880 F.3d 620 (2d Cir. 2018).
    - *Indus.* Quick *Search, Inc. v. Miller, Rosado & Algois, LLP*, No. 13 Civ. 5589 (ER), 2018 U.S. Dist. LEXIS 391 (S.D.N.Y. Jan 2, 2018).
2. **Technology Assisted Review (TAR): What is it and Should You Be Using It?**
    - *Winfield v. City of New York*, No.15-cv-5236 (LTS) (KHP), 2017 WL 5664852, at *8-10 (S.D.N.Y. Nov. 27, 2017).
3. **Raising Objections to the Format of ESI Productions: Do it Early and Do it Clearly.**
4. **Amended FRE 902 Expands Self-Authentication to Certain Electronic Data.**
5. **RULE 26(b)(1) and "Proportionality": How to make a winning argument in the context of eDiscovery.**
    - *In re Namenda Direct Purchaser Antitrust Litig.,* No. 15 Civ. 7488 (CM) (JCF), 2017 U.S. Dist. LEXIS 173403 (S.D.N.Y. 2017)
    - *Moll v. Telesector Res. Grp., Inc*., No. 04-CV-0805S(Sr), 2017 WL 2241967 (W.D.N.Y. May 23, 2017).
    - *Oxbow Carbon & Minerals* LLC *v. Union Pacific Railroad Company*, 322 F.R.D. 1 (D.D.C. 2017).

EDRM MODEL

GLOSSARY

ETHICS RULES, STATE BAR ETHICS OPNIONS AND OTHER RESOURCES

1. New York Rules of Professional Conduct [22 NYCRR 1200.0] Rule 1.1 – Competence.
2. New York Rules of Professional Conduct [22 NYCRR 1200.0] Rule 1.1 Comment [8].
3. New York Rules of Professional Conduct [22 NYCRR 1200.0] Rule 5.3 – Lawyer's Responsibility for Conduct of Non-lawyers.
4. New York Rules of Professional Conduct [22 NYCRR 1200.0] Rule 5 Comment [3].
5. NYSBA Comm. On Professional Ethics, Formal Op. 1020, September 12, 2014
6. State Bar of California Standing Comm. On Professional Responsibility and Conduct Formal Op. 2015-193.
7. WDNY Local Rules of Civil Procedure Rule 16(b)(2)(A).
8. Request for Public Comment on Proposed Amendment of Rule 11-e of the Rules of the Commercial Division (22 NYCRR §202.70[g], Rule 11-e), to Address Technology-Assisted Review.

1. Federal Rule of Civil Procedure 37 (e): Sanctions for Destruction of ESI

Federal Rule of Civil Procedure 37(e) outlines the potential consequences for failure to preserve Electronically Stored Information (ESI):

> "(e) Failure to Preserve Electronically Stored Information. If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery, the court:
>
> (1) Upon finding prejudice to another party from loss of the information, may order measures no greater than necessary to cure the prejudice; or
> (2) only upon finding that the party acted with the intent to deprive another party of the information's use in the litigation may:
> (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."

Sanctions imposed under Rule 37 (e) can be quite drastic and the courts have broad discretion to sanction parties who fail to preserve ESI, though the harshest penalties are reserved for those who act in bad faith.[1]

One recent case, *GN Netcom v. Plantronics*, No. CV 12-1318-LPS, 2016 WL 3792833 (D. Del. July 12, 2016) fleshes out the contours of Rule 37 (e) and illustrates the threat that a rogue employee can pose to an organization's best laid plans for preservation of data. In *GN Netcom*, Plaintiff GN Netcom sued Defendant Plantronics in the United States District Court for the District of Delaware for attempted monopolization, restraint of trade, and tortious interference with business relations. Plaintiff moved for sanctions after learning Defendant's Senior Vice President had intentionally deleted emails and directed his subordinates to follow suit. Defendant opposed Plaintiff's motion for sanctions citing its "extensive document preservation efforts."

At first glance, Defendant Plantronics seemed to have taken all the right steps to preserve ESI. Upon receiving Plaintiff's demand letter, Defendant promptly issued a legal hold, provided training sessions to ensure employee compliance and sent quarterly reminders to its employees. Nonetheless, Defendant's Senior Vice President continued to delete potentially responsive emails, ultimately more than 40% during the three-month period covered by Defendant's legal hold.

After discovering the deletions, Defendant's in-house counsel took a number of aggressive steps to recover the lost data and implemented an "anti-email-deletion litigation feature." Ultimately, however, Defendant's efforts to retrieve the deleted emails seemed mostly for show. Defendant fired a forensics expert before its work was done and unrestored the emails the expert had restored. Defendant's outside counsel also told

[1] See Fed. R. Civ. P. 37(e) 2015 advisory committee notes.

Plaintiff it was "incorrect to assume deletion" at a time when the Defendant had *actual knowledge* of the deletion.

The Court found Defendant acted in bad faith, imputing the actions of Defendant's Senior Vice President to the company based upon his high position. The company's lack of transparency and cooperation further "buttress[ed]" the Court's bad faith finding. In the end, the Court awarded attorney fees, $3,000,000 in punitive damages, and $1,900,000 in monetary sanctions to Plaintiff.[2] The Court also imposed evidentiary sanctions in the form of instructions allowing the jury to draw adverse inferences that destroyed emails would have been favorable to Plaintiff's case and/or unfavorable to Defendant's defense.[3]

GN Netcom shows that issuing a legal hold alone will not always prevent deletion of ESI or insulate a party from sanctions. Active monitoring of the compliance with the hold is important. Moreover, organizations that routinely face litigation may benefit from using technology to automate legal hold procedures and to lock down employee data to prevent it from being altered or deleted after a hold is in place.

As mentioned above, sanctions imposed under Rule 37 (e) can be quite drastic and the harshest penalties are reserved for those who act in bad faith. A more recent and closer to home illustration of this can be seen in *Klipsch Group, Inc. v. ePRO E-Commerce Limited*, 880 F.3d 620 (2d Cir. 2018). In *Klipsch*, the Second Circuit affirmed the imposition of sanctions finding that $2.7 million to compensate plaintiff for its corrective discovery efforts and a corresponding asset restraint in that amount, permissive and mandatory jury instructions, and an additional $2.3 million bond to preserve plaintiff's ability to recover damages and fees at the end of the case, properly compensated the plaintiff for the corrective steps taken with the court's permission in response to defendant's discovery-related misconduct. In reaching that decision, the Second Circuit emphasized that although the value of the case, perhaps as low as $20,000, was a fraction of the amount of the sanctions, "discovery sanctions should be commensurate with the cost of discovery efforts created by the sanctionable behavior" not bounded by the value of the case itself.

A lawyer's failure to advise their client to preserve ESI can also result in professional malpractice. In *Industrial Quick Search, Inc. v. Miller, Rosado & Algois, LLP*, No. 13 Civ. 5589 (ER), 2018 U.S. Dist. LEXIS 391 (S.D.N.Y. Jan 2, 2018), plaintiff's legal malpractice claims survived summary judgment. Material factual questions included whether defendant had failed to advise plaintiff of its duty to preserve evidence, including the need to issue a legal hold, in a prior matter in which plaintiff was sanctioned for spoliating evidence. In finding the malpractice claim could proceed, the court stated that "counsel has an obligation to take reasonable steps to ensure the preservation of relevant information," and that "an attorney's failure to fulfill that 'obligation' falls below the ordinary and reasonable skill possessed by members of the bar."

---

[2] *GN Netcom v. Plantronics*, No. C.A. No. 12-cv-1318-LPS (D. Del. October 3, 2016) (Stipulation and [Proposed] Order Related to Monetary Spoliation Sanctions).

[3] *GN Netcom v. Plantronics*, No. C.A. No. 12-1318-LPS, 2018 U.S. Dist. LEXIS 533 (D. Del. January 3, 2018).

2. Technology Assisted Review (TAR): What is it and Should You Be Using It?

Today, organizations, and even many individuals, possess thousands if not millions of pieces of electronic data, all of which are potentially subject to discovery. When litigation arises, a party will need to comb through this data to look for and produce relevant documents. This process usually starts by generating a universe of potentially relevant documents, which in turn are reviewed by a team, most often attorneys, who check for relevance, privilege, confidentiality and other pertinent content and who assess which documents must be produced to opposing counsel.

Collecting, reviewing and electronically processing these documents can be expensive and disruptive to business. Therefore, it is important to be strategic when identifying the universe of documents to be reviewed and potentially produced. Wholesale, unfiltered collections of employee email inboxes, laptops and hard drives will invariably be over-inclusive. To deal with this, many attorneys craft and run search terms across a client's data to sift through the noise and identify potentially relevant documents. By way of example only, for a matter alleging misappropriation of trade secrets by "Al Steelit" with respect to "Dirt-Away", a cleaning product whose key ingredient is seaweed, the attorney may have his client run terms such as "Dirt-Away", "cleaning", and "seaweed" across Al Steelit's emails, to identify a universe of potentially relevant emails to review. However, even after search terms are applied to a data set, the results are often over-inclusive.

Enter Technology Assisted Review (TAR), also referred to as Predictive Coding or Computer Assisted Review. TAR combines human expertise with computer learning technologies to cull large amounts of data down to a reasonably sized review universe. Although there are variations, the TAR process generally involves attorneys reviewing a small set of data for responsiveness (or lack thereof) and other issues specific to the case, and then feeding this information to the TAR software. The software then propagates the human coding to the entire set of data to emulate decisions that the reviewing attorneys would make. In this manner, by using TAR, a large set of documents can be culled down to a much smaller and more manageable set consisting of the documents most likely to be responsive. It should be noted that there are many ways to leverage technology to analyze and cull data, short of a full blown TAR. Such technology is often collectively referred to as Early Case Assessment (ECA) tools. ECA tools can help to detect and visualize patterns in unstructured data, which in turn can help attorneys to make smart, legally defensible decisions on data collections and data review.

The idea of substituting the judgement of a human for that of a computer inevitably raises eyebrows. However, not only is TAR accepted by many courts, some courts are now mandating TAR. See, for instance, *Winfield v. City of New York*, No.15-cv-5236 (LTS) (KHP), 2017 WL 5664852, at *8-10 (S.D.N.Y. Nov. 27, 2017) ("[G]iven the volume of documents collected, this Court directed the City to … begin using [TAR] software to hasten the identification, review, and production of documents responsive to Plaintiff's document requests.").

Winfield, in fact, *may* close the loop on a line of cases by United States Magistrate Judge Andrew Peck signaling that district's embrace of TAR. In 2012, Judge Peck Judge

Peck explicitly approved the use TAR and observed that "while some lawyers still consider manual review to be the 'gold standard,' that is a myth, as statistics clearly show that computerized searches are at least as accurate, if not more so, than manual review."[4] Three years later, in *Rio Tinto PLC v. Vale S.A.*, Judge Peck de-mystified TAR and cast it as just another tool to manage electronic discovery that "[should not be held] to a higher standard than keywords or manual review."[5] Finally, in 2016, Judge Peck held in *Hyles v. New York City* that a producing party cannot be compelled to use TAR but noted that "[t]here may come a time when TAR is so widely used that it might be unreasonable for a party to decline to use TAR. We are not there yet."[6] With *Winfield*, it appears that we might now be "there", or getting closer to it.

TAR is also making waves in the New York Unified Court System. On March 8, 2018, the Office of Court Administration issued a request for public comment on the addition of the following proposed language to Rule 11-e of the Rules of the Commercial Division:

> The parties are encouraged to use the most efficient means to review documents, including electronically stored information ("ESI"), that is consistent with the parties' disclosure obligations under Article 31 of the CPLR and proportional to the needs of the case. Such means may include technology assisted review, including predictive coding, in appropriate cases.

The stated purpose of the amendment, while not prescribing any particular form of TAR, is to "make clear that that the Commercial Division is sensitive to the cost of document review in complex commercial cases and is in line with other courts including other centers of high-stakes commercial litigation such as the Southern District and the Delaware Chancery Court, in supporting the use of technology assisted review, including predictive coding, in appropriate cases."

---

[4] *Moore v. Publicis Groupe*, 287 F.R.D. 182, 191–93 (S.D.N.Y. 2012), *adopted sub nom. Moore v. Publicis Groupe SA*, No. 11 CIV. 1279 ALC AJP, 2012 WL 1446534 (S.D.N.Y. Apr. 26, 2012).
[5] *Rio Tinto v. Vale,* 306 F.R.D. 125, 129 (S.D.N.Y. 2012).
[6] *Hyles v. New York City,* No. 10 CIV. 3119 AT AJP, 2016 WL 4077114, at *3 (S.D.N.Y. Aug. 1, 2016).

3. Raising Objections to the Format of ESI Productions: Do it Early and Do it Clearly

Electronically stored information ("ESI") can be produced in "native format" or in modified electronic formats, such as "load files" or "image files." When ESI is produced in "native format," it is produced to the demanding party in the same electronic format in which it existed in the hands of the producing party. For example, a spreadsheet created in Excel would be produced in its "native" format by providing the Excel file to the demanding party.

