USE OF SOCIAL MEDIA & ESI IN FAMILY LAW LITIGATION

2018 SC FAMILY LAW INTENSIVE CLE
Grove Park Inn
November 2 – 4, 2018

MELISSA FULLER BROWN
56 Wentworth Street, Ste. 100
Charleston, SC 29401
843.722.8900
Melissa@melissa-brown.com
www.scdivorcelaw.com

34

RULE 34

Producing Documents, Electronically Stored Information, and Tangible Things, or Entering onto Land, for Inspection and Other Purposes

New Rule Provisions

. . . . .

(b) Procedure.

. . . . .

(2) *Responses and Objections.*

(A) Time to Respond. The party to whom the request is directed must respond in writing within 30 days after being served or—if the request was delivered under Rule 26(d)(2)—within 30 days after the parties' first Rule 26(f) conference. A shorter or longer time may be stipulated to under Rule 29 or be ordered by the court.

(B) Responding to Each Item. For each item or category, the response must either state that inspection and related activities will be permitted as requested or state ~~an objection~~ with specificity the grounds for objecting to the request, including the reasons. The responding party may state that it will produce copies of documents or of electronically stored information instead of permitting inspection. The production must then be completed no later than the time for inspection specified in the request or another reasonable time specified in the response.

(C) Objections. An objection must state whether any responsive materials are being withheld on the basis of that objection. An objection to part of a request must specify the part and permit inspection of the rest.

Committee Note

Several amendments are made in Rule 34, aimed at reducing the potential to impose unreasonable burdens by objections to requests to produce.

Rule 34(b)(2)(A) is amended to fit with new Rule 26(d)(2). The time to respond to a Rule 34 request delivered before the parties' Rule 26(f) conference is 30 days after the first Rule 26(f) conference.

Rule 34(b)(2)(B) is amended to require that objections to Rule 34 requests be stated with specificity. This provision adopts the language of Rule 33(b)(4), eliminating any doubt that less specific objections might be suitable under Rule 34. The specificity of the objection ties to the new provision in Rule 34(b)(2)(C) directing that an objection must state whether any responsive materials are being withheld on the basis of that objection. An objection may state that a request is overbroad, but if the objection recognizes that some part of the request is appropriate the objection should state the scope that is not overbroad. Examples would be a statement that the responding party will limit the search to documents or electronically stored information created within a given period of time prior to the events in suit, or to specified sources. When there is such an objection, the statement of what has been withheld can properly identify as matters "withheld" anything beyond the scope of the search specified in the objection.

Rule 34(b)(2)(B) is further amended to reflect the common practice of producing copies of documents or electronically stored information rather than simply permitting inspection. The response to the request must state that copies will be produced. The production must be completed either by the time for inspection specified in the request or by another reasonable time specifically identified in the response. When it is necessary to make the production in stages the response should specify the beginning and end dates of the production.

Rule 34(b)(2)(C) is amended to provide that an objection to a Rule 34 request must state whether anything is being withheld on the basis of the objection. This amendment should end the confusion that frequently arises when a producing party states several objections and still produces information, leaving the requesting party uncertain whether any relevant and responsive information has been withheld on the basis of the objections. The producing party does not need to provide a detailed description or log of all documents withheld, but does need to alert other parties to the fact that documents have been withheld and thereby facilitate an informed discussion of the objection. An objection that states the limits that have controlled the search for responsive and relevant materials qualifies as a statement that the materials have been "withheld."

Amendment Analysis

Specified Discovery Responses and Objections

Rule 34 is substantially amended in three parts. Taken as a whole, these amendments aim to limit any confusion with regards to production

obligations and objections to requests for production.

First, Rule 34(b)(2)(A) is amended to align with new Rule 26(d)(2) that affords parties the option of delivering requests for production before the Rule 26(f) conference. Next, new amendments to Rule 34(b)(2)(B) require that objections to Rule 34 requests must "be stated with specificity." In addition, Rule 34(b)(2)(B) will be revised to recognize the common practice whereby a responding party produces copies of documents or ESI instead of permitting inspection. Last, Rule 34(b)(2)(C) requires parties objecting to a Rule 34 request to disclose whether or not any responsive information is being withheld based on the objection and the Committee Note attempts to explain how that requirement can be met in the complex world of ediscovery.

Impact for Corporations and Law Firms

New Rule Eliminates Boilerplate Objections

The necessity for making specific objections is likely to have an impact on the use of boilerplate objections. Broad and boilerplate objections will no longer be allowed in discovery disputes. While the Committee Note suggests that an objection may be raised to the broad nature of a request, that objection must state that the scope is not overbroad if a portion of that request remains appropriate.

Objection Rules Raise Issues About the Necessity to Log Withheld Information

The requirement for specificity of objections ties directly with the new provision that an objection must also include whether any responsive materials are withheld on the basis of that objection. The Committee clearly intends to prevent misleading objections, which leave the requesting party in the dark about whether information is nonetheless being withheld after a partial production. Based on these revisions, parties may benefit from keeping a running record of material withheld (i.e., privilege log), making it easier to state the reason for the objection and to demonstrate to both the other party and the court what items are being withheld. Although a "detailed description or log of all documents withheld" need not be furnished, parties must "alert" the other party and facilitate an informed discussion of withheld material. An objection which states the limit of the search parameters (such as number of custodians, dates, data sources, etc.) would suffice as a statement that materials have been withheld.

Parties Must Produce by Specific Date in Lieu of Inspections

The amended rule also mandates that producing documents in lieu of a request for inspection must be completed "no later than the time for inspection specified in the request or another reasonable time specified in the response." Some practices before this new rule saw parties stating that documents would be produced in the future without committing to a specific date. This new rule will eliminate that ambiguous approach by forcing parties to agree to specific dates in returning a response to prevent game-playing and to force parties to keep a schedule—

although there may be some disagreement as to what constitutes producing within a "reasonable time." The new rules, whether in scheduling or in production, reflect a new urgency on the processes of collection and production. Parties will do well to have a thorough understanding regarding the status of their data well before discovery requests and productions transpire.

34

37

RULE 37

Failure to Make Disclosures or to Cooperate in Discovery; Sanctions

New Rule Provisions

(a) Motion for an Order Compelling Disclosure or Discovery.

• • • • •

(3) *Specific Motions.*

• • • • •

(B) To Compel a Discovery Response. A party seeking discovery may move for an order compelling an answer, designation, production, or inspection. This motion may be made if:

• • • • •

(iv) a party fails to produce documents or fails to respond that inspection will be permitted—or fails to permit inspection—as requested under Rule 34.

• • • • •

(e) Failure to ~~Provide~~Preserve Electronically Stored Information. ~~Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.~~ 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.

* * * * *

Committee Note

Subdivision (a). Rule 37(a)(3)(B)(iv) is amended to reflect the common practice of producing copies of documents or electronically stored information rather than simply permitting inspection. This change brings item (iv) into line with paragraph (B), which provides a motion for an order compelling "production, or inspection."

Subdivision (e). Present Rule 37(e), adopted in 2006, provides: "Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system." This limited rule has not adequately addressed the serious problems resulting from the continued exponential growth in the volume of such information. Federal circuits have established significantly different standards for imposing sanctions or curative measure on parties who fail to preserve electronically stored information. These developments have cause litigants to expend excessive effort and money on preservation in order to avoid the risk of severe sanctions if a court finds they did not do enough.