A document produced in native format will usually include all the metadata attached to the document. Metadata is often described as "information about information." It is the data associated with an electronic file that describes things like how, when and by whom the file was collected, created, accessed, modified or formatted. While certain metadata fields are typically produced in electronic document production, practitioners should take care to understand what exactly has been requested for production, and what they will be producing. The type of metadata included with an image file or load file is sometimes negotiated at the outset of discovery

Federal Rule of Civil Procedure 34(b)(2)(E) specifically addresses the production format of ESI:

> (E) *Producing the Documents or Electronically Stored Information.* Unless otherwise stipulated or ordered by the court, these procedures apply to producing documents or electronically stored information:
>
> (i) A party must produce documents as they are kept in the usual course of business or must organize and label them to correspond to the categories in the request;
>
> (ii) If a request does not specify a form for producing electronically stored information, a party must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms; and
>
> (iii) A party need not produce the same electronically stored information in more than one form.

If the demanding party does not specify the format for producing ESI, the producing party can produce the ESI in the form in which it is ordinarily maintained (i.e., native format) or "in a reasonably usable form or forms." Federal Rules of Civil Procedure 34(b)(2)(B) & -(D) provide that if the producing party objects to the ESI format requested by the demanding party, the producing party must: (1) state its objection with specificity; and (2) must state the alternative format it intends to use[7].

The producing party must object to the ESI format specified by the demanding party within 30 days of being served with the discovery demand, or within 30 days of the parties' first Rule 26(f) conference if the demanding party delivers an "Early Rule 34

[7] Fed. R. Civ. P. 34(b)(2)(B), -(D).

Request" to the producing party.[8] If, after the producing party has raised objections to ESI format and the demanding party is not satisfied with the alternative ESI format suggested by the producing party, the parties must meet and confer under Rule 37(a)(2)(B) to try resolving the matter before the demanding party files a motion to compel.[9]

A party who neglects to timely and clearly object to a party's demand that ESI be produced in a particular format risks waiver of its objections, as illustrated in a recent court order from the Eastern District of California in *Morgan Hill Concerned Parents Association v. California Department of Education*. On the flipside, if a demanding party is not careful, its own actions may operate against waiver. In *Morgan Hill*, Plaintiff demanded that Defendant produce ESI in its native format with all metadata attached.[10] Although Defendant objected to nearly all of Plaintiff's document demands, it did not object to Plaintiff's native format demand. Defendant also neglected to propose an alternative ESI format per Rule 34(b)(2)(D). Ultimately, Defendant produced 29,000 documents, not in the native format specified by Plaintiff, but in a load file format without all the metadata. Plaintiff then moved to compel Defendant to produce the emails in native format.

The *Morgan Hill* court found Defendant first raised an objection, "of sorts," to Plaintiff's desired ESI format more than three years after Plaintiff initially served its document demands on Defendant.[11] Therefore, Defendant's objection was "untimely."[12] However, the Court also held an "outright waiver based *solely* upon timeliness of [Defendant's] objection [was] not warranted" because: (1) Plaintiff failed to argue in its Motion to Compel that Defendant waived objections to format; and (2) Plaintiff had on a previous occasion agreed to waive native format for the emails.[13] Ultimately, Defendant's objections notwithstanding, the Court granted Plaintiff's Motion to Compel. The Court rejected Defendant's argument that it would be too burdensome to re-produce 29,000 documents in Plaintiff's desired native format, as any inconvenience to Defendant was of its own making, namely for failing to object to native format ESI in the manner set forth in Fed. R. Civ. P. 34.

TAKEAWAYS

For producing/objecting parties:

Raise objections to the format of ESI clearly, with specificity, and within the timeframes set forth in Fed. R. Civ. P. 34(b)(2)(A).

[8] Fed. R. Civ. P. 34(b)(2)(A); 26(d)(2).
[9] *Morgan Hill Concerned Parents Assoc. v. Cal. Dep't of Edu.*, 2:11-cv-3471 KJM AC, 2017 LEXIS 14983, at *3 (E.D. Cal. Feb. 1, 2017) (quoting Fed. R. Civ. P. 34 advisory committee's note to 2006 Amendments).
[10] *Id.*, at *3.
[11] *Id.*
[12] *Id.* at *11.
[13] *Id.* at *11, 12.

For the party seeking to compel production of ESI:

Argue in your Motion to Compel that your opponent has waived all objections to your discovery demands by failing to timely and/or properly object to them. Plaintiff's failure to argue waiver in its Motion to Compel was one of the factors cited by the *Morgan Hill* court in declining to find an "outright waiver" of Defendant's objections.

Do not waffle on your discovery demands:

In *Morgan Hill,* Plaintiff conceded during discovery negotiations that Defendant could produce emails in non-native format. Plaintiff's waffling was the second factor cited by the *Morgan Hill* court in declining to find an "outright waiver" of Defendant's objection.

4. Amended FRE 902 Expands Self-Authentication to Certain Electronic Data

A recent amendment to Federal Rule of Evidence 902, effective December 17, 2017, allows electronic data recovered "by a process of digital identification" to be considered self-authenticating. Rule 902 lists a variety of documents and records that are presumed to be self-authenticating without additional evidence of authenticity. Previously, public records and other government documents, notarized documents, newspapers and periodicals, and records kept in the ordinary course of business were the only types of records considered to be self-authenticating. The newly added subsection (14) now adds electronic data collected through a process of digital identification to that list:

> **(14) Certified Data Copied from an Electronic Device, Storage Medium, or File.** Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent also must meet the notice requirements of Rule 902(11).

Now, data copied from an electronic device, storage medium or file will no longer require the trial testimony of a forensic or technical expert to provide evidence of authenticity. Instead, authenticity may now be established by submission of a written affidavit attested to by a "qualified person." The "qualified person" will often be the eDiscovery or information technology professional who collected the evidence and who can explain the process of digital identification applied to the records offered as evidence.

The Judicial Conference Advisory Committee explains in the amendment's accompanying notes that this change is intended to streamline the admission of electronic evidence where its foundation is not at issue, while providing a notice procedure whereby "the parties can determine in advance of trial whether a real challenge to authenticity will be made and can then plan accordingly."

The Committee goes on to say that the preferred way to satisfy the standard for self-authentication is through the production of "hash values" and confirmation of those values post-production: "A hash value is a number that is often represented as a sequence of characters and is produced by an algorithm based upon the digital contents of a drive, medium, or file . . . [i]f the hash values for the original and copy are the same, it is highly improbable that the original and copy are not identical." Therefore a "qualified person" can "reliably attest to the fact" that an original and copy with identical hash values are exact duplicates. While this is the preferred method of authentication, Rule 902 allows for other dependable methods of identification.

However, the benefits of self-authentication that accompany the digital identification and verification process can only be taken advantage of if data collection is performed by eDiscovery data collection and preservation means. Those parties who seek to admit evidence collected without observing best practices may encounter additional scrutiny. This is because the amendment discredits electronic evidence collection schemes that fail to utilize a defensible "digital identification" and verification process. Such schemes include custodian self-collection methods and "print screen"

methods for social media and website preservation and production. These methods will not receive the benefit of the presumption of self-authentication.

It is important to note that while properly certified electronic data will be afforded a strong presumption of authenticity, opposing parties may still object but they will bear the burden to rebut that presumption. This may require a party objecting to the authenticity of electronic evidence to engage a forensic technical expert to question the technical information about the system or process at issue. Also, it bears mentioning that as before, opposing parties may still object to admissibility on other grounds such as relevance or hearsay.

5. RULE 26(b)(1) and "Proportionality": How to make a winning argument in the context of eDiscovery.

Rule 26(b)(1) of the Federal Rules of Civil Procedure was amended December 1, 2015 to include a proportionality standard for obtaining discovery. The amendment also did away with the former "reasonably calculated to lead to the discovery of admissible evidence" standard. The amended Rule 26(b)(1) now reads as follows:

> *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.

Courts appear largely to view the 2015 amendment to Rule 26(b)(1) not so much as ushering in a new approach, but rather as a reaffirmation of proportionality's importance in defining the scope of discovery and as an invitation to the courts to "be more aggressive in identifying and discouraging discovery overuse."[14] Several post amendment decisions shed light on how courts are now evaluating proportionality in the context of eDiscovery and what constitute winning and losing arguments for parties seeking the court's intervention.

In *In re Namenda Direct Purchaser Antitrust Litig.*, No. 15 Civ. 7488 (CM) (JCF), 2017 U.S. Dist. LEXIS 173403 (S.D.N.Y. 2017), the court granted a party's motion to compel electronic records. The court analyzed the motion under the revised Rule 26(b)(1) and concluded that the requested information was proportional to the needs of the case. Among the factors considered by the court was the relatively low burden to the non-party to produce the documents, 150 hours of employee time at a cost of $10,000 to $15,000, relative to the value of the case. Tellingly, the court noted that although the non-party also claimed it would incur additional attorney expenses for privilege and objection review, it did not state how much those expenses would be. We can't know if things would have turned out differently had the non-party stated the value of the additional attorney expenses. However, at a minimum, *In re Namenda* shows that if you want the court to take costs into consideration in a Rule 26(b)(1) proportionality analysis, you better put a price tag on it.

On the other hand, as shown in *Oxbow Carbon & Minerals LLC v. Union Pacific Railroad Company*, 322 F.R.D. 1 (D.D.C. 2017), litigants who focus solely on the expense

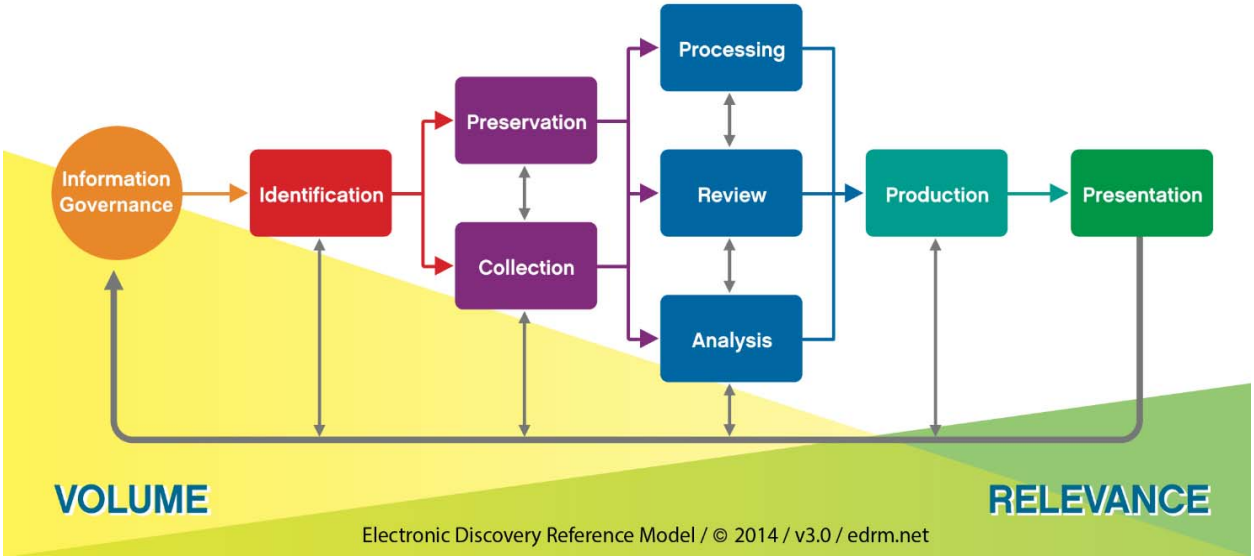
---

[14] *O'Garra v. Northwell Health*, CV No. 16-2191 (DRH)(AYS), 2018 LEXIS 9746, at *4, 5 (E.D.N.Y. January 22, 2018); *Winfield v. City of New York*, No. 15-cv-05236 (LTS) (KHP), 2018 LEXIS 56160, at *9 (S.D.N.Y. March 29, 2018) (quoting the advisory committee's note to the 2015 amendment to Fed. R. Civ. P 26); *Robertson v. People Magazine*, No. 14 Civ. 6759 (PAC), 2015 LEXIS 168525, at * 3, 4 (S.D.N.Y. December 16, 2015) ("[T]he 2015 amendment does not create a new standard; rather it serves to exhort judges to exercise their preexisting control over discovery more exactingly.")

of discovery efforts when making a proportionality argument may also find themselves on the losing side. In *Oxbow Carbon & Minerals,* plaintiffs claimed that the defendant railroads conspired to fix transportation rates forcing the plaintiffs to pay higher prices to ship their goods. During discovery, the defendant railroads sought the production of emails and documents from Oxbow's CEO, which Oxbow initially claimed would cost $250,000 to locate, review and produce. After applying agreed-upon search terms and technology-assisted review strategies to an initial sampling of the documents, that number was cut nearly in half. Oxbow produced the responsive documents identified from the sampling and review but refused to review the remaining documents claiming that the cost of producing the additional documents was not proportional to the needs of the case. The defendants filed a motion to compel.

In opposing the motion to compel, Oxbow focused solely on the burden and cost of the proposed review, asserting that this factor outweighed all other factors outlined in Rule 26. The court disagreed, considering each of the other factors and finding that they weighed in favor of granting the motion to compel. First, the court found that Oxbow itself had previously stressed the importance of the case and its potential widespread impact in multiple public comments. Second, the court found that the amount in controversy – anywhere between $50 million to $150 million – did not render the $142,000 discovery costs unreasonable by comparison. Third, the court found that the "information asymmetry" favored Oxbow, because Oxbow's CEO was in possession of relevant, unique information that could not be obtained from another source. Fourth, Oxbow's refusal to provide the requested discovery was, by Oxbow's admission, not based on an inability to pay the discovery costs. Fifth, Oxbow's CEO possessed important information regarding the company's finances and business strategies. Finally, the court noted that the burden and expense, taking all of the other proportionality factors into account, was not excessive, especially considering that Oxbow had already spent over $1.3 million reviewing and producing other documents.

Electronic Discovery Reference Model



Information Governance – Getting your electronic house in order to mitigate risk & expenses should e-discovery become an issue, from initial creation of ESI (electronically stored information) through its final disposition.

Identification – Locating potential sources of ESI & determining its scope, breadth & depth.

Preservation – Ensuring that ESI is protected against inappropriate alteration or destruction.

Collection – Gathering ESI for further use in the e-discovery process (processing, review, etc.).

Processing – Reducing the volume of ESI and converting it, if necessary, to forms more suitable for review & analysis.

Review – Evaluating ESI for relevance & privilege.

Analysis – Evaluating ESI for content & context, including key patterns, topics, people & discussion.

Production – Delivering ESI to others in appropriate forms & using appropriate delivery mechanisms.

Presentation – Displaying ESI before audiences (at depositions, hearings, trials, etc.), especially in native & near-native forms, to elicit further information, validate existing facts or positions, or persuade an audience.

GLOSSARY

Clustering - Grouping documents or other objects by similarity.

Document Family -A group of related documents that includes parent and child documents. For example, an email is a parent document and its attachments are its children.

Document Metadata – Data stored in a document about the document. Often this data is not immediately viewable in software application used to create/edit the document, but often can be accessed via a "properties" view. (For example: Last Accessed Date, Last Edited By, Users, etc.).

Duplicates - An exact duplicate of another document in a database. Duplicates typically arise when multiple document productions from separate sources are coded and contain copies of the same documents.

De-duplication - The process of determining which documents are duplicates. File systems can contain many copies of the same document, which need to be identified for efficiency's sake. Every time an email is sent it typically creates two additional copies of the email and its attachments, one in the sender's sent-items folder and once in the recipient's inbox. An email may also be sent to multiple recipients, thereby creating more copies.

Near Duplicate Detection – A term generally used to describe a method of grouping together "nearly identical" documents, typically used to reduce review costs, and to ensure consistent coding.

Early Case Assessment - A term generally used to describe a variety of tools or methods for investigating and quickly learning about a Document Collection for the purposes of estimating the risk(s) and cost(s) of pursuing a particular legal course of action.

Electronically Stored Information ("ESI") - Information created, manipulated, communicated, stored, and best utilized in digital form, requiring the use of computer hardware and software for access.

Email Threading - An email thread is a single email conversation that starts with an original email and includes all of the subsequent replies and forwards pertaining to that original email. Email threading greatly reduces the time and complexity of reviewing emails, by gathering all forwards, replies, and

reply-all messages together and isolating for review only those documents that contain unique content.

Hash Value - A unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of the data set. “Hashing” is used to guarantee the authenticity of an original data set and can be used as a digital equivalent of the Bates stamp used in paper document production.

Image File - A rendered image of a native file. An image is an exact copy of the original.

Keyword Searching - A common search technique that uses query words (“keywords”) and looks for them in ESI.

Native File - A native file is the true document or file. That is the original Word document, spreadsheet, or Outlook email as it was found on a computer or device in its native format.

Technology Assisted Review (“TAR”) – A process that combines human expertise with computer learning technologies to cull large amounts of data down to a reasonably sized review universe. Although there are variations, the TAR process generally involves attorneys reviewing a small set of data for responsiveness (or lack thereof) and other issues specific to the case, and then feeding this information to the TAR software. The software then propagates the human coding to the entire set of data to emulate decisions that the reviewing attorneys would make. In this manner, by using TAR, a large set of documents can be culled down to a much smaller and more manageable set consisting of the documents most likely to be responsive.

NOTE: The EDRM reference model, EDRM reference model definitions and glossary terms are provided by and/or adapted from EDRM (edrm.net).

NEW YORK RULES OF PROFESSIONAL CONDUCT

Effective April 1, 2009
As amended through January 1, 2017
With Commentary as amended through January 1, 2017

TABLE OF CONTENTS

Rule	Title	Page
1.0	Terminology	6
1.1	Competence	11
1.2	Scope of Representation and Allocation of Authority Between Client and Lawyer	14
1.3	Diligence	19
1.4	Communication	21
1.5	Fees and Division of Fees	24
1.6	Confidentiality of Information	29
1.7	Conflict of Interest: Current Clients	38
1.8	Current Clients: Specific Conflict of Interest Rules	49
1.9	Duties to Former Clients	60
1.10	Imputation of Conflicts of Interest	63
1.11	Special Conflicts of Interest for Former and Current Government Officials and Employees	69
1.12	Specific Conflicts of Interest for Former Judges, Arbitrators, Mediators, or Other Third-Party Neutrals	74
1.13	Organization as Client	77
1.14	Client with Diminished Capacity	82
1.15	Preserving Identity of Funds and Property of Others; Fiduciary Responsibility; Commingling and Misappropriation of Client Funds or Property; Maintenance of Bank Accounts; Record Keeping; Examination of Records	85
1.16	Declining or Terminating Representation	90
1.17	Sale of Law Practice	94
1.18	Duties to Prospective Clients	99
2.1	Advisor	103
2.2	[Reserved]	105
2.3	Evaluation for Use by Third Persons	106
2.4	Lawyer Serving as Third-Party Neutral	108
3.1	Non-Meritorious Claims and Contentions	110
3.2	Delay of Litigation	111

RULE 1.1:
COMPETENCE

(a) A lawyer should provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

(b) A lawyer shall not handle a legal matter that the lawyer knows or should know that the lawyer is not competent to handle, without associating with a lawyer who is competent to handle it.

(c) A lawyer shall not intentionally:

(1) fail to seek the objectives of the client through reasonably available means permitted by law and these Rules; or

(2) prejudice or damage the client during the course of the representation except as permitted or required by these Rules.

New York Rules of Professional Conduct [22 NYCRR 1200.0] Rule 1.1 Comment [8].

[8] To maintain the requisite knowledge and skill, a lawyer should (i) keep abreast of changes in substantive and procedural law relevant to the lawyer's practice, (ii) keep abreast of the benefits and risks associated with technology the lawyer uses to provide services to clients or to store or transmit confidential information, and (iii) engage in continuing study and education and comply with all applicable continuing legal education requirements under 22 N.Y.C.R.R. Part 1500.

RULE 5.3:
LAWYER'S RESPONSIBILITY FOR CONDUCT OF NONLAWYERS

(a) A law firm shall ensure that the work of nonlawyers who work for the firm is adequately supervised, as appropriate. A lawyer with direct supervisory authority over a nonlawyer shall adequately supervise the work of the nonlawyer, as appropriate. In either case, the degree of supervision required is that which is reasonable under the circumstances, taking into account factors such as the experience of the person whose work is being supervised, the amount of work involved in a particular matter and the likelihood that ethical problems might arise in the course of working on the matter.

(b) A lawyer shall be responsible for conduct of a nonlawyer employed or retained by or associated with the lawyer that would be a violation of these Rules if engaged in by a lawyer, if:

(1) the lawyer orders or directs the specific conduct or, with knowledge of the specific conduct, ratifies it; or

(2) the lawyer is a partner in a law firm or is a lawyer who individually or together with other lawyers possesses comparable managerial responsibility in a law firm in which the nonlawyer is employed or is a lawyer who has supervisory authority over the nonlawyer; and

(i) knows of such conduct at a time when it could be prevented or its consequences avoided or mitigated but fails to take reasonable remedial action; or

(ii) in the exercise of reasonable management or supervisory authority should have known of the conduct so that reasonable remedial action could have been taken at a time when the consequences of the conduct could have been avoided or mitigated.

New York Rules of Professional Conduct [22 NYCRR 1200.0] Rule 5.3 Comment [3].

[3] A lawyer may use nonlawyers outside the firm to assist the lawyer in rendering legal services to the client. Examples include (i) retaining or contracting with an investigative or paraprofessional service, (ii) hiring a document management company to create and maintain a database for complex litigation, (iii) sending client documents to a third party for printing or scanning, and (iv) using an Internet-based service to store client information. When using such services outside the firm, a lawyer or law firm must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the professional obligations of the lawyer and law firm. The extent of the reasonable efforts required under this Rule will depend upon the circumstances, including: (a) the education, experience and reputation of the nonlawyer; (b) the nature of the services involved; (c) the terms of any arrangements concerning the protection of client information; (d) the legal and ethical environments of the jurisdictions in which the services will be performed, particularly with regard to confidentiality; (e) the sensitivity of the particular kind of confidential information at issue; (f) whether the client will be supervising all or part of the nonlawyer's work. *See also* Rules 1.1 (competence), 1.2 (allocation of authority), 1.4 (communication with client), 1.6 (confidentiality), 5.4 (professional independence of the lawyer) and 5.5 (unauthorized practice of law). When retaining or directing a nonlawyer outside the firm, a lawyer should communicate directions appropriate under the circumstances to give reasonable assurance that the nonlawyer's conduct is compatible with the professional obligations of the lawyer.

NEW YORK STATE BAR ASSOCIATION

Serving the legal profession and the community since 1876

ETHICS OPINION 1020

New York State Bar Association
Committee on Professional Ethics

Opinion 1020 (9/12/2014)

Topic: Confidentiality; use of cloud storage for purposes of a transaction

Digest: Whether a lawyer to a party in a transaction may post and share documents using a "cloud" data storage tool depends on whether the particular technology employed provides reasonable protection to confidential client information and, if not, whether the lawyer obtains informed consent from the client after advising the client of the relevant risks.

Rules: 1.1, 1.6

FACTS

1. The inquirer is engaged in a real estate practice and is looking into the viability of using an electronic project management tool to help with closings. The technology would allow sellers' attorneys, buyers' attorneys, real estate brokers and mortgage brokers to post and view documents, such as drafts, signed contracts and building financials, all in one central place.

QUESTION

2. May a lawyer representing a party to a transaction use a cloud-based technology so as to post documents and share them with others involved in the transaction?

OPINION

3. The materials that the inquirer seeks to post, such as drafts, contracts and building financials, may well include confidential information of the inquirer's clients, and for purposes of this opinion we assume that they do.[1] Thus the answer to this inquiry hinges on whether use of the contemplated technology would violate the inquirer's ethical duty to preserve a client's confidential information.

4. Rule 1.6(a) contains a straightforward prohibition against the knowing disclosure of confidential information, subject to certain exceptions including a client's informed consent, and Rule 1.6(c) contains the accompanying general requirement that a lawyer "exercise reasonable care to prevent … [persons] whose services are utilized by the lawyer from disclosing or using confidential information of a client."

5. Comment [17] to Rule 1.6 addresses issues raised by a lawyer's use of technology:

> When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. The duty does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to use a means of communication or security measures not required by this Rule, or may give informed consent (as in an engagement letter or similar document) to the use of means or measures that would otherwise be prohibited by this Rule.

6. In the recent past, our Committee has repeatedly been asked to provide guidance on the interplay of technology and confidentiality. N.Y. State 1019 (2014) catalogues the Committee's opinions on technology. In that opinion, we considered whether a law firm could provide its lawyers with remote access to its electronic files. We concluded that a law firm could use remote access "as long as it takes reasonable steps to ensure that confidential information is maintained." *Id.* ¶12

7. Similarly, in N.Y. State 842 (2010), which considered the use of cloud data storage, we concluded that a lawyer could use this technology to store client records provided that the lawyer takes reasonable care to protect the client's confidential information. We also reached a similar conclusion in N.Y. State 939 (2012) as to the issue of lawyers from different firms sharing a computer system.