New Rule 37(e) replaces the 2006 rule. It authorizes and specifies measures a court may employ if information that should have been preserved is lost, and specifies the findings necessary to justify these measures. It therefore forecloses reliance on inherent authority or state law to determine when certain measures should be used. The rule does not affect the validity of an independent tort claim for spoliation if state law applies in a case and authorizes the claim.

The new rule applies only to electronically stored information, also the focus of the 2006 rule. It applies only when such information is lost. Because electronically stored information often exists in multiple locations, loss from one source may often be harmless when substitute information can be found elsewhere.

The new rule applies only if the lost information should have been preserved in the anticipation or conduct of litigation and the party failed to take reasonable steps to preserve it. Many court decisions hold that potential litigants have a duty to preserve relevant information when litigation is reasonably foreseeable. Rule 37(e) is based on this common-law duty; it does not attempt to create a new duty to preserve. The rule does not apply when information is lost before a duty to preserve arises.

37

In applying the rule, a court may need to decide whether and when a duty to preserve arose. Courts should consider the extent to which a party was on notice that litigation was likely and that the information would be relevant. A variety of events may alert a party to the prospect of litigation. Often these events provide only limited information about the prospective litigation, however, so that the scope of information that should be preserved may remain uncertain. It is important not to be blinded to this reality by hindsight arising from familiarity with an action as it is actually filed.

Although the rule focuses on the common-law obligation to preserve in the anticipation or conduct of litigation, courts may sometimes consider whether there is an independent requirement that the lost information be preserved. Such requirements arise from many sources—statutes, administrative regulations, an order in another case, or a party's own information-retention protocols. The court should be sensitive, however, to the fact that such independent preservation requirements may be addressed to a wide variety of concerns unrelated to the current litigation. The fact that a party had an independent obligation to preserve information does not necessarily mean that it had such a duty with respect the litigation, and the fact that the party failed to observe some other preservation obligation does not itself prove that its efforts to preserve were not reasonable with respect to a particular case.

The duty to preserve may in some instances be triggered or clarified by a court order in the case. Preservation orders may become more common, in part because Rules 16(b)(3)(B)(iii) and 26(f)(3)(C) are amended to encourage discovery plans and orders that address preservation. Once litigation has commenced, if the parties cannot reach agreement about preservation issues, promptly seeking judicial guidance about the extent of reasonable preservation may be important.

The rule applies only if the information was lost because the party failed to take reasonable steps to preserve the information. Due to the ever-increasing volume of electronically stored information and the multitude of devices that generate such information, perfection in preserving all relevant electronically stored information is often impossible. As under the current rule, the routine, good-faith operation of an electronic information system would be a relevant factor for the court to consider in evaluating whether a party failed to take reasonable steps to preserve lost information, although the prospect of litigation may call for reasonable steps to preserve information by intervening in that routine operation. This rule recognizes that "reasonable steps" to preserve suffice; it does not call for perfection. The court should be sensitive to the party's sophistication with regard to litigation in evaluating preservation efforts; some litigants, particularly individual litigants, may be less familiar with preservation obligations than others who have considerable experience in litigation.

Because the rule calls only for reasonable steps to preserve, it is inapplicable when the loss of information occurs despite the party's reasonable steps to preserve. For example, the information may not be in the party's control. Or information the party has preserved may be destroyed by

events outside the party's control—the computer room may be flooded, a "cloud" service may fail, a malign software attack may disrupt a storage system, and so on. Courts may, however, need to assess the extent to which a party knew of and protected against such risks.

Another factor in evaluating the reasonableness of preservation efforts is proportionality. The court should be sensitive to party resources; aggressive preservation efforts can be extremely costly, and parties (including governmental parties) may have limited staff and resources to devote to those efforts. A party may act reasonably by choosing a less costly form of information preservation, if it is substantially as effective as more costly forms. It is important that counsel become familiar with their clients' information systems and digital data—including social media—to address these issues. A party urging that preservation requests are disproportionate may need to provide specifics about these matters in order to enable meaningful discussion of the appropriate preservation regime.

When a party fails to take reasonable steps to preserve electronically stored information that should have been preserved in the anticipation or conduct of litigation, and the information is lost as a result, Rule 37(e) directs that the initial focus should be on whether the lost information can be restored or replaced through additional discovery. Nothing in the rule limits the court's powers under Rules 16 and 26 to authorize additional discovery. Orders under Rule 26(b)(2)(B) regarding discovery from sources that would ordinarily be considered inaccessible or under Rule 26(c)(1)(B) on allocation of expenses may be pertinent to solving such problems. If the information is restored or replaced, no further measures should be taken. At the same time, it is important to emphasize that efforts to restore or replace lost information through discovery should be proportional to the apparent importance of the lost information to claims or defenses in the litigation. For example, substantial measures should not be employed to restore or replace information that is marginally relevant or duplicative.

Subdivision (e)(1). This subdivision applies only if information should have been preserved in the anticipation or conduct of litigation, a party failed to take reasonable steps to preserve the information, information was lost as a result, and the information could not be restored or replaced by additional discovery. In addition, a court may resort to (e)(1) measures only "upon finding prejudice to another party from loss of the information." An evaluation of prejudice from the loss of information necessarily includes an evaluation of the information's importance in the litigation.

The rule does not place a burden of proving or disproving prejudice on one party or the other. Determining the content of lost information may be a difficult task in some cases, and placing the burden of proving prejudice on the party that did not lose the information may be unfair. In other situations, however, the content of the lost information may be fairly evident, the information may appear to be unimportant, or the abundance of preserved information may appear sufficient to meet the needs of all parties. Requiring the party seeking curative measures to prove prejudice may be reasonable in such

situations. The rule leaves judges with discretion to determine how best to assess prejudice in particular cases.

Once a finding of prejudice is made, the court is authorized to employ measures "no greater than necessary to cure the prejudice." The range of such measures is quite broad if they are necessary for this purpose. There is no all-purpose hierarchy of the severity of various measures; the severity of given measures must be calibrated in terms of their effect on the particular case. But authority to order measures no greater than necessary to cure prejudice does not require the court to adopt measures to cure every possible prejudicial effect. Much is entrusted to the court's discretion.

In an appropriate case, it may be that serious measures are necessary to cure prejudice found by the court, such as forbidding the party that failed to preserve information from putting on certain evidence, permitting the parties to present evidence and argument to the jury regarding the loss of information, or giving the jury instructions to assist in its evaluation of such evidence or argument, other than instructions to which subdivision (e)(2) applies. Care must be taken, however, to ensure that curative measures under subdivision (e)(1) do not have the effect of measures that are permitted under subdivision (e)(2) only on a finding of intent to deprive another party of the lost information's use in the litigation. An example of an inappropriate (e)(1) measure might be an order striking pleadings related to, or precluding a party from offering any evidence in support of, the central or only claim or defense in the case. On the other hand, it may be appropriate to exclude a specific item of evidence to offset prejudice caused by failure to preserve other evidence that might contradict the excluded item of evidence.

Subdivision (e)(2). This subdivision authorizes courts to use specified and very severe measures to address or deter failures to preserve electronically stored information, but only on finding that the party that lost the information acted with the intent to deprive another party of the information's use in the litigation. It is designed to provide a uniform standard in federal court for use of these serious measures when addressing failure to preserve electronically stored information. It rejects cases such as *Residential Funding Corp. v. DeGeorge Financial Corp.*, 306 F.3d 99 (2d Cir. 2002), that authorize the giving of adverse-inference instructions on a finding of negligence or gross negligence.

Adverse-inference instructions were developed on the premise that a party's intentional loss or destruction of evidence to prevent its use in litigation gives rise to a reasonable inference that the evidence was unfavorable to the party responsible for loss or destruction of the evidence. Negligent or even grossly negligent behavior does not logically support that inference. Information lost through negligence may have been favorable to either party, including the party that lost it, and inferring that it was unfavorable to that party may tip the balance at trial in ways the lost information never would have. The better rule for the negligent or grossly negligent loss of electronically stored information is to preserve a broad range of measures to cure prejudice caused by its loss, but to limit the most severe measures to instances of intentional loss or destruction.

Similar reasons apply to limiting the court's authority to presume or infer that the lost information was unfavorable to the party who lost it when ruling on a pretrial motion or presiding at a bench trial. Subdivision (e)(2) limits the ability of courts to draw adverse inferences based on the loss of information in these circumstances, permitting them only when a court finds that the information was lost with the intent to prevent its use in litigation.

Subdivision (e)(2) applies to jury instructions that permit or require the jury to presume or infer that lost information was unfavorable to the party that lost it. Thus, it covers any instruction that directs or permits the jury to infer from the loss of information that it was in fact unfavorable to the party that lost it. The subdivision does not apply to jury instructions that do not involve such an inference. For example, subdivision (e)(2) would not prohibit a court from allowing the parties to present evidence to the jury concerning the loss and likely relevance of information and instructing the jury that it may consider that evidence, along with all the other evidence in the case, in making its decision. These measures, which would not involve instructing a jury it may draw an adverse inference from loss of information, would be available under subdivision (e)(1) if no greater than necessary to cure prejudice. In addition, subdivision (e)(2) does not limit the discretion of courts to give traditional missing evidence instructions based on a party's failure to present evidence it has in its possession at the time of trial.

Subdivision (e)(2) requires a finding that the party acted with the intent to deprive another party of the information's use in the litigation. This finding may be made by the court when ruling on a pretrial motion, when presiding at a bench trial, or when deciding whether to give an adverse inference instruction at trial. If a court were to conclude that the intent finding should be made by a jury, the court's instruction should make clear that the jury may infer from the loss of the information that it was unfavorable to the party that lost it only if the jury first finds that the party acted with the intent to deprive another party of the information's use in the litigation. If the jury does not make this finding, it may not infer from the loss that the information was unfavorable to the party that lost it.

Subdivision (e)(2) does not include a requirement that the court find prejudice to the party deprived of the information. This is because the finding of intent required by the subdivision can support not only an inference that the lost information was unfavorable to the party that intentionally destroyed it, but also an inference that the opposing party was prejudiced by the loss of information that would have favored its position. Subdivision (e)(2) does not require any further finding of prejudice.

Courts should exercise caution, however, in using the measures specified in (e)(2). Finding an intent to deprive another party of the lost information's use in the litigation does not require a court to adopt any of the measures listed in subdivision (e)(2). The remedy should fit the wrong, and the severe measures authorized by this subdivision should not be used when the information lost was relatively unimportant or lesser measures such as those specified in subdivision (e)(1) would be sufficient to redress the loss.

37

Amendment Analysis

Uniform Standard for Sanctions

Revised Rule 37(e) addresses and resolves a historical split among the Federal Circuits concerning the level of culpability required to issue severe sanctions, including adverse inferences, for failing to preserve electronically stored information. One group of Circuits only required a finding of negligent failure to preserve ESI, while others required a finding of bad faith.

The amendment to Rule 37(e) completely replaces the previous version of the rule and will only permit the most serious sanctions when there is proof of an "intent to deprive" a party of the use of ESI in the course of the matter, thereby displacing the existing Circuit rulings on the topic, which were based on the exercise of inherent sanction power. The new rule, however, broadly authorizes courts to impose measures designed to address the prejudice from covered losses without a showing of culpability provided that they are no greater than necessary to do so and do not constitute the type of case-dispositive measures that require a showing of specific intent to deprive.

Scope of Rule Limited to Losses of ESI Meeting Specified Criteria

The rule was significantly revised after public comment so as to apply only to failures to preserve ESI which has been lost as the result of a failure to take "reasonable steps" to preserve and which cannot be restored or replaced by additional discovery. If these threshold requirements are not met, none of the measures available under the revised rule may be imposed by a court.

The Committee Note explains that the new Rule 37(e) does not create a new duty to preserve, but rather codifies the existing common law duty to preserve relevant information when litigation is reasonably foreseeable. It is clear, however, that by imposing the threshold requirements, a significant overlay on the common law requirements has been posited by the Rules Committee and it remains to be seen whether and how courts will react to the new provisions.

Reasonable Steps

The Committee Note also clarifies that "reasonable steps to preserve suffice; it does not call for perfection," but also mentions that proportionality, including consideration of the party's resources, will be a factor when evaluating the reasonableness of preservation efforts. This represents a move away from a strict liability test and a move toward an assessment on good faith and proportionality when it comes to the duty to preserve.

Impact for Corporations and Law Firms

When It Comes to Preservation, Good Faith and Reasonableness are Paramount

It is no secret that preservation is one of the thorniest issues in ediscovery. With data volumes and locations rising year-over-year, how does an organization and its counsel ensure that all relevant documents are protected and

anything else is sent to the digital equivalent of a paper shredder? Unfortunately, preservation is a balancing act. Preserve too much and an organization is exposed to increased costs and risk associated with saving out-of-date records; save too little and an organization faces possible sanctions for destroying potentially relevant information when litigation was reasonably foreseeable. Striking this balance is not easy, as evidenced by an abundance of past judicial opinions deliberating the validity of sanctions when ESI is lost. Unfortunately, despite a bulk of case law, there are no bright line rules and, even worse, a split was starting to develop amongst courts.

The changes to Rule 37 are designed to reset the preservation duty by allowing courts and counsel to use good faith and reasonableness as the guide, and granting courts flexibility in determining an appropriate sanction for errors. If a party fails to take reasonable steps to preserve information it should have preserved, and it cannot be restored or replaced, Rule 37(e)(1) permits a broad range of measures short of the harsh measures barred by Rule 37(e)(2) without a showing of specific intent. Subdivision (e)(1) requires no additional showing of culpability, provided the measures are "no greater than necessary to cure the prejudice."

While any organization's efforts to preserve will be retroactively assessed on good faith and proportionality, proportionality is not a good tool for planning. Nonetheless forward-thinking organizations should make sure to proactively demonstrate good faith efforts in preserving their data.

For organizations and law firms, the question remains how best to make a good faith effort in preserving data. The Rules Committee adopted the "reasonable steps" test to encourage responsible and targeted preservation and retention efforts. Instead of preserving or retaining information from an entire department in an organization, targeting individual custodians may demonstrate an appropriate showing of good faith to the courts. Further, implementing solid information governance protocols—from setting and enforcing policies to understanding how data flows across an organization via a data map—will allow the court to see that organizations and law firms are thinking critically about how their information is stored and can contribute to a good faith showing.

In addition, proactive parties may wish to consider obtaining a preservation agreement from the opposing party, taking sanctions arguments off the table completely in most situations. All in all, these preservation and sanction scenarios are likely to play out in judicial opinions in the coming months and years, as courts grapple with the definitions of reasonableness and good faith.

About KLDiscovery

KLDiscovery provides technology-driven services and software to help legal, corporate and government entities as well as consumers manage, recover, search, analyze, produce and present data efficiently and cost-effectively. In addition to its award-winning suite of software, KLDiscovery provides data recovery, data destruction, electronic discovery, and document review.