8. The concerns presented by the current inquiry were also present in N.Y. State 1019, N.Y. State 939 and N.Y. State 842, and those opinions govern the outcome here. That is, the inquirer may use the proposed technology provided that the lawyer takes reasonable steps to ensure that confidential information is not breached.[2] The inquirer must, for example, try to ensure that only authorized parties have access to the system on which the information is shared. Because of the fact-specific and evolving nature of technology, we do not purport to specify in detail the steps that will constitute reasonable care in any given set of circumstances. *See* N.Y. State 1019. ¶10. We note, however, that use of electronically stored information may not only require reasonable care to protect that information under Rule 1.6, but may also, under Rule 1.1, require the competence to determine and follow a set of steps that will constitute such reasonable care.[3]

9. Finally, we note that Rule 1.6 provides an exception to confidentiality rules based on a client's informed consent. Thus, as quoted in paragraph 5 above, a client may agree to the use of a technology that would otherwise be prohibited by the Rule. But as we have previously pointed out, "before requesting client consent to a technology system used by the law firm, the firm must disclose the risks that the system does not provide reasonable assurance of confidentiality, so that the consent is 'informed' within the meaning of Rule 1.0(j), i.e. that the client has information adequate to make an informed decision." N.Y. State 1019 ¶11.

CONCLUSION

10. Whether a lawyer for a party in a transaction may post and share documents using a "cloud" data storage tool depends on whether the particular technology employed provides reasonable protection to confidential client information and, if not, whether the lawyer obtains informed consent from the client after advising the client of the relevant risks.

(17-14)

[1]Rule 1.6(a) defines "confidential information" generally to include "information gained during or relating to the representation of a client, whatever its source, that is (a) protected by the attorney-client privilege, (b) likely to be embarrassing or detrimental to the client if disclosed, or (c) information that the client has requested be kept confidential."

[2]This result is consistent with results in other jurisdictions that have considered lawyers' use of off-site, third-party cloud services for storing and sharing documents. *See, e.g.,* ABA 95-398; Arizona Opinion 05-04; California Opinion 2010-179; Connecticut Inf. Opinion 2013-07; Florida Opinion 12-3 (2013); Illinois Opinion 10-01 (2009); Iowa Opinion 11-01; Maine Opinion 207 (2013); Massachusetts Opinion 12-03; Massachusetts Opinion 05-04; Missouri Inf. Opinion 2006-0092; Nebraska Opinion 06-05; New Hampshire Opinion 2012-13/4 (2013); New Jersey Opinion 701 (2006); North Carolina Opinion 2011-6 (2012); North Dakota Opinion 99-03 (1999); Ohio Opinion 2013-03; Oregon Opinion 2011-188; Pennsylvania Opinion 2011-200; Pennsylvania Opinion 2010-060; Vermont Opinion 2010-6 (2012); Washington Inf. Opinion 2215 (2012).

[3]It has been said for example that the duty of competence may require litigators, depending on circumstances, to possess a basic or even a more refined understanding of electronically stored information. *See, e.g.*, Zachary Wang, "Ethics and Electronic Discovery: New Medium, Same Problems," 75 Defense Counsel Journal 328, at 7 (October 2008) ("disclosure of privileged information as a result of a lack of knowledge of a client's IT system would subject an attorney to discipline under Rules 1.1 and 1.6"). The California State Bar Standing Committee on Professional Responsibility and Conduct has tentatively approved an interim opinion interpreting California ethical rules as follows:

> Attorney competence related to litigation generally requires, at a minimum, a basic understanding of, and facility with, issues relating to e-discovery, i.e., the discovery of electronically stored information ("ESI"). On a case-by-case basis, the duty of competence may require a higher level of technical knowledge and ability, depending on the e-discovery issues involved in a given matter and the nature of the ESI involved. … An attorney lacking the required competence for the e-discovery issues in the case at issue has three options: (1) acquire sufficient learning and skill before performance is required; (2) associate with or consult technical consultants or competent counsel; or (3) decline the client representation.

COPRAC Proposed Formal Opinion 11-0004 (2014).

One Elk Street, Albany , NY 12207
Phone: 518-463-3200 **Secure Fax:** 518.463.5993

THE STATE BAR OF CALIFORNIA
STANDING COMMITTEE ON
PROFESSIONAL RESPONSIBILITY AND CONDUCT
FORMAL OPINION NO. 2015-193

ISSUE: What are an attorney's ethical duties in the handling of discovery of electronically stored information?

DIGEST: An attorney's obligations under the ethical duty of competence evolve as new technologies develop and become integrated with the practice of law. Attorney competence related to litigation generally requires, among other things, and at a minimum, a basic understanding of, and facility with, issues relating to e-discovery, including the discovery of electronically stored information ("ESI"). On a case-by-case basis, the duty of competence may require a higher level of technical knowledge and ability, depending on the e-discovery issues involved in a matter, and the nature of the ESI. Competency may require even a highly experienced attorney to seek assistance in some litigation matters involving ESI. An attorney lacking the required competence for e-discovery issues has three options: (1) acquire sufficient learning and skill before performance is required; (2) associate with or consult technical consultants or competent counsel; or (3) decline the client representation. Lack of competence in e-discovery issues also may lead to an ethical violation of an attorney's duty of confidentiality.

AUTHORITIES INTERPRETED: Rules 3-100 and 3-110 of the Rules of Professional Conduct of the State Bar of California.[1/]

Business and Professions Code section 6068(e).

Evidence Code sections 952, 954 and 955.

STATEMENT OF FACTS

Attorney defends Client in litigation brought by Client's Chief Competitor in a judicial district that mandates consideration of e-discovery[2/] issues in its formal case management order, which is consistent with California Rules of Court, rule 3.728. Opposing Counsel demands e-discovery; Attorney refuses. They are unable to reach an agreement by the time of the initial case management conference. At that conference, an annoyed Judge informs both attorneys they have had ample prior notice that e-discovery would be addressed at the conference and tells them to return in two hours with a joint proposal.

In the ensuing meeting between the two lawyers, Opposing Counsel suggests a joint search of Client's network, using Opposing Counsel's chosen vendor, based upon a jointly agreed search term list. She offers a clawback agreement that would permit Client to claw back any inadvertently produced ESI that is protected by the attorney-client privilege and/or the work product doctrine ("Privileged ESI").

[1/] Unless otherwise indicated, all references to rules in this opinion will be to the Rules of Professional Conduct of the State Bar of California.

[2/] Electronically stored information ("ESI") is information that is stored in technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities (e.g., Code Civ. Proc., § 2016.020, sub. (d) – (e)). Electronic Discovery, also known as e-discovery, is the use of legal means to obtain ESI in the course of litigation for evidentiary purposes.

Attorney believes the clawback agreement will allow him to pull back anything he "inadvertently" produces. Attorney concludes that Opposing Counsel's proposal is acceptable and, after advising Client about the terms and obtaining Client's authority, agrees to Opposing Counsel's proposal. Judge thereafter approves the attorneys' joint agreement and incorporates it into a Case Management Order, including the provision for the clawback of Privileged ESI. The Court sets a deadline three months later for the network search to occur.

Back in his office, Attorney prepares a list of keywords he thinks would be relevant to the case, and provides them to Opposing Counsel as Client's agreed upon search terms. Attorney reviews Opposing Counsel's additional proposed search terms, which on their face appear to be neutral and not advantageous to one party or the other, and agrees that they may be included.

Attorney has represented Client before, and knows Client is a large company with an information technology ("IT") department. Client's CEO tells Attorney there is no electronic information it has not already provided to Attorney in hard copy form. Attorney assumes that the IT department understands network searches better than he does and, relying on that assumption and the information provided by CEO, concludes it is unnecessary to do anything further beyond instructing Client to provide Vendor direct access to its network on the agreed upon search date. Attorney takes no further action to review the available data or to instruct Client or its IT staff about the search or discovery. As directed by Attorney, Client gives Vendor unsupervised direct access to its network to run the search using the search terms.

Subsequently, Attorney receives an electronic copy of the data retrieved by Vendor's search and, busy with other matters, saves it in an electronic file without review. He believes that the data will match the hard copy documents provided by Client that he already has reviewed, based on Client's CEO's representation that all information has already been provided to Attorney.

A few weeks later, Attorney receives a letter from Opposing Counsel accusing Client of destroying evidence and/or spoliation. Opposing Counsel threatens motions for monetary and evidentiary sanctions. After Attorney receives this letter, he unsuccessfully attempts to open his electronic copy of the data retrieved by Vendor's search. Attorney hires an e-discovery expert ("Expert"), who accesses the data, conducts a forensic search, and tells Attorney potentially responsive ESI has been routinely deleted from Client's computers as part of Client's normal document retention policy, resulting in gaps in the document production. Expert also advises Attorney that, due to the breadth of Vendor's execution of the jointly agreed search terms, both privileged information and irrelevant but highly proprietary information about Client's upcoming revolutionary product were provided to Chief Competitor in the data retrieval. Expert advises Attorney that an IT professional with litigation experience likely would have recognized the overbreadth of the search and prevented the retrieval of the proprietary information.

What ethical issues face Attorney relating to the e-discovery issues in this hypothetical?

DISCUSSION

I. Duty of Competence

A. Did Attorney Violate The Duty of Competence Arising From His Own Acts/Omissions?

While e-discovery may be relatively new to the legal profession, an attorney's core ethical duty of competence remains constant. Rule 3-110(A) provides: "A member shall not intentionally, recklessly, or repeatedly fail to perform legal services with competence." Under subdivision (B) of that rule, "competence" in legal services shall mean to apply the diligence, learning and skill, and mental, emotional, and physical ability reasonably necessary for the performance of such service. Read together, a mere failure to act competently does not trigger discipline under rule 3-110. Rather, it is the failure to do so in a manner that is intentional, reckless or repeated that would result in a disciplinable rule 3-110 violation. (See *In the Matter of Torres* (Reviwe Dept. 2000) 4 Cal. State Bar Ct. Rptr. 138, 149 ("We have repeatedly held that negligent legal representation, even that amounting to legal malpractice, does not establish a [competence] rule 3-110(A) violation."); see also, *In the Matter of Gadda* (Review Dept. 2002) 4 Cal. State Bar Ct. Rptr. 416 (reckless and repeated acts); *In the Matter of Riordan* (Review Dept. 2007) 5 Cal. State Bar Ct. Rptr. 41 (reckless and repeated acts).)

Legal rules and procedures, when placed alongside ever-changing technology, produce professional challenges that attorneys must meet to remain competent. Maintaining learning and skill consistent with an attorney's duty of competence includes keeping "abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, . . ." ABA Model Rule 1.1, Comment [8].[3/] Rule 3-110(C) provides: "If a member does not have sufficient learning and skill when the legal service is undertaken, the member may nonetheless perform such services competently by 1) associating with or, where appropriate, professionally consulting another lawyer reasonably believed to be competent, or 2) by acquiring sufficient learning and skill before performance is required." Another permissible choice would be to decline the representation. When e-discovery is at issue, association or consultation may be with a non-lawyer technical expert, if appropriate in the circumstances. Cal. State Bar Formal Opn. No. 2010-179.

Not every litigated case involves e-discovery. Yet, in today's technological world, almost every litigation matter *potentially* does. The chances are significant that a party or a witness has used email or other electronic communication, stores information digitally, and/or has other forms of ESI related to the dispute. The law governing e-discovery is still evolving. In 2009, the California Legislature passed California's Electronic Discovery Act adding or amending several California discovery statutes to make provisions for electronic discovery. See, e.g., Code of Civil Procedure section 2031.010, paragraph (a) (expressly providing for "copying, testing, or sampling" of "electronically stored information in the possession, custody, or control of any other party to the action.")[4/] However, there is little California case law interpreting the Electronic Discovery Act, and much of the development of e-discovery law continues to occur in the federal arena. Thus, to analyze a California attorney's current ethical obligations relating to e-discovery, we look to the federal jurisprudence for guidance, as well as applicable Model Rules, and apply those principles based upon California's ethical rules and existing discovery law.[5/]

We start with the premise that "competent" handling of e-discovery has many dimensions, depending upon the complexity of e-discovery in a particular case. The ethical duty of competence requires an attorney to assess at the outset of each case what electronic discovery issues might arise during the litigation, including the likelihood that e-discovery will or should be sought by either side. If e-discovery will probably be sought, the duty of competence requires an attorney to assess his or her own e-discovery skills and resources as part of the attorney's duty to provide the client with competent representation. If an attorney lacks such skills and/or resources, the attorney must try to acquire sufficient learning and skill, or associate or consult with someone with expertise to assist. Rule 3-110(C). Attorneys handling e-discovery should be able to perform (either by themselves or in association with competent co-counsel or expert consultants) the following:

- initially assess e-discovery needs and issues, if any;
- implement/cause to implement appropriate ESI preservation procedures;[6/]

[3/] Although not binding, opinions of ethics committees in California should be consulted by members for guidance on proper professional conduct. Ethics opinions and rules and standards promulgated by other jurisdictions and bar associations may also be considered. Rule 1-100(A).

[4/] In 2006, revisions were made to the Federal Rules of Civil Procedure, rules 16, 26, 33, 34, 37 and 45, to address e-discovery issues in federal litigation. California modeled its Electronic Discovery Act to conform with mostly-parallel provisions in those 2006 federal rules amendments. (See Evans, *Analysis of the Assembly Committee on Judiciary regarding AB 5* (2009). (http://www.leginfo.ca.gov/pub/09-10/bill/asm/ab_0001-0050/ab_5_cfa_20090302_114942_asm_comm.html).)