For more information about KLDiscovery and its offerings please visit: www.KLDiscovery.com or follow @KLDiscovery on Twitter and Facebook.

8201 Greensboro Drive, Suite 717 | McLean, VA 22102
888.881.3789 | www.KLDiscovery.com

EXHIBIT 4

Discussion of Electronic Discovery at Rule 26(f) Conferences: A Guide for Practitioners

INTRODUCTION

Virtually all modern discovery involves electronically stored information (ESI). The production and review of such information can be complex and expensive. Competent litigators must be familiar with the fundamentals of electronic discovery; they cannot delegate that duty to clients or non-lawyers. Moreover, lawyers' early identification, discussion, and joint resolution of potential e-discovery issues will help minimize future disputes. It will also assure that discovery proceeds efficiently, consistent with the goals of Fed. R. Civ. P. 1 and 26. Conversely, lawyers who lack this competence, and who fail to cooperate in discovery, are likely to increase the cost of litigation and may face the risk of sanctions. In August 2012, the ABA amended Model Rule 1.1 to require, as part of a lawyer's duty to provide "competent representation," that such competency include "keep[ing] abreast of *changes* in the law and its practice, including the benefits and risks associated with *relevant technology*." ABA Model Rule 1.1, cmt. 8 (emphasis added). An argument could be made that this includes lawyers' duty to keep abreast of changes in the technology of e-discovery.

This Guide was prepared by this U.S. District Court, District of Minnesota's Federal Practice Committee for the purpose of helping counsel anticipate, discuss, and resolve common e-discovery issues. Because each case is different, however, this Guide is neither a court rule nor a one-size-fits-all checklist. It identifies a variety of issues relating to e-discovery that *may* arise in civil litigation before this Court, but by no means intends to suggest that all such issues will be relevant or that they must be addressed in any given case.[1] Rather, its goal is to assist counsel at the Rule 26(f) conference to engage in a meaningful discussion about the scope and process of ESI search, review, and production that is reasonable, proportionate, and efficient in view of the circumstances of their case.

[1] On the other hand, the Guide is also not intended to be encyclopedic. Counsel who wish to learn more will find representative resources listed at the end of this Guide.

A. Preservation and Litigation Hold[2]

- ☐ **Issuance.** Has each party issued a litigation hold/preservation notice?
  - o If so, when?
  - o If so, to whom?
- ☐ **Updates.** Does the hold or notice need to be updated?
- ☐ **Burden.** Does the hold or notice unfairly burden any party?
  - o If so, can the parties agree upon ways to relieve that burden?
  - o For example:
    - ▪ Limiting its scope?
    - ▪ Limiting the number or types of custodians covered?
- ☐ **Exclusions.** Can the parties agree that certain ESI sources need not be preserved because the burden of preservation outweighs the likelihood that the sources will contain probative information not otherwise available in more accessible forms? Such potential ESI sources could include:
  - o backup tapes
  - o printer files
  - o mobile devices
  - o voicemail
  - o legacy systems
  - o deleted files
  - o archival systems
  - o certain cloud storage repositories
  - o others
- ☐ **Retention and destruction practices.** What are each party's regular record retention/disposal practices (to understand and set expectations about

[2] The law is unsettled on whether litigation holds are privileged or otherwise immune from discovery. Counsel should consider this before disclosing information regarding the issuance and contents of a litigation hold.

what otherwise relevant ESI (or other documents) may no longer be available or reasonably accessible)?

- ☐ **Non-parties.** Are any non-parties likely to have significant relevant information? If so:
  - o **Preservation.** Should a preservation letter be sent?
  - o **Cost.** Should one or both parties reimburse some or all of the expenses that may be incurred by the non-party as a result of the anticipated discovery?

B. Relevant ESI Types and Reasonable Accessibility

- ☐ **Priority.** Should certain types and/or sources of ESI (or other documents) be prioritized for early review and production?
- ☐ **Early 30(b)(6).** Would an early Rule 30(b)(6) deposition help the parties to better focus their ESI requests?
- ☐ **E-mail.** Should the parties defer serving requests for e-mail until after they exchange other discovery (electronic or otherwise)? Some considerations include:
  - o How likely is it that information that is relevant to the issues in the case and not cumulative of information available from other sources will be found in the party's e-mail?
  - o Does either party ordinarily maintain potentially relevant business records (*e.g.*, contracts, financial reports, strategic plans) *only* as e-mail attachments, rather than maintaining them separately?
  - o Should requests for e-mail be:
    - Distinguished from other discovery requests?
    - Focused on particular issues?
- ☐ **Databases.** How will the parties produce relevant information from databases?
  - o Produce the entire database?
  - o Grant database access to the opposing party's counsel or expert?
  - o Produce report(s) of relevant information out of the database?
- ☐ **Legacy software or media.** Is any potentially relevant ESI likely to reside in obsolete, proprietary, or unsupported software or media that may no longer be available or readable? If so, is it likely to be cumulative of information available from other, more accessible sources?

- ☐ **Cloud storage.** Is any potentially relevant ESI likely to reside in cloud storage (e.g., Dropbox, Google Drive, OneDrive)?
- ☐ **Social media.** Is any potentially relevant ESI likely to reside in social media (e.g., Facebook, Twitter, LinkedIn, Google Plus)?
- ☐ **Personal e-mail, storage, and social media.** Is any potentially relevant ESI likely to reside in personal e-mail accounts, personal cloud storage (*e.g.*, Dropbox, Google Drive, OneDrive), or on personal social media sites (*e.g.*, Facebook, LinkedIn, Twitter)?
- ☐ **Former employees.** Does each party have a process to identify and preserve potentially relevant ESI of custodians who leave the company?
- ☐ **Passwords/Encryption.** How will the parties handle encrypted or password-protected ESI?
- ☐ **Mobile devices.** Under what circumstances, if any, will the parties search for ESI on mobile devices, such as cellular phones, tablets, PDAs, or wearable devices?
- ☐ **Voicemail.**
    - o Is potentially relevant information likely to reside in voicemail?
    - o Does a party's voicemail system convert messages into audio and/or text files, sending them automatically to the custodian's e-mail account?
    - o In light of the above, or other circumstances, will the parties search or collect voicemail? If so,
        - For what sources?
        - In what format will it be produced?
- ☐ **Non-accessible ESI.** Is any other source of potentially relevant ESI not reasonably accessible for other reasons?
- ☐ **Burden outweighing benefit.** Can the parties agree that certain sources or types of ESI (e.g., backup tapes, printer files, mobile devices, voicemail, legacy systems, deleted files, archival systems, etc.) need not be searched or collected because the information is not reasonably accessible or searchable, such that the burden outweighs the likely probative value of the information, and/or it is likely that any probative information is available in other, more accessible forms?