[5/] Federal decisions are compelling where the California law is based upon a federal statute or the federal rules. (See *Toshiba America Electronic Components, Inc. v. Superior Court (Lexar Media, Inc.)* (2004) 124 Cal.App.4th 762, 770 [21 Cal.Rptr.3d 532]*; Vasquez v. Cal. School of Culinary Arts, Inc.* (2014) 230 Cal.App.4th 35 [178 Cal.Rptr.3d 10]; see also footnote 4, *supra.*)

[6/] This opinion does not directly address ethical obligations relating to litigation holds. A litigation hold is a directive issued to, by, or on behalf of a client to persons or entities associated with the client who may possess potentially relevant documents (including ESI) that directs those custodians to preserve such documents, pending further direction. See generally Redgrave, *Sedona Conference ® Commentary on Legal Holds: The Trigger and The Process* (Fall 2010) The Sedona Conference Journal, Vol. 11 at pp. 260 – 270, 277 – 279. Prompt issuance of a litigation hold may prevent spoliation of evidence, and the duty to do so falls on both the party and outside counsel working on the matter. See

- analyze and understand a client's ESI systems and storage;
- advise the client on available options for collection and preservation of ESI;
- identify custodians of potentially relevant ESI;
- engage in competent and meaningful meet and confer with opposing counsel concerning an e-discovery plan;
- perform data searches;
- collect responsive ESI in a manner that preserves the integrity of that ESI; and
- produce responsive non-privileged ESI in a recognized and appropriate manner.[7/]

See, e.g., *Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities, LLC* (S.D.N.Y. 2010) 685 F.Supp.2d 456, 462 – 465 (defining gross negligence in the preservation of ESI), (abrogated on other grounds in *Chin v. Port Authority* (2nd Cir. 2012) 685 F.3d 135 (failure to institute litigation hold did not constitute gross negligence per se)).

In our hypothetical, Attorney had a general obligation to make an e-discovery evaluation early, prior to the initial case management conference. The fact that it was the standard practice of the judicial district in which the case was pending to address e-discovery issues in formal case management highlighted Attorney's obligation to conduct an early initial e-discovery evaluation.

Notwithstanding this obligation, Attorney made *no* assessment of the case's e-discovery needs or of his own capabilities. Attorney exacerbated the situation by not consulting with another attorney or an e-discovery expert prior to agreeing to an e-discovery plan at the initial case management conference. He then allowed that proposal to become a court order, again with no expert consultation, although he lacked sufficient expertise. Attorney participated in preparing joint e-discovery search terms without experience or expert consultation, and he did not fully understand the danger of overbreadth in the agreed upon search terms.

Even after Attorney stipulated to a court order directing a search of Client's network, Attorney took no action other than to instruct Client to allow Vendor to have access to Client's network. Attorney did not instruct or supervise Client regarding the direct network search or discovery, nor did he try to pre-test the agreed upon search terms or otherwise review the data before the network search, relying on his assumption that Client's IT department would know what to do, and on the parties' clawback agreement.

After the search, busy with other matters and under the impression the data matched the hard copy documents he had already seen, Attorney took no action to review the gathered data until after Opposing Counsel asserted spoliation and threatened sanctions. Attorney then unsuccessfully attempted to review the search results. It was only then, at the end of this long line of events, that Attorney finally consulted an e-discovery expert and learned of the e-discovery problems facing Client. By this point, the potential prejudice facing Client was significant, and much of the damage already had been done.

At the least, Attorney risked breaching his duty of competence when he failed at the outset of the case to perform a timely e-discovery evaluation. Once Opposing Counsel insisted on the exchange of e-discovery, it became certain that e-discovery would be implicated, and the risk of a breach of the duty of competence grew considerably; this should have prompted Attorney to take additional steps to obtain competence, as contemplated under rule 3-110(C), such as consulting an e-discovery expert.

[Footnote Continued…]

Zubulake v. UBS Warburg LLC (S.D.N.Y. 2003) 220 F.R.D. 212, 218 and *Zubulake v. UBS Warburg LLC* (S.D.N.Y. 2004) 229 F.R.D. 422, 432. Spoliation of evidence can result in significant sanctions, including monetary and/or evidentiary sanctions, which may impact a client's case significantly.

[7/] This opinion focuses on an attorney's ethical obligations relating to his own client's ESI and, therefore, this list focuses on those issues. This opinion does not address the scope of an attorney's duty of competence relating to obtaining an opposing party's ESI.

Had the e-discovery expert been consulted at the beginning, or at the latest once Attorney realized e-discovery would be required, the expert could have taken various steps to protect Client's interest, including possibly helping to structure the search differently, or drafting search terms less likely to turn over privileged and/or irrelevant but highly proprietary material. An expert also could have assisted Attorney in his duty to counsel Client of the significant risks in allowing a third party unsupervised direct access to Client's system due to the high risks and how to mitigate those risks. An expert also could have supervised the data collection by Vendor.[8/]

Whether Attorney's acts/omissions in this single case amount to a disciplinable offense under the "intentionally, recklessly, or repeatedly" standard of rule 3-110 is beyond this opinion, yet such a finding could be implicated by these facts.[9/] See, e.g., *In the Matter of Respondent G.* (Review Dept. 1992) 2 Cal. State Bar Ct. Rptr. 175, 179 (respondent did not perform competently where he was reminded on repeated occasions of inheritance taxes owed and repeatedly failed to advise his clients of them); *In re Matter of Copren* (Review Dept. 2005) 4 Cal. State Bar Ct. Rptr. 861, 864 (respondent did not perform competently when he failed to take several acts in single bankruptcy matter); *In re Matter of Layton* (Review Dept. 1993) 2 Cal. State Bar Ct. Rptr. 366, 377 – 378 (respondent did not perform competently where he "recklessly" exceeded time to administer estate, failed to diligently sell/distribute real property, untimely settled supplemental accounting and did not notify beneficiaries of intentions not to sell/lease property).

B. Did Attorney Violate The Duty of Competence By Failing To Supervise?

The duty of competence in rule 3-110 includes the duty to supervise the work of subordinate attorneys and non-attorney employees or agents. See Discussion to rule 3-110. This duty to supervise can extend to outside vendors or contractors, and even to the client itself. See California State Bar Formal Opn. No. 2004-165 (duty to supervise outside contract lawyers); San Diego County Bar Association Formal Opn. No. 2012-1 (duty to supervise clients relating to ESI, citing *Cardenas v. Dorel Juvenile Group, Inc.* (D. Kan. 2006) 2006 WL 1537394).

Rule 3-110(C) permits an attorney to meet the duty of competence through association with another lawyer or consultation with an expert. See California State Bar Formal Opn. No. 2010-179. Such expert may be an outside vendor, a subordinate attorney, or even the client, if they possess the necessary expertise. This consultation or association, however, does not absolve an attorney's obligation to supervise the work of the expert under rule 3-110, which is a non-delegable duty belonging to the attorney who is counsel in the litigation, and who remains the one primarily answerable to the court. An attorney must maintain overall responsibility for the work of the expert he or she chooses, even if that expert is the client or someone employed by the client. The attorney must do so by remaining regularly engaged in the expert's work, by educating everyone involved in the e-discovery workup about the legal issues in the case, the factual matters impacting discovery, including witnesses and key evidentiary issues, the obligations around discovery imposed by the law or by the court, and of any relevant risks associated with the e-discovery tasks at hand. The attorney should issue appropriate instructions and guidance and, ultimately, conduct appropriate tests until satisfied that the attorney is meeting his ethical obligations prior to releasing ESI.

Here, relying on his familiarity with Client's IT department, Attorney assumed the department understood network searches better than he did. He gave them no further instructions other than to allow Vendor access on the date of the network search. He provided them with no information regarding how discovery works in litigation, differences

---

[8/] See Advisory Committee Notes to the 2006 Amendments to the Federal Rules of Civil Procedure, rule 34 ("Inspection or testing of certain types of electronically stored information or of a responding party's electronic information system may raise issues of confidentiality or privacy. The addition of testing and sampling to Rule 34(a) . . . is not meant to create a routine right of direct access to a party's electronic information system, although such access might be justified in some circumstances. Courts should guard against undue intrusiveness resulting from inspecting or testing such systems."). See also The Sedona Principles Addressing Electronic Document Production (2nd Ed. 2007), Comment 10(b) ("Special issues may arise with any request to secure direct access to electronically stored information or to computer devices or systems on which it resides. Protective orders should be in place to guard against any release of proprietary, confidential, or personal electronically stored information accessible to the adversary or its expert.").

[9/] This opinion does not intend to set or define a standard of care of attorneys for liability purposes, as standards of care can be highly dependent on the factual scenario and other factors not applicable to our analysis herein.

between a party affiliated vendor and a neutral vendor, what could constitute waiver under the law, what case-specific issues were involved, or the applicable search terms. Client allowed Vendor direct access to its entire network, without the presence of any Client representative to observe or monitor Vendor's actions. Vendor retrieved proprietary trade secret and privileged information, a result Expert advised Attorney could have been prevented had a trained IT individual been involved from the outset. In addition, Attorney failed to warn Client of the potential significant legal effect of not suspending its routine document deletion protocol under its document retention program.

Here, as with Attorney's own actions/inactions, whether Attorney's reliance on Client was reasonable and sufficient to satisfy the duty to supervise in this setting is a question for a trier of fact. Again, however, a potential finding of a competence violation is implicated by the fact pattern. See, e.g., *Palomo v. State Bar* (1984) 36 Cal.3d 785, 796 [205 Cal.Rptr. 834] (evidence demonstrated lawyer's pervasive carelessness in failing to give the office manager any supervision, or instruction on trust account requirements and procedures).

II. Duty of Confidentiality

A fundamental duty of an attorney is "[t]o maintain inviolate the confidence, and at every peril to himself or herself to preserve the secrets, of his or her client." (Bus. & Prof. Code, § 6068 (e)(1).) "Secrets" includes "information, other than that protected by the attorney-client privilege, that the client has requested be held inviolate or the disclosure of which would be embarrassing or would be likely to be detrimental to the client." (Cal. State Bar Formal Opinion No. 1988-96.) "A member shall not reveal information protected from disclosure by Business and Professions Code section 6068, subdivision (e)(1), without the informed consent of the client, or as provided in paragraph (B) of this rule." (Rule 3-100(A).)

Similarly, an attorney has a duty to assert the attorney-client privilege to protect confidential communications between the attorney and client. (Evid. Code, §§ 952, 954, 955.) In civil discovery, the attorney-client privilege will protect confidential communications between the attorney and client in cases of inadvertent disclosure *only if* the attorney and client act reasonably to protect that privilege. See *Regents of University of California v. Superior Court (Aquila Merchant Services, Inc.)* (2008) 165 Cal.App.4th 672, 683 [81 Cal.Rptr.3d 186]. This approach also echoes federal law. [10/] A lack of reasonable care to protect against disclosing privileged and protected information when producing ESI can be deemed a waiver of the attorney-client privilege. See *Kilopass Tech. Inc. v. Sidense Corp.* (N.D. Cal. 2012) 2012 WL 1534065 at 2 – 3 (attorney-client privilege deemed waived as to privileged documents released through e-discovery because screening procedures employed were unreasonable).

In our hypothetical, because of the actions taken by Attorney prior to consulting with any e-discovery expert, Client's privileged information has been disclosed. Due to Attorney's actions, Chief Competitor can argue that such disclosures were not "inadvertent" and that any privileges were waived. Further, non-privileged, but highly confidential proprietary information about Client's upcoming revolutionary new product has been released into the hands of Chief Competitor. Even absent any indication that Opposing Counsel did anything to engineer the overbroad disclosure, it remains true that the disclosure occurred because Attorney participated in creating overbroad search terms. All of this happened unbeknownst to Attorney, and only came to light after Chief Competitor accused Client of evidence spoliation. Absent Chief Competitor's accusation, it is not clear when any of this would have come to Attorney's attention, if ever.

The clawback agreement on which Attorney heavily relied may not work to retrieve the information from the other side. By its terms, the clawback agreement was limited to inadvertently produced Privileged ESI. Both privileged information, and non-privileged, but confidential and proprietary information, have been released to Chief Competitor.

[10/] See Federal Rules of Evidence, rule 502(b): "Inadvertent Disclosure. When made in a federal proceeding or to a federal office or agency, the disclosure does not operate as a waiver in a federal or state proceeding 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)."

Under these facts, Client may have to litigate whether Client (through Attorney) acted diligently enough to protect its attorney-client privileged communications. Attorney took no action to review Client's network prior to allowing the network search, did not instruct or supervise Client prior to or during Vendor's search, participated in drafting the overbroad search terms, and waited until after Client was accused of evidence spoliation before reviewing the data – all of which could permit Opposing Counsel viably to argue Client failed to exercise due care to protect the privilege, and the disclosure was not inadvertent.[11/]

Client also may have to litigate its right to the return of non-privileged but confidential proprietary information, which was not addressed in the clawback agreement.

Whether a waiver has occurred under these circumstances, and what Client's rights are to return of its non-privileged/confidential proprietary information, again are legal questions beyond this opinion. Attorney did not reasonably try to minimize the risks. Even if Client can retrieve the information, Client may never "un-ring the bell."

The State Bar Court Review Department has stated, "Section 6068, subdivision (e) is the most strongly worded duty binding on a California attorney. It requires the attorney to maintain 'inviolate' the confidence and 'at every peril to himself or herself' preserve the client's secrets." (See *Matter of Johnson* (Rev. Dept. 2000) 4 Cal. State Bar Ct. Rptr. 179.) While the law does not require perfection by attorneys in acting to protect privileged or confidential information, it requires the exercise of reasonable care. Cal. State Bar Formal Opn. No. 2010-179. Here, Attorney took only minimal steps to protect Client's ESI, or to instruct/supervise Client in the gathering and production of that ESI, and instead released everything without prior review, inappropriately relying on a clawback agreement. Client's secrets are now in Chief Competitor's hands, and further, Chief Competitor may claim that Client has waived the attorney-client privilege. Client has been exposed to that potential dispute as the direct result of Attorney's actions. Attorney may have breached his duty of confidentiality to Client.

CONCLUSION

Electronic document creation and/or storage, and electronic communications, have become commonplace in modern life, and discovery of ESI is now a frequent part of almost any litigated matter. Attorneys who handle litigation may not ignore the requirements and obligations of electronic discovery. Depending on the factual circumstances, a lack of technological knowledge in handling e-discovery may render an attorney ethically incompetent to handle certain litigation matters involving e-discovery, absent curative assistance under rule 3-110(C), even where the attorney may otherwise be highly experienced. It also may result in violations of the duty of confidentiality, notwithstanding a lack of bad faith conduct.

This opinion is issued by the Standing Committee on Professional Responsibility and Conduct of the State Bar of California. It is advisory only. It is not binding upon the courts, the State Bar of California, its Board of Trustees, any persons or tribunals charged with regulatory responsibilities, or any member of the State Bar.

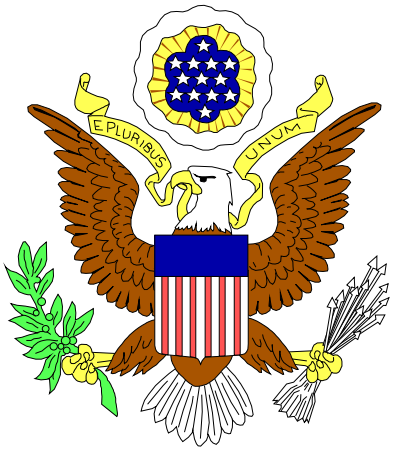
*[**Publisher's Note**: Internet resources cited in this opinion were last accessed by staff on June 30, 2015. Copies of these resources are on file with the State Bar's Office of Professional Competence.]*

[11/] Although statute, rules, and/or case law provide some limited authority for the legal claw back of certain inadvertently produced materials, even in the absence of an express agreement, those provisions may not work to mitigate the damage caused by the production in this hypothetical. These "default" claw back provisions typically only apply to privilege and work product information, and require both that the disclosure at issue has been truly inadvertent, and that the holder of the privilege has taken reasonable steps to prevent disclosure in the first instance. See Federal Rules of Evidence, rule 502; see also generally *State Compensation Insurance Fund v. WPS, Inc.* (1999) 70 Cal.App.4th 644 [82 Cal.Rptr.2d 799]; *Rico v. Mitsubishi Motors Corp.* (2007) 42 Cal.4th 807, 817 – 818 [68 Cal.Rptr.3d 758]. As noted above, whether the disclosures at issue in our hypothetical truly were "inadvertent" under either the parties' agreement or the relevant law is an open question. Indeed, Attorney will find even less assistance from California's discovery clawback statute than he will from the federal equivalent, as the California statute merely addresses the procedure for litigating a dispute on a claim of inadvertent production, and not the legal issue of waiver at all. (See Code Civ. Proc., § 2031.285.)

UNITED STATES DISTRICT COURT

FOR THE

WESTERN DISTRICT OF NEW YORK



LOCAL RULES OF CIVIL PROCEDURE
(Effective January 1, 2018)

(c) **Assessment of Jury Costs**. In any civil case in which a settlement is reached, or in which the Court is notified of settlement later than the close of business on the last business day before jurors are to appear for jury selection, the Court, in its discretion, may impose the Court's costs of compensating jurors for their needless appearance against one or more of the parties, or against one (1) or more counsel. Funds so collected shall be deposited by the Clerk of Court into the Treasury of the United States.

RULE 15

AMENDING PLEADINGS

(a) A movant seeking to amend or supplement a pleading must attach an unsigned copy of the proposed amended pleading as an exhibit to the motion. The proposed amended pleading must be a complete pleading superseding the original pleading in all respects. No portion of the prior pleading shall be incorporated into the proposed amended pleading by reference.

(b) Unless the movant is proceeding *pro se*, the amendment(s) or supplement(s) to the original pleading shall be identified in the proposed pleading through the use of a word processing "redline" function or other similar markings that are visible in both electronic and paper format.

(c) The granting of the motion does not constitute the filing of the amended pleading. Unless the order granting leave to amend or supplement contains a different deadline, the moving party must file and serve the amended pleading upon the existing parties within fourteen (14) days of entry of the order granting the motion. Service upon any new parties must be completed in accordance with Fed.R.Civ.P. 4(m). If the moving party is proceeding *pro se*, the Clerk of Court will file the amended pleading upon granting of the motion.

RULE 16

ALTERNATIVE DISPUTE RESOLUTION AND PRETRIAL CONFERENCES

(a) **Alternative Dispute Resolution**. This Court has adopted an Alternative Dispute Resolution Plan ("ADR"), as implemented by Standing Order, under which certain civil cases are referred automatically to ADR upon filing. A copy of the Plan is available on the Court's website, http://www.nywd.uscourts.gov. The Clerk of Court will provide notice to the parties when a case is automatically referred. Any civil case that is not automatically referred may be referred to ADR by order of the presiding Judge, in their discretion. The ADR process is confidential. Litigants in cases not referred automatically to ADR must consider possible agreement to the use of an ADR process.

(b) **Initial Pretrial Conference**.

(1) **Purpose**. The Court shall hold an initial pretrial conference in all cases except those exempted from initial disclosure requirements under Fed.R.Civ.P. 26(a)(1)(B). The purpose of this conference is to establish a case management plan.

(2) **Party Conference**. Prior to the initial pretrial conference, counsel for all parties and any *pro se* litigants shall confer as required by Fed.R.Civ.P. 26(f), and shall file with the Court a joint, written discovery plan consistent with Fed.R.Civ.P. 26(f). If they are unable to agree to a plan, each party shall file its own proposed plan.

(A) **Electronically Stored Information**. The Court expects the parties to cooperatively reach agreement on how to preserve and conduct discovery of electronically stored information ("ESI").[1] Prior to the Fed.R.Civ.P. 26(f) conference, counsel should become knowledgeable about their clients' information management systems and their operation, including how information is stored and retrieved. In addition, counsel should make a reasonable attempt to ascertain the contents of their client's ESI, including backup, archival, and legacy data (outdated formats or media) and ESI that may not be reasonably accessible. In particular, prior to or at the Fed.R.Civ.P. 26(f) conference, the parties should confer regarding the following matters:

(i) **Preservation**. Counsel should attempt to agree on steps the parties will take to segregate and preserve ESI in order to avoid accusations of spoliation.

(ii) **E-mail Information**. Counsel should attempt to agree on the scope of e-mail discovery and e-mail search protocol.

(iii) **Back-up and Archival Data**. Counsel should attempt to agree on whether responsive back-up and archival data exists, the extent to which back-up and archival data is reasonably accessible, and who will bear the cost of obtaining such data.

(iv) **Format and Media**. Counsel should attempt to agree on the format and media to be used in the production of ESI, and whether production of some or all ESI in paper form is agreeable in lieu of production in electronic format.

---

[1]Except for the term "document," which is defined at L.R.Civ.P. 26(d)(3)(B), the Court will rely on The Sedona Conference Glossary: E-Discovery & Digital Information Management (Second Edition), for definitions of terms related to discovery of ESI.

(v) **Reasonably Accessible Information and Costs**. Counsel should attempt to determine if any responsive ESI is not reasonably accessible, *i.e.*, is accessible only by incurring undue burdens or costs.

(B) **Privileged or Trial Preparation Materials.** Counsel also should attempt to reach agreement regarding what will happen in the event privileged or trial preparation materials are inadvertently disclosed.

(3) **Content of the Initial Conference**. In addition to all of the matters in Fed.R.Civ.P. 16(c)(2), counsel and unrepresented parties shall be prepared to discuss meaningfully the following:

(A) if the case is referred automatically to ADR pursuant to the Court's Alternative Dispute Resolution Plan, selection of a neutral, and timing for ADR;

(B) if the case is not referred automatically to ADR, possible stipulation to the use of a confidential ADR process;

(C) any problems currently known and reasonably anticipated to arise in connection with discovery of ESI;

(D) proposed methods to limit and/or decrease the time and expense of discovery;

(E) the use of experts during discovery and at trial; and

(F) the possibility of consent to the Magistrate Judge conducting all or part of the proceedings in a case provided, however, that unless there is unanimous consent among the parties, no party shall discuss its position with the Court.

(4) **Scheduling Order**. After the initial pretrial conference, pursuant to Fed.R.Civ.P. 16(b), the Court shall issue an order providing:

(A) deadlines for joinder of parties and amendment of pleadings;

(B) a date for a first judicial settlement conference, or, if the case will proceed to ADR, deadlines for an initial ADR session and the conclusion of ADR;

(C) a discovery cut-off date;

(D) a deadline for filing dispositive motions;

(E) deadlines for the disclosure of expert witnesses, if applicable; and

NEW YORK STATE
Unified Court System
OFFICE OF COURT ADMINISTRATION

LAWRENCE K. MARKS
CHIEF ADMINISTRATIVE JUDGE

JOHN W. McCONNELL
COUNSEL

MEMORANDUM

March 8, 2018

To: All Interested Persons

From: John W. McConnell

Re: Request for Public Comment on Proposed Amendment of Rule 11-e of the Rules of the Commercial Division (22 NYCRR §202.70[g], Rule 11-e), to Address Technology-Assisted Review in Discovery

==========

The Administrative Board of the Courts is seeking public comment on a proposed amendment of Rule 11-e of the Rules of the Commercial Division (22 NYCRR §202.70[g], Rule 11-e), proffered by the Commercial Division Advisory Council, to include the following language addressing technology-assisted review in discovery (Exh. A, pp. 2-3):

> The parties are encouraged to use the most efficient means to review documents, including electronically stored information ("ESI"), that is consistent with the parties' disclosure obligations under Article 31 of the CPLR and proportional to the needs of the case. Such means may include technology-assisted review, including predictive coding, in appropriate cases.

As described in the Council's explanatory memorandum (Exh. A), the goal of this amendment is to encourage parties and the court, in considering appropriate discovery techniques for electronically-stored information, to include increasingly common practices such as keyword searching, concept searching, email threading, near-duplicate identification. clustering, and predictive coding (Exh. A, pp. 3-4). Although the rule would not prescribe use of particular ESI discovery techniques, the Council believes that its adoption "would make clear that the Commercial Division is sensitive to the cost of document review in complex commercial cases and is in line with other courts, including other centers of high-stakes commercial litigation such as the Southern District and the Delaware Chancery Court, in supporting the use of technology-assisted review … in appropriate cases" (Exh. A. p. 6).

==========

Persons wishing to comment on the proposed rule should e-mail their submissions to rulecomments@nycourts.gov or write to: John W. McConnell, Esq., Counsel, Office of Court Administration, 25 Beaver Street, 11th Fl., New York, New York 10004. **Comments must be received no later than May 15, 2018.**

All public comments will be treated as available for disclosure under the Freedom of Information Law and are subject to publication by the Office of Court Administration. Issuance of a proposal for public comment should not be interpreted as an endorsement of that proposal by the Unified Court System or the Office of Court Administration.

EXHIBIT A

MEMORANDUM

TO: Commercial Division Advisory Council

FROM: Subcommittee on Procedural Rules to Promote Efficient Case Resolution ("Subcommittee")

DATE: December 11, 2017

RE: Proposal for a Rule Concerning the Use of Technology-Assisted Review in Discovery

---

INTRODUCTION

It is generally agreed that the most expensive stage of complex commercial litigation today is document review. A 2012 RAND study found that document review consumes on average 73% of the total cost of document production in cases involving electronic discovery, notwithstanding such common economies as the use of vendors to do first-level document review.[1] Conducting this resource-intensive stage of litigation in the most efficient manner consistent with defensible results is therefore in the best interest of both litigants and the judicial system. Sophisticated litigants know that the use of technology-assisted review—of which there are many types, ranging from widely used software tools like keyword searching to more sophisticated algorithmic technologies such as predictive coding—can yield substantial cost savings, as well as streamline and accelerate document review and production. The courts of New York State thus would be well-advised to encourage parties to consider the use of technology-assisted review in appropriate cases to speed discovery and reduce its cost.