C. Collection/Search/Review Protocol and Limitations

- ☐ **Limiting scope of search and collection**
  - o **Number of sources.** Should parties agree on limits to the number of sources searched?
    - For potentially relevant ESI generally?
    - For e-mail specifically?
  - o **Type of sources.** Should parties agree that certain types of ESI sources, even though accessible, need not be searched, e.g., because of the burdensomeness of the search in comparison to the likelihood that relevant information that is not cumulative of other sources will be retrieved.
  - o **Deadline for limiting scope.** If the parties lack information needed to agree to such limits, should they set a deadline for exchanging sufficient information to reach such an agreement?
  - o **Factors.** How will those sources be selected?
    - Criteria?
    - Number?
    - Who will make the selection (i.e., the producing party or the requesting party)?
    - Can sources later be added to or taken off the list, and if so, under what circumstances?
    - How will the parties resolve disputes regarding the number or identity of sources?
  - o **Other limitations.** Can the parties agree on other limitations on scope of search or collection?
    - Date range?
    - Metadata (e.g., particular fields or file types)
- ☐ **Uncommon ESI.** Does some potentially relevant ESI require special handling or production methods?
  - o Pictures or drawings?
  - o GPS coordinates?
  - o Car black box data?
  - o Source code?
  - o Others?

- ☐ **International collection.** Does any party store potentially relevant ESI internationally?
  - o **Privacy laws.** If so, does the host country have privacy laws that could impede, prevent, or constrain collection? Constrain review?
  - o **Foreign languages.** Is any party likely to have foreign-language documents that would require translation to determine their relevance? If so:
    - **Protocol.**
      - Can the parties agree on a translation protocol?
      - Can the parties agree upon a joint translator?
      - Will translation be the responsibility of the producing party, or will the documents be produced untranslated, with each party translating the documents for itself?
    - **Costs.** How will the parties allocate translation costs?
- ☐ **Technological efficiencies and accuracy.** What methods could assist the parties in efficiently and accurately culling, reviewing, and producing the ESI?[3]
  - o **De-duplication?**
    - If so, how?
      - Across the entire production?
      - Only within each source?
    - How will near duplicates be handled?
    - How will e-mail threads (e.g., e-mails with the same text but different attachments) be handled?
  - o **Keyword searching?**[4] If so, what information about the process will the parties exchange or agree to?
    - Limit on number of keywords
    - Degree of specificity of keywords

[3] Parties might not necessarily agree to use the same methodologies, as a number of factors — including disparate sizes of document populations, the nature of the responsive ESI, and how the parties maintain and organize their ESI — may make one methodology appropriate for one party but not for another.

[4] Keyword search is the search of ESI content and/or file metadata that identifies documents and files containing one or more of the key terms, key term combinations, or key phrases from a pre-determined list.

- Process for proposing, reviewing, and revising keyword list
- Testing/sampling/auditing of proposed keywords
- Process for resolving disputes regarding keywords
- Process/justification for subsequent addition of keywords, including whether costs of additional searches would be shifted to requesting party
- Others?

- **Technology-assisted review (TAR),**[5] such as predictive or iterative coding? If so, what information about the process will the parties exchange or agree to?
  - Particular technology platform?
  - Vendor?
  - Reviewing party?
  - Size of document populations?
  - Quality controls?
  - Additional disclosures requested by the receiving party?
    - sampling rates?
    - precision rates?
    - recall rates?
    - responsiveness rates?
- **Methodology validation.** Will parties share information about their ESI culling and review methodology to verify or validate the process?
- **Methodology application.** To what populations of documents will the parties apply the methodology selected?
    - All ESI?
    - E-mail only?
- **Exceptions to application of methodologies?** Conversely, will there be any exceptions to the application of the methodology

[5] Technology-assisted review (TAR) is document review that is facilitated by the use of advanced analytics to help categorize the review population — either by conceptual analysis of the document content performed entirely by the software, or "predictive" analysis and ranking performed by the software, based on initial human input.

selected, i.e., certain types of sources of ESI that will be reviewed without first applying the methodology?

D. Metadata[6]

- ☐ What, if any, metadata fields *will* be preserved?
- ☐ What, if any, metadata fields *will not* (or cannot) be preserved?
- ☐ Will any metadata be produced? If so,
  - o What metadata?
  - o For what ESI?
    - ▪ All ESI?
    - ▪ E-mail only?
    - ▪ Others?
- ☐ Metadata issues. Do the parties know of any metadata issues?
  - o Incomplete metadata
    - ▪ Because of storage method?
    - ▪ Because of transmission method?
    - ▪ Because of how the ESI is identified and captured for review?
  - o Other metadata issues?
- ☐ Attorney-client information and tracked changes. Are there potential privilege issues associated with metadata, such as counsel's revisions or notations on drafts?

E. Form of Production

- ☐ What will be the default ESI production method?
  - o native?
  - o image only?
  - o image and text?
  - o image, text, and metadata?

---

[6] Metadata captures data elements or attributes (name, size, date, type, etc.), data about records or data structures (length, fields, columns, etc.) and data about data (where it is located, how it is associated, ownership, etc.).

- PDF?
  - image only?
  - image and text?
- paper (i.e., printed out and produced in hard copy)?

☐ **Scanning.** Will the parties scan paper documents, producing them electronically?

- If so, will the parties implement Optical Character Recognition (OCR) to make the images' text searchable?

☐ **Load files.** Will load/unitization files[7] be produced?

- If so, what format?
  - Summation DII?
  - *.csv?
  - Others?

☐ **Color.** Must images be produced in color? Or will black and white suffice?

☐ **Document beginning/end; attachments.**

- How will a document's beginning and end be indicated?
- How will the production indicate the association of attachments with parent documents?

☐ **Exceptions to format.** Will there be any exceptions to the general production format?

- Natively produce Excel spreadsheets and PowerPoint presentations?
- Natively produce only upon a party's request for specific documents? (e.g., spreadsheets or presentations)
- If ESI stored in personal email, on websites, or on social media sites is to be produced, how will that be accomplished?
  - screen shots?
  - HTML and associated files?
  - PDFs?
  - direct access?

---

[7] A load/unitization file is a structured file — containing converted document data and associated file/image links — which is imported into a litigation-support or document-review system. It is usually accompanied by the associated image or native document files.

- authorizations for release of information?
- subpoenas to service providers?

☐ **Bates and identification.** How will the parties identify the documents (e.g., Bates number scheme, prefix identifying the producing party)?

☐ **Identification of native files.** If files are produced natively, how will they be identified and authenticated for use in depositions, motions, or trial?

☐ **Sources and custodians.** Will the parties identify each document's source or custodian?

- o If so, how?
- o If a document is found in multiple locations, will each source and custodian be identified?

☐ **Redactions.** How will redactions be handled?

- o Will the specific reason for redaction be endorsed on the document? In load/unitization files?
- o Will redactions for reasons other than privilege or immunity from discovery (*e.g.*, irrelevance or trade secret) be allowed?
- o Will redactions be included on a log?
- o Will ESI that has been redacted be produced in searchable form, or only as an image?

☐ **Encryption and passwords.** How will the parties handle ESI that is encrypted or password-protected?

☐ **Non-convertible, corrupt, and non-document ESI.** How will parties handle non-convertible, corrupt, or "non-document" (*e.g.*, Audio, Video, etc.) files?

☐ **Production media.** On what type of media will productions be made (*e.g.*, CD, DVD, hard drive, cloud storage like Dropbox, etc.)? If by cloud storage or similar transfer means, how will security for confidential information be assured?

F. Timing of Production

☐ **Phases?** Would the litigation proceed more efficiently with a phased approach to discovery, focusing on certain issues or early decisions?

☐ **Rolling?** Should parties produce on a rolling basis?

- ☐ **Prioritized production?** Can the parties agree to prioritize certain custodians, document types, or ESI sources?
- ☐ **Deadlines for substantial completion?** Can the parties agree on deadlines for when productions, or at least certain portions, will be substantially complete?