---

[1] NICHOLAS M. PACE & LAURA ZAKARAS, RAND INST. FOR CIVIL JUSTICE, WHERE THE MONEY GOES: UNDERSTANDING LITIGANT EXPENDITURES FOR PRODUCING ELECTRONIC DISCOVERY, at xv-xvi, 25-27, 41 (2012).

Although technology-assisted review has been available for years, neither the CPLR nor, for that matter, the Federal Rules of Civil Procedure address whether, in what circumstances, or how a party may use technology-assisted review to fulfill its disclosure obligations. In the federal courts, however, the judiciary has provided some guidance through decisions addressing e-discovery issues. In contrast, the New York State courts—including in the Commercial Division, where the costs of document review are likely to be most burdensome—have provided little analogous guidance.

To fill that gap, the Subcommittee proposes a new rule for the Commercial Division addressing technology-assisted review. The proposed rule would do no more than to confirm that technology-assisted review is a legitimate disclosure tool that parties may make use of in appropriate cases, as many are already doing, and that, as with any other document review, the producing party is best situated to determine in the first instance whether and how to use technology-assisted review. The proposed rule would not limit in any way the presiding justice's oversight of the discovery process, nor would it endorse or require any particular kind of technology-assisted review. By supporting the use of technology-assisted review in appropriate cases, however, the proposed rule would make clear that the Commercial Division is receptive to technological innovations that lessen the burdens and cost of complex litigation.

THE PROPOSED RULE

The proposed rule, which might be incorporated as a subpart of current Rule 11-e of the Rules of the Commercial Division, would read as follows:

The parties are encouraged to use the most efficient means to review documents, including electronically stored information ("ESI"), that is consistent with the

parties' disclosure obligations under Article 31 of the CPLR and proportional to the needs of the case. Such means may include technology-assisted review, including predictive coding, in appropriate cases.

DISCUSSION

Background. Litigants in complex commercial cases today use a wide range of technology-assisted review techniques to facilitate the review of what is often an enormous volume of electronically stored information ("ESI"). In such document-intensive cases, human review of each and every collected document for responsiveness can be slower, more costly, and less accurate than the appropriate use of technology-assisted review,[2] which relies on software to help identify potentially irrelevant documents for culling from a large data set, to group together similar documents so as to promote efficient review and consistency of results, or to "teach" a computer to recognize those documents that are most likely to be responsive.

The threshold challenge faced in reviewing a large volume of ESI is that most ESI is unstructured, meaning that it is not organized in any predetermined way. The most common example of unstructured data in the disclosure context is email, which has few predetermined data fields and typically is stored without regard to subject matter. Review of ESI thus often begins by collecting a large volume of unstructured ESI, frequently limited only by custodian and date range, and then running a *keyword search*, which uses software to identify words or phrases that are likely to be found in responsive

[2] *See, e.g., id.* at 55-58, 61-69.

documents, to identify the documents to be reviewed.[3] A more sophisticated variant is *concept searching*, which uses advanced technology to identify documents incorporating concepts similar to the specific search terms used.[4]

The efficiency of the ensuing review and consistency of results can be enhanced through techniques to group similar or related documents together, such as *email threading*, which packages together email strings and any attachments as one chronological thread;[5] *near-duplicate identification*, which groups together similar documents based on their textual similarities (*e.g.*, different drafts of a document);[6] and *clustering*, which uses conceptual analytics technology to group and categorize similar documents.[7]

While these common techniques can help to cull a data set and organize it for review, none of them obviates the need for human review for responsiveness. The form of technology-assisted review generally referred to as *predictive coding* purports, however, to do just that. Predictive coding uses a "machine learning algorithm to distinguish relevant from non-relevant documents, based on subject matter experts'

---

[3] *See, e.g.*, THE SEDONA CONFERENCE, COMMENTARY ON DEFENSE OF PROCESS: PRINCIPLES AND GUIDELINES FOR DEVELOPING AND IMPLEMENTING A SOUND E-DISCOVERY PROCESS 25 (Public Comment Version, 2016).

[4] *See, e.g.*, *Concept Searching*, RELATIVITY.COM, https://www.relativity.com/relativity/Portals/0/Documents/8.0%20Documentation%20Help%20Site/Content/Features/Analytics/Concept%20searching.htm (last visited Nov. 29, 2017).

[5] *See* Nik Balepur, *5 Email Threading Facts That May Surprise You*, THE RELATIVITY BLOG (Apr. 16, 2015), http://blog.kcura.com/relativity/blog/5-email-threading-facts-that-may-surprise-you.

[6] D4, *Near-Duplicate Detection Finds Documents No One Thought Could be Found*, D4 CASE STUDIES BLOG (June 11, 2015), http://d4discovery.com/discover-more/near-duplicate-detection-finds-documents-no-one-thought-could-be-found#sthash.tI5DevpH.dpbs; EQUIVIO, CHOOSING A NEAR-DUPLICATE IDENTIFICATION SOLUTION (2012), http://www.equivio.com/files/files/White%20Paper%20-%20Choosing%20A%20Near-Duplicate%20Identification%20Solution.pdf.

[7] *Document Clustering for eDiscovery Review*, CLOUDNINE, https://www.ediscovery.co/legacy/document-clustering/(last visited Nov. 29, 2017).

coding of a training set of documents."[8] Predictive coding uses computers to extrapolate human judgments about responsiveness, based on human review of a sample "seed set" or "training set" of documents, across the remaining document collection.[9] Because predictive coding requires an upfront investment of time in "teaching" the computer to recognize the characteristics of responsive documents, it generally is cost-effective only when dealing with a large volume of unstructured ESI, but in those circumstances it has the potential to enhance the speed, accuracy, and cost-effectiveness of document review.[10]

Rationale for the Proposed Rule. Both federal and state courts have endorsed the use of technology-assisted review. The United States District Court for the Southern District of New York, for example, has noted that "[p]redictive coding is an automated method that credible sources say has been demonstrated to result in more accurate searches at a fraction of the cost of human reviewers." *Chevron Corp.* v. *Donziger*, 11-CV-0691, 2013 WL 1087236, at *32 n.255 (S.D.N.Y. March 15, 2013). Indeed, the Delaware Chancery Court has actually required parties to use predictive coding. *EORHB, Inc., et al.* v. *HOA Holdings, LLC, et al.*, No. 7409, 2012 WL 4896670 (Del. Ch. Ct. Oct. 15, 2012). Courts have noted in particular the utility of predictive coding for reviewing a large volume of ESI. In the Southern District, for example, Magistrate Judge Andrew Peck has observed that "computer-assisted review is an

---

[8] *The Grossman-Cormack Glossary of Technology-Assisted Review*, 7 FED. COURTS L. REV. 8, 26 (2013) (capitals omitted).

[9] *Id.* at 29, 32-33. Other implementations of predictive coding use a "Continuous Active Learning" model in which the computer "learns" while humans review documents, allowing for the re-classification of documents as the software continuously evolves its "understanding."

[10] JOHN TREDENNICK ET AL., TAR FOR SMART PEOPLE: HOW TECHNOLOGY ASSISTED REVIEW WORKS AND WHY IT MATTERS FOR LEGAL PROFESSIONALS 35-41 (2016).

available tool and should be seriously considered for use in large-data-volume cases." *Moore* v. *Publicis Groupe*, 287 F.R.D. 182, 193 (S.D.N.Y. 2012). Another federal district court has granted a plaintiff's request, over the defendant's objection, to use predictive coding to review approximately 2 million documents for responsiveness. *See Bridgestone Ams., Inc.* v. *Int'l Bus. Machs. Corp.*, No. 3:13-1196, 2014 WL 4923014, at *1 (M.D. Tenn. 2014). Foreign courts have likewise recognized the utility of predictive coding in reviewing large volumes of ESI. *See, e.g., Irish Bank Resolution Corp. Ltd & ors* v. *Quinn &* ors, [2015] IEHC 175 (Ir.); *Brown* v. *BCA Trading Ltd.*, [2016] EWHC 1464 (Ch) (Eng.); *Pyrrho Invs. Ltd.* v. *MWB Prop. Ltd.*, [2016] EWHC 256 (Ch) (Eng.).

The proposed rule would make clear that the Commercial Division is sensitive to the cost of document review in complex commercial cases and is in line with other courts, including other centers of high-stakes commercial litigation such as the Southern District and the Delaware Chancery Court, in supporting the use of technology-assisted review, including predictive coding, in appropriate cases. The proposed rule would not, however, prescribe whether or when any particular form of technology-assisted review may or should be used. These technologies are evolving at a rapid rate, so that any effort to prescribe permissible or impermissible methodologies would quickly become obsolete, and in any event the appropriateness of a given methodology can only be determined in the context of the particular case and the data set to be reviewed. Nothing in the proposed rule is intended to limit the role of the presiding justice in supervising document disclosure, *see* CPLR 3104(a), or to insulate the responding party's production from challenge, *see* CPLR 3124.

Need for Proportionality. Regardless of the method a party uses to review a large collection of ESI for responsiveness, the result will not be perfect. "There simply is no review tool that guarantees perfection. . . . [T]here are risks inherent in any method of reviewing electronic documents." *Moore* v. *Publicis Groupe*, 11-CV-1279, 2012 WL 1446534, at *3 (S.D.N.Y Apr. 26, 2012) (affirming Magistrate Judge Peck's acceptance of predictive coding). Courts have recognized that the standard for a review, whether technology-assisted or entirely human, "is not perfection, or using the 'best' tool, but whether the search results are reasonable and proportional." *Hyles* v. *N.Y. City*, 10-CV-3119, 2016 WL 4077114, at *3 (S.D.N.Y. Aug. 1, 2016). "The goal is for the review method to result in higher recall and higher precision than another review method, at a cost proportionate to the 'value' of the case." *Moore*, 287 F.R.D. at 190.

This concept of proportionality is embedded in the Commercial Division Rules. The Preamble to the Rules provides: "The Commercial Division is mindful of the need to conserve client resources, *encourage proportionality in discovery*, promote efficient resolution of matters, and increase respect for the integrity of the judicial process" (emphasis added). Consistent with these principles, the CPLR limits the scope of disclosure to "all matter *material and necessary* in the prosecution or defense of an action." CPLR 3101(a) (emphasis added). Federal procedure is aligned with the CPLR and the Commercial Division Rules in this respect; the Federal Rules of Civil Procedure similarly limit discovery to that which is "proportional to the needs of the case."[11]

[11] Fed. R. Civ. P. 26(b)(1) limits the "scope of discovery" to "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 discovery in resolving the issues, *and whether the burden or expense of the proposed discovery outweighs its likely benefit*" (emphases added).

Accordingly, it should not be a legitimate objection to a party's use of predictive coding or other technology-assisted review that the chosen method may not deliver perfect results. If the methodology chosen is reasonable in the circumstances—that is, "if the burden of identifying additional ESI outweighs the need for [additional] discovery and its importance in resolving the issues in dispute"—then it should be deemed sufficient to meet a party's disclosure obligations.[12] To underscore this principle, the proposed rule incorporates proportionality as a relevant consideration in determining the appropriateness of a document review method.

Parties Encouraged to Cooperate. Because the responding party knows best what kinds and volume of documents it has, how they are stored, and what it will cost to review them, "[r]esponding parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own electronically stored information." *Hyles* v. *N.Y. City*, 10-CV-3119, 2016 WL 4077114, at *3 (S.D.N.Y. Aug. 1, 2016) (quoting THE SEDONA CONFERENCE, THE SEDONA PRINCIPLES: SECOND EDITION BEST PRACTICES RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION, at Principle 6 Illustration i (2d ed. 2007), *available at* www.thesedonaconference.org). "Unless [the responding party's] choice is manifestly unreasonable or the requesting party demonstrates that the resulting production is deficient, the court should play no role in dictating the design of the search." *Mortg. Resolution Servicing, Inc.* v. *JPMorgan Chase Bank, N.A.*, 15-CV-0293, 2017 WL 2305398, at *2 (S.D.N.Y. May 18, 2017).

---

[12] *See id.*

The proposed rule makes clear that, while the responding party is best placed to analyze in the first instance what it believes to be the most efficient means to review its own documents, including ESI, subject to its disclosure obligations under the CPLR, parties are well advised to confer and agree on an appropriate approach to document review, and the proposed rule encourages them to do so. The proposed rule encourages the responding party to consider the most efficient means to meet its obligations, including technology-assisted review where appropriate, but it does not prevent the requesting party from challenging those means as inadequate or a production as incomplete, nor does the proposed rule constrain in any way the presiding justice's oversight of the disclosure process.

CONCLUSION

The proposed rule would simply align the Commercial Division with those courts, state and federal, that have had occasion to consider the appropriate use of technology-assisted review to promote efficiency and proportionality, consistent with the responding party's disclosure obligations. The proposed rule would reserve to the presiding justice, however, the power to determine whether in the circumstances of a particular case a responding party has met its disclosure obligations.