G. ESI in Custody or Control of Non-Parties

- ☐ **Non-party custodians.** Does either party have potentially relevant information kept by non-parties (*e.g.*, service providers, outside contractors, or other agents) with whom the party has a right of access?
- ☐ **Non-party collection and production.** If so, how will the party handle collection and production?

H. Privileged Material

- ☐ **Privilege logs.** Will the parties produce privilege logs?
- ☐ **Timing.** When will privilege logs be produced?
  - o With or shortly after each production?
  - o After production is substantially complete?
  - o Other timing?
- ☐ **Detail.** In how much detail will privileged documents be described?
- ☐ **E-mail logging.** Will e-mail strings be logged as a single document or multiple documents?
- ☐ **Date limitations.** Can the parties agree to date limitations on log entries?
  - o E.g., exclude privileged documents or ESI dated on or after the complaint?
- ☐ **Consolidated entries.** Can parties log certain categories of privileged documents or ESI as a single entry, rather than individually?
  - o E.g., communications with outside litigation counsel?
- ☐ **"Quick peek" reviews.** Will the parties allow "quick peek" reviews?
  - o To permit the opposing party to review documents or ESI that have not yet been reviewed for privilege?
  - o To allow the producing party to reserve the right to demand the return of privileged documents or ESI without risk of waiver?

- ☐ **Inadvertent productions.** Will the parties agree that inadvertent production of privileged documents or ESI will not waive the privilege, even without a producing party's showing that it took reasonable steps to avoid disclosure?
- ☐ **Clawback.** How will the parties handle return of privileged documents or ESI?
  - o Return production media upon request and remove privileged data from receiving party's system?
  - o Produce replacement media?
  - o Produce privilege log for documents returned?
  - o Potential motions to compel production?
    - ▪ Procedure for such motions?
- ☐ **Stipulated protective order.** Will the parties stipulate to a protective order provision under Fed. R. Evid. 502, providing for circumstances under which disclosure of privileged information will not constitute waiver?

I. Confidentiality and Protective Orders

- ☐ **Presence and types of confidential information.** Is either party's production likely to include potential confidential information?
  - o If so, what types of potentially confidential information?
- ☐ **In-house counsel access.** Will in-house counsel be permitted access to the other side's confidential information?
  - o If so, under what conditions?
- ☐ **Confidentiality designations.** How will the parties indicate confidentiality designations on produced ESI, documents, files, media, and other discovery (e.g., deposition testimony)?
- ☐ **Protection of confidentiality.** How will each party or counsel assure the continued confidentiality of information received from the other side?
- ☐ **Export controls.** Is either party's production likely to contain information that is export-controlled? If so:
  - o What information types?
  - o What must the receiving party do to ensure its protection?
- ☐ **Inadvertent failure to designate.** How will the parties handle a producing party's inadvertent failure to designate information as confidential?

- ☐ **Non-party confidential information.** How will the parties protect the confidentiality of non-party information?
- ☐ **Readiness for protective order.** Are the parties ready to negotiate an appropriate protective order?
    - o NOTE: Consider preparing a draft in anticipation of the conference. Suggested forms may be found on the Court's website.

J. Costs and Cost Allocation

- ☐ **Estimated costs.** Can the parties reasonably estimate the likely costs of collecting, searching, and producing ESI?
    - o If not, should the parties set a date to make by which they will make such an estimate?
- ☐ **Cost sharing.** Under what circumstances would the parties agreed to shift or share the costs of discovery?
    - o Additional sources?
    - o Additional searches?
    - o Searches of ESI that is not reasonably accessible?
    - o Other circumstances?
- ☐ **Cost saving.** Can the parties agree to additional cost-saving measures?
    - o Common e-discovery vendor with protocols to ensure no unauthorized access to opposing parties' information?
    - o Shared document repository?
    - o Others?

K. Forensic Preservation and Searching[8]

Forensic preservation and searching is not commonly required. But if the need arises, counsel should discuss possible forensic preservation and searching methods, including:

- ☐ Identify a vendor to undertake forensic efforts
- ☐ Vendor's role (e.g., jointly retained, court expert, or retained by one party)
- ☐ Collection protocols and limitations

---

[8] A process used for the collection and preservation of ESI, such as drive imaging, that ensures the ESI is handled in such a fashion that the file content and associated metadata are not altered.

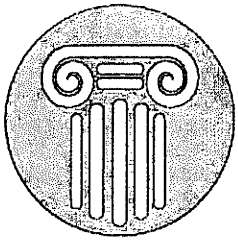
- ☐ Search protocols and limitations
- ☐ Review of producing party's search results (and timing of that review)
- ☐ Production of search results; format of that production
- ☐ Retention of searched information
- ☐ Costs and cost-sharing

L. Continuing Communications

Should the parties schedule periodic discovery conferences to discuss discovery status and issues?

SUGGESTED RESOURCES

1. "The Sedona Conference Working Group Series" contains a number of educational resources and publications proposing best practices in the area of electronic discovery. https://thesedonaconference.org/
2. EDRM (Electronic Discovery Reference Model) offers a number of practical resources relating to electronic discovery and information governance. http://www.edrm.net/
3. American Bar Association – "Your At-a-GlanceTool for Information on E-Discovery"
   http://www.americanbar.org/groups/litigation/resources/e-discovery.html
4. Ediscovery Team blog – A blog by Ralph Losey on the team approach to electronic discovery. http://e-discoveryteam.com/ See also the companion site "Electronic Discovery Best Practices" > http://www.edbp.com/
5. Association of Certified E-Discovery Specialists (ACEDS) – ACEDS is an organization of professionals in the private and public sectors who work in the field of electronic discovery. http://www.aceds.org
6. The Electronic Discovery Institute (EDI). EDI conducts studies of litigation processes that incorporate modern technologies. http://www.ediscoveryinstitute.org
7. "The Implications of Rule 26(g) on the Use of Technology-Assisted Review," 7 FEDERAL COURTS LAW REVIEW 239 (2013).



South Carolina Bar

Continuing Legal Education Division

Family Law Intensive

Friday, November 2-4, 2018

Discovery: How to Properly Request & Obtain Social Media Through Online Searches & Discovery Requests

Melissa Fuller Brown

DISCOVERY: HOW TO PROPERLY REQUEST & OBTAIN SOCIAL MEDIA THROUGH ONLINE SEARCHES, DISCOVERY, MOTIONS & COURT ORDERS
PART II
[Day 2, Afternoon Session]

PENDING SOUTH CAROLINA SUPREME COURT CASE TO WATCH: *Vanderwege v. Vanderwege*

An important case addressing the discovery of social media is pending in the South Carolina Supreme Court. Oral arguments are scheduled for November 28, 2018.

CASE BACKGROUND:

CASE OVERVIEW:

The case, ***Vanderwege v. Vanderwege***, involves Wife's discovery request to Husband all of his social media usernames and passwords. Wife filed a Motion to Compel, and the trial court agreed with Wife and ordered Husband to turn over his all his social media usernames and passwords. Shortly thereafter, Husband petitioned the South Carolina Supreme Court for a common law *writ of certiorari* and an order staying the proceedings pending resolution of the matter. Husband's request for a stay was granted on June 1, 2018.

SPECIFIC FACTS:

The timing of discovery was as follows: On February 7, 2017 Husband filed a Complaint alleging Wife "routinely falsely accuses him of adultery." Husband denied committing adultery, and Wife denied accusing him of committing adultery. Regarding this and other issues, Wife on October 13, 2017, served Interrogatory Number 24 upon Husband, which included the following Interrogatory request:

> 24. Identify all social media accounts to which you have had access in the last three years. For each account, include the user name and password you used to access each account.

On December 18, 2017, Husband answered the Interrogatories, responding to Interrogatory 24 as follows:

> Plaintiff objects to Interrogatory No. 24. The information sought is not relevant to the subject matter of the pending action, or if so, does not outweigh the prejudice to Plaintiff's constitutional right to privacy. Further, the information sought does not appear calculated to lead to the discovery of admissible evidence.

A month and a half later, Wife obtained new counsel on February 1, 2018, and her new attorney filed her Motion to Compel one week later. The Motion to Compel requested the Court to require Husband to fully answer Interrogatory 24.

Following the Motion to Compel on March 12, 2018, the trial court entered an order as follows:

> 3. The [Husband] objected to [Wife's] Interrogatory twenty-four. This Court finds that this Interrogatory is appropriate, and that the [Husband] should serve a response within thirty (30) days of this order.

On May 3, 2018, Husband petitioned the South Carolina Supreme Court for a common law *writ of certiorari* and an order staying the proceedings pending resolution of the matter. Husband's request for a stay was granted on June 1, 2018.

Subsequently, the Supreme Court invited several South Carolina legal organizations to file *Amicus Curiae* briefs. The South Carolina Chapter of the American Academy of Matrimonial Lawyers (SCAAML) accepted the Supreme Court's invitation and filed an *Amicus Curiae* brief.

The SCAAML's Brief, concludes:

> "For the most part, the move from paper discovery to e-discovery does not require a re-invention of the wheel so much as an adaptation of underlying principles that have evolved over the past several decades, most prominently in the Federal Courts. Facebook and LinkedIn posts are the love letters and secret business deals previously snail-mailed to paramours and undisclosed business partners, but no less damning. Preservation of the integrity of ESI evidence is simply a more careful application of chain-of-custody procedures established by the criminal justice system when forensic analysis of crime scenes developed. Confidentiality of sensitive personal matters and privileged communications can be maintained with the security protocols first applied to trade secrets. True, the sheer volume of information has ballooned tremendously but, not to be flippant, such daunting workloads can be managed because there's an app for that.
>
> However, the risk of extensive, possibly irrecoverable, and irreparable damage from a new phenomenon, appropriation of one's very identity by simply giving possession of it to an opposing party, (i.e. giving them a username and password) is the equivalent of giving a possible terrorist the launch codes for a thermonuclear missile. Even a slight chance of extreme harm requires equally extreme protective measures."

AUDIENCE PARTICIPATION:

1. *If you were the trial judge, how would you have ruled?*

NOTES SUGGESTIONS FROM AUDIENCE....

_____

_____

_____

_____

_____

2. *If you represent the H and file a Motion for a Protective Order, what is the basis for your motion?*
(List ideas here.)

_____

_____

_____

_____

_____

3. *If you are the judge, what issues would you want to see included in a Protective Order regarding the parties' discovery of each others' social media presence and ESI?*
List most important issues to include in the Order.

_____

_____

_____

_____

_____

Sample PROTECTIVE ORDER (EXHIBIT 5).

4. *Pretend you represent Husband, and a certified forensic technology expert has downloaded all Husband's social media posts for the past 3 years, what are you, the attorney looking for to include in a Privilege Log?*

_____

_____

_____

_____

_____

Sample PRIVILEGE LOG (EXHIBIT 6)

LET'S THINK AHEAD
WHAT SHOULD EVERY LAWYER DO IN EVERY FAMILY COURT CASE TO GATHER WHAT WE ROUTINELY HEAR ARE A TREASURE TROVE OF EVIDENCE ON THE INTERNET IN ALMOST EVERY FAMILY COURT CASE?

Things to consider:

- Have a system set up where a staff member conducts in-house online Internet social media searches for all public information available about the potential client coming in for an Initial Consult (IC); the opposing party of the person coming in for an IC; about both parties' employers; about their assets; and about any other litigation either party or businesses owned by them have been involved.

- Check all of the following:

  Facebook
  LinkedIn
  Instagram
  Twitter
  CharlestonCounty.org
  Google
    Basic online search
    Google reverse image search, images.google.com
    UserName search
  Search on Wayback for old websites
  Asset Search

Searches for arrests & convictions
Other website searches:

_____
_____
_____
_____
_____

Search programs???? See suggestions in *Electronic Evidence for Family Law Attorneys*, Conlon, Timothy J. and Hughes, Aaron, (2017).

_____
_____
_____
_____
_____
_____

- File a Motion for the Other Party's Electronic Devices, See Timothy J. Conlon's Motion to Sequester Electronic Devices, Exhibit 8, p. 157, *Electronic Evidence for Family Law Attorneys*, Conlon, Timothy J. and Hughes, Aaron, (2017).

- Traditional Discovery Requests (to both *obtain ESI and social evidence from the OP* and *to authenticate the OP's ESI & social media posts*).

TRADITIONAL DISCOVERY REQUESTS

1. **Interrogatories**
Examples of Interrogatory request materials:

- Name and platform address of every social networking website used by the Plaintiff during [*list specific period of time, such as from the date of marriage/separation/filing to date*].
- Each and every email address, username, screen names, IM names, user IDs, handles, login name, for every website, social media and blog on which Plaintiff has an account and include any aliases used by Plaintiff on any of these accounts.
    - Do not ask for the opposing party's password. Instead, request that a qualified person, such as a forensic computer technician download and preserve the information for a *particular period of time* or limit the specific search for particular people/activities/gifts.
    - Then, the party and their counsel should have the opportunity to review the material;
    - And, if any of the material is subject to a privilege, the party should be allowed to create a privilege log; or

- A review by 3rd party; or
- Some courts might permit an *in camera* review. [Given the limitations on SC's Family Court Judges' time, it is doubtful this suggestion will be accepted by our judges.]

- URL for each social networking website.
- Date responding party last accessed each social media platform.
- Date party last changed security settings on social media platforms.
- ***Other suggestions from the Audience:***

_____
_____
_____
_____
_____
_____
_____

2. **Requests for Production**

When requesting social media or ESI materials from the opposing party, be sure to request that they provide the information in their original, native format. And, the same advice is true regarding the submission of a Consent Protective Order.

Also, read the Notes to SCRCP 34. Our Supreme Court has followed the Federal Court in the past when amending our Rules. Therefore, the chances of our Supreme Court amending our rules regarding electronic discovery is highly likely.

CURRENT SCRCP RULE 34

PRODUCTION OF DOCUMENTS AND THINGS AND ENTRY UPON LAND FOR INSPECTION AND OTHER PURPOSES

"**(a) Scope.** Any party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on his behalf, to inspect and copy, any designated documents, or **electronically stored information** ....

(b) Procedure. The request may, without leave of court, be served upon the plaintiff after commencement of the action and upon any other party with or after service of the summons and complaint upon that party. The request shall set forth the items to be inspected either by individual item or by category, and describe each item and category with reasonable particularity. The request shall specify a reasonable time, place, and manner of making the inspection and performing the related acts. **The request may specify the form or forms in which electronically stored information is to be produced.** . . .

Unless the parties otherwise agree, or the court otherwise orders:

(1) If a request does not specify the form or forms for producing electronically stored information, a responding party must produce

the information in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable; and

(2) a party need not produce the same electronically stored information in more than one form."