IN THE COURT OF CHANCERY OF THE STATE OF DELAWARE

Plaintiff, v. Defendants.	Case No. xxxxxxxxxxx

ELECTRONIC DISCOVERY PROTOCOL

After conferring on these matters, Plaintiff ("Plaintiff") and Defendants ("Defendants") in the above-captioned action (collectively, the "Parties," and individually, a "Party"), by and through their undersigned counsel, hereby stipulate and agree to this Electronic Discovery Protocol ("EDP" or "Protocol").

A. General Terms

1. Application. The procedures set forth in this Protocol shall govern the production of "documents" and "electronically stored information" (as those terms are used in the Rules of the Court of Chancery of the State of Delaware ("Chancery Court

Rules") and other applicable court rules or orders) that are stored in electronic format, including paper documents that have been converted to an electronic format either prior to or in connection with the litigation (collectively, "ESI") in the above captioned action (the "Litigation"). For purposes of this Protocol, the Party requesting production of ESI shall be referred to as the "Requesting Party," and the Party producing ESI in response to such requests shall be referred to as the "Producing Party." Nothing in this Protocol shall be construed to alter the Producing Party's rights arising under applicable law or otherwise to withhold production of ESI because, for example, the source of the ESI is not reasonably accessible or its production would be unduly burdensome or duplicative.

2. Subject Matter and Scope of Discovery. This Protocol does not establish any agreement as to either the appropriate temporal or subject matter scope of discovery in the Litigation.

3. Reservation of Rights. All Parties reserve all rights under applicable law for matters relating to the production of ESI that are not specifically addressed in this Protocol, including the right to object to production of any ESI.

4. Confidentiality. All ESI, including the procedure for clawback of any ESI, shall be governed by any confidentiality, protective, and/or clawback orders entered in this Litigation. Responsive documents in TIFF format will be stamped with the appropriate confidentiality designation in accordance with the Stipulation and Order for the Production and Exchange of Confidential Information ("Confidentiality

Order") in this Litigation. Each responsive document produced in native format will have its confidentiality designation identified in the filename of the native file.

5. Security. The Parties will make reasonable efforts to ensure that any productions made are free from viruses and provided on encrypted media.

B. General Document Production Procedures

1. Format. For all ESI that are not spreadsheet files (*e.g.*, Microsoft Office Excel files) or presentation files (*e.g.*, Microsoft Office PowerPoint files), the Producing Party shall produce ESI in single-page TIFF image files with at least 300 dots per inch (dpi) ("TIFF format"). Each TIFF image file should be one page and named according to the unique Bates number, followed by the extension ".TIF." Each image shall be branded according to the Bates number and its confidentiality designation pursuant to the Confidentiality Order entered in this action. Original document orientation should be maintained (*i.e.*, portrait to portrait and landscape to landscape).

Nothing herein shall preclude the Producing Party from also producing ESI in native format, or the Requesting Party from requesting, upon a showing of good cause, that certain ESI also be produced in native format, whereupon such request will not be unreasonably denied. For TIFF files generated from native format, the Producing Party shall provide extracted and word searchable text files. Along with each TIFF file, the Producing Party shall provide searchable metadata and corresponding text (as required by Exhibit A, hereto) that is functionally equivalent to

the metadata and text available in the native file before processing. For ESI that constitutes spreadsheet or presentation files (*e.g.*, ESI with file types .xls, .ppt, .xlsx, or .pptx), the Producing Party shall produce the ESI in native format, unless the material must be redacted prior to production, in which case the Producing Party shall produce the ESI in TIFF format as outlined above.

2. Production Media. The Producing Party may produce ESI (i) on readily accessible computer or electronic media, including without limitation CD-ROM, DVD, external hard drive (with standard PC-compatible interface), (ii) via secure, password-protected File Transfer Protocol, or (iii) by such other media as the Parties may agree upon ("Production Media"). The Producing Party shall affix a unique identifying label to each piece of Production Media, which shall identify the date of the production, the producing party, and the Bates range for the materials being produced.

3. Preservation of Original Documents. The Producing Party shall retain a copy of all ESI gathered and produced in this Litigation (including a copy of any documents that were gathered and ultimately withheld from production) until the Litigation is complete. The Producing Party shall take reasonable measures to maintain such copies in a manner so as to preserve the metadata associated with these electronic materials as they existed in the ordinary course of business and at the time of collection.

4. Related Documents. If a file or document attaches another file or document (such as an icon indicating an email attachment) then the referenced document will be considered for purposes of this protocol as a "Related Document." A link in a document (to a web site, internal file, etc.) is not considered a "Related Document" for purposes of this Protocol. To the extent technologically feasible, the Producing Party shall produce all attached files, however referenced in the parent document, with the attachment immediately following the parent document in sequential order, while maintaining the relationship between the parent file and each of its attachments. In the event the Producing Party discovers that the production of related documents as provided in this Paragraph is not technologically feasible for any category of ESI, the Producing Party will notify the Requesting Party and the Parties will meet and confer to discuss such ESI.

5. De-Duplication. Where practicable, the Producing Party shall endeavor to de-duplicate documents within and across its production custodians and produce one version of the document. If there is any handwriting or other alteration of a document, it shall not be considered a duplicate under this provision.

C. TIFF Production Procedures

1. Creation of TIFF Files. The Producing Party shall (i) create single page group IV TIFF files of electronic documents (absent reasonable exceptions that must be discussed between the Parties prior to production, the Producing Party may not create TIFF files of electronic documents by printing out paper copies of the

electronic documents and then scanning those paper copies); and (ii) create TIFF files of paper documents by, where reasonably practicable, scanning the original paper documents or a copy of the original paper documents that is as legible as the original. Each TIFF shall be endorsed with a unique document identifier (*e.g.*, a Bates stamp number).

2. OCR. For TIFF files created from paper-based documents, the Producing Party will, to the extent practical, supply an electronic translation of all text (typewritten or printed) contained on all images (OCR). Said OCR files shall be produced as document level text files and be named consistently with their corresponding TIFF files.

3. Extracted Text. For TIFF files generated from native format, the Producing Party shall provide extracted and word searchable text files. Said extracted text files shall be produced as document level extracted text files and be named consistently with their corresponding TIFF files.

4. Load Files. For ESI that the Producing Party produces in TIFF format, the Producing Party shall produce (i) a corresponding file that relates to a set of scanned images that indicates where individual pages belong together as documents and/or attachments and may also contain ESI relevant to the individual document (a "Load File") to accompany the TIFF image, which shall include, for each file, (a) if ascertainable, the original file name and complete file path where the file was located including all directories and subdirectories in order to convey the precise media on

which the document was originally stored during the normal course of business; and (b) if available, a metadata file containing fielded data relevant to the individual document as set forth in Exhibit A; and (ii) a corresponding file that contains a page-level cross reference between the TIFF images, their paths and/or locations, and their assigned document numbers (an "Image Load File"). Said load files shall be consistent with industry standard load files such as those associated with CONCORDANCE. The Producing Party shall produce the documents in the manner and method reasonably calculated to make them usable.

5. Technical Specifications. For ESI that the Producing Party produces in TIFF Format, the Producing Party shall produce all TIFF files as single-page, black and white, dithered (if appropriate), Group 4 TIFF at 300 x 300 dpi resolution and 8½ x 11 inch page size, except for documents requiring different resolution or page size. The Producing Party shall accompany each TIFF format file with a unitization file in standard format showing the unique document number of each page and the appropriate unitization of the documents.

6. Document Bates Numbering. For ESI that the Producing Party produces in TIFF Format, the Producing Party shall electronically "burn" a legible, unique number onto each page at a location that does not obliterate, conceal or interfere with any information from the source document (document numbers for documents produced by Plaintiff shall be in the format "XYZ 00000001" and document numbers for documents produced by Defendants shall be in the format "ABC 00000001"). For

ESI that the Producing Party produces in native format, the Producing Party shall include a single slipsheet in TIFF Format with a legible, unique number in the same format described above, along with the following or substantially similar phrase: "Produced in Native Format." The corresponding native file shall be named in such a manner so that the same Bates number appears in the filename.

7. Redactions. For ESI that the Producing Party produces in TIFF Format, if the Producing Party is redacting information from a page, the Producing Party shall electronically "burn" the word "Redacted" onto the page at or reasonably near to the location of the redaction(s). An electronic copy of the original, unredacted data shall be securely preserved in such a manner so as to preserve without modification, alteration or addition the content of such data including any metadata therein.

D. Terms and Conditions

1. Cooperation. The Parties shall, as necessary, meet and confer to exchange information regarding issues associated with any production of ESI. The Parties shall meet and confer to resolve any procedures or disputes that arise under this Protocol prior to filing any motion with or seeking the intervention of the Court. If a Party objects to any actions taken by another Party, the objecting Party shall state the specific objection in a letter or email to counsel for the opposing Party or Parties. Any practice or procedure set forth herein may be varied by written agreement of the Parties.

2. Notices. All notices, request and demands to or upon any of the Parties under this Protocol shall be in writing, and, unless otherwise expressly provided herein, shall be deemed to have been duly given or made when (i) for delivery by mail or courier, when delivered, or three (3) business days after being deposited in the mail, postage prepaid, whichever is soonest; or (ii) for delivery by facsimile or email, when received, addressed as follows, or to such other address as may be hereafter indicated by any Party

For Plaintiff

For Defendants

Any of the Parties may change its address and transmission numbers for Notices by Notice in the manner provided in this Paragraph.

3. Objections to Admissibility Preserved. Nothing in this Protocol shall be construed to affect in any way the rights of any Party to object to the admissibility of any materials into evidence at the trial of this Litigation.

4. No Waiver of Privileges or Protections. Nothing in this Protocol, including any production of ESI under this Protocol, shall constitute a waiver by any Party of any claim of privilege or other protection from discovery. No production of

any ESI that the Producing Party contends is attorney-client privileged or protected by the work product doctrine shall constitute a waiver of that privilege or protection, and all procedures in any confidentiality and protective orders entered in this Litigation shall be followed with respect to such ESI.

5. Non Parties. The production of any ESI by any Non Party shall be subject to and governed by the terms of this Protocol unless otherwise agreed to by the Parties or as ordered by the Court.

6. Agreement Upon Execution. The Parties agree to be bound by the terms of this Protocol as of the date counsel for all Parties execute this Protocol.

STIPULATED AND AGREED,

DATE: By:_____

Attorney for Plaintiff

DATE: By:_____

Attorney for Defendants

Exhibit A

Paper Document Specifications

1. Paper scanned to Group IV formatted single page TIFF files named by the image key (no images smaller than Letter size);

2. Document level OCR text files named for the first image key will be provided in a .txt file;

3. .DAT formatted metadata load file with the following fields:

DESIGNATION	DEFINITION
CUSTODIAN or Producing Party's Designation	Name of the original custodian of the document.
BEGDOC or Producing Party's Designation	User-assigned beginning document number.
ENDDOC or Producing Party's Designation	User-assigned ending document number.
BEGATTAC or Producing Party's Designation	Beginning document number of full parent/child.
ENDATTAC or Producing Party's Designation	Ending document number of full parent/child.
PAGECOUNT	Actual number of TIFF pages generated

Electronic Document Specifications

1. Electronic files processed to Group IV formatted single page TIFF files named by the image key (no images smaller than Letter size);

2. Documents level Extracted Text files named for the first image key will be provided in .txt. file;

3. .DAT formatted metadata load file with the following fields:

DESIGNATION	DEFINITION
CUSTODIAN (SOURCE)	Name of the original custodian of the document
CUSTODIANSALL	Names of all custodians that possessed document but were excluded from production as a result of de-duplication
CONFIDENTIAL	Populated with the Confidentiality legend if necessary
BEGDOC or Producing Party's Designation	User-assigned beginning document number or image key
ENDDOC or Producing Party's Designation	User-assigned ending document number or image key
BEGATTAC or Producing Party's Designation	Beginning document number of full parent/child
ENDATTAC or Producing Party's Designation	Ending document number of full parent/child
ATTACHCO or Producing Party's Designation	Number of attachments to a parent item
PAGECOUN or Producing Party's Designation	Actual number of TIFF pages generated
AUTHOR (FROM)	Common user name and/or address, if it exists, for an email. Author name for an e-file.
RECIPIEN (TO)	String of names to whom the email was sent
CC	Additional email recipients
BCC	Hidden recipients to an email
SUBJECT	Subject line of emails or use inputted metadata from an e-file
TITLE	Title from properties of document
DATESENT	Date an email was sent
TIMESENT	Time an email was sent
DATECREA	Date when a file was created
TIMECREA	Time when a file was created
DATEMOD	Date the file was last modified
TIMEMOD	Time the file was last modified
ORIGFILE	Complete file name and extension
FILESIZE	Size of a file in Kilobytes or Bytes
EDDRDTTM	The date and time when an email was received by the addressee

DESIGNATION	DEFINITION
EDDSENTD	The date and time when an email was sent by the Author.
FILEPATH	The complete file path where the file was located
NATIVELINK	Native File Link (Native Files Only)