Note:

This is the language of the current Federal Rule [*Actually, our current Rule 34 does not mirror the current FRCP 34*], and is an amended version of the rule which served as a guide for present Circuit Court Rule 88. The major change is that the requirement of good cause is eliminated because it was an erratic and uncertain guide for decisions by the court. It also saves the court having to handle the matter unless there is an objection to the document requests. Thirty days are permitted for a response, and there is provision for an independent action for discovery against persons not parties to the action.

Note to 2011 Amendment:

The amendments to Rules 16, 26, 33, 34, 37 and 45 of the South Carolina Rules of Civil Procedure concerning electronic discovery **are substantially similar to the corresponding provisions in the Federal Rules of Civil Procedure. [*Actually, our Rule 34 is not substantially similar to the FRCP 34, which was amended on December 1, 2015.*]** The rules concerning electronic discovery are intended to provide a practical, efficient and cost-effective method to assure reasonable discovery. **Pursuit of electronic discovery must relate to the claims and defenses asserted in the pleadings and should serve as a means for facilitating a just and cost-effective resolution of disputes.**

Examples of Requests for Production for social media and ESI:

- Change the Definition of "Documents" in your RFP request header to the following:

> "Document" means any medium upon which intelligence or information has been recorded or from which it was retrieved and includes, without limitation, the original and each copy regardless of origin and location, of any book, pamphlet, periodical, letter, email, text message (including any instant message, chat, tweet, SMS, or other messaging application transmission), memorandum (including any memorandum or report of a meeting or conversation), invoice, bill, order form, receipt, financial statement, accounting entry, diary, calendar or calendar entry, telex, telegram, facsimile, cable, report, record, contract, agreement, study, handwritten note, draft, working paper, chart, paper, print, laboratory record, drawing, sketch, graph, index, list, tape,

photograph, microfilm, data sheet, data processing card, computer file, computer disk, thumb drive or flash drive, SIM card or computer tape or other magnetic or optical media, or any other written, recorded, digitized, transcribed, punched, taped, filmed or graphic matter, however produced or reproduced, to which you have or have had access.

- For each of your social media accounts, produce your account data *from and including the date of marriage (November 12, 2011) through present (or other relevant period)*. You may download and print your Facebook, Twitter and LinkedIn data by logging onto those platforms and the unique instructions to download your account for each Platform.
- Provide copies of each page of the Plaintiff's social media websites *[be sure to request a specific, relevant period of time].*
- Provide copies of all posts made by the Plaintiff on each social media website *[request a specific, relevant period of time].*
- Provide copies of all posts by others on each of the Plaintiff's social networking websites *[request a specific relevant period of time].*
- Provide copies of every photograph downloaded/uploaded to each of the Plaintiff's social media websites *[request a specific relevant period of time].*
- Provide copies of all direct messages sent and received by the Plaintiff on each of his social media websites *[request a specific relevant period of time].*
- ***Other suggestions from the Audience:***

_____
_____
_____
_____
_____

3. **Requests to Admit**
Examples of Social Media/ESI Requests to Admit

- Defendant maintains a Twitter, Facebook, etc account.
- Defendant's Twitter user name is @XXX.
- On July 1, 2014, Defendant posted a tweet stating "can't wait to quit my job tomorrow so I can head to the beach early for July 4th!! #Partynonstop."
- ***Other suggestions from the Audience:***

_____
_____
_____
_____
_____

Allowing the Opposing Party Unchecked Access to the Other Party's Social Media Passwords[8] is a BAD IDEA!

1. Passwords and encryption codes: These are the keys that protect and preserve the Information Technology Fortress of Solitude but, in the wrong hands, can turn into Kryptonite.

a. Example: A Word document on a computer not even connected to the Internet is subject to accidental destruction of evidence if, for example, it is converted to a pdf.[9] This happens because documents created with today's software programs, aside from the text or chart themselves, also contain metadata in the background.

(1) Metadata is information about the document itself such as its history: who initially created the document; when the document was created; how many versions were created; what language was removed and what language added, again, by whom and when.

(2) Indeed, merely placing a cursor over the document will reveal the last date the document was opened; opening the document to see it changes the metadata to the current date and time.[10]

---

[8] Technically, "passwords" are "a sequence of characters required for access to a computer system." Merriam-Webster. However, the discussion here includes anything required to obtain access to a device or data as some smart phones require "two factor authentication," meaning a second password, or encryption keys. "Encryption is a security feature that some modern [devices] use in addition to password protection. When such [devices] lock, data becomes protected by sophisticated encryption that renders a [device] all but 'unbreakable' unless [someone] know[s] the password." *Riley v. California, supra*, at 2486. Accordingly, access to a single password may not be sufficient to obtain the data being sought. At the same time, ephemeral social media (platforms whose posts are deleted after having been read one time or after the passage of a certain period of time, such as Snapchat) are not as protected as advertised: using the appropriate feature, the last 30 days of posts on Snapchat can be retrieved.

[9] A "pdf" is "a computer file format for the transmission of a multimedia document that is not intended to be edited." Merriam-Webster. Put another way, it is essentially a picture of a document that cannot be easily altered.

[10] Even where protections were put into place, lawyers and forensic computer/technology experts have unintentionally spoliated the other party's

(3) This has been important in more than one case where there was a question about when an incriminating document was created – whether it was created on the date at the head of the letter, or later, with the date at the head backdated.

(4) In fact, metadata[11] may reveal information inserted into draft settlement offers involving attorney-client communications, such as monetary offers, that were proposed to the client and removed before sharing with opposing counsel. Thus, careful attorneys either wipe out any metadata from documents mailed in Word format to the opposing counsel or more commonly, only send pdf versions.

2. Social Media Posts: Such materials are typically targeted for discovery, whether stored on a device itself, or in the cloud.[12] **Unrestricted access by an opposing litigant creates the obvious opportunity for disclosure of privileged material (HIPAA records, attorney client communications and the like), not to mention the possible accidental, or intentional, deletion or forging of compromising information.**

a. Indeed, the device itself may contain passwords for other accounts in a designated file, mobile application software, or "app."

b. Simply put, allowing the opposing party to access the other party's social media account allows the opposing party *to assume the identity* of the account owner, which gives the opposing party access to the entire account as well as other platforms such as Venmo and Paypal, which are frequently linked to sites such as Facebook.

---

electronically stored information ("ESI") by their lack of knowledge regarding the proper handling and authentication of the data.

[11] Metadata "is data about data, or descriptive information relating to the file in which it is embedded, for example, information about the creation and editing of the file. It may contain camera settings, GPS locations, dates of file creation and modification, or details about the software and software version of the program that created or edited the file. . . . [M]etadata is not a standard, but rather the potential result of one program or device acting on another, the types and presence of metadata in any given document vary depending on the nature of the document and the process that was used to create it." Fn. 1, p. 2-3, *Electronic Evidence for Family Lawyers*, Conlon, Timothy J. and Hughes, Aaron, (2017).

[12] "Cloud computing is the capacity of Internet connected devices to display data stored in remote servers rather than on the device itself. Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference." *Riley v. California, supra,* at 2491.

c. Indeed, such unauthorized entry potentially allows the opposing party to change the account owner's privacy and other settings, whether on a platform or on a smart device itself.

(1) Ex: One could add the GPS feature to Facebook photo posts so when the account owner posts pictures or comments about restaurants, concerts or other activities, the site would include the owner's location where previously the owner had not chosen to use that feature. This could put the user under stricter surveillance than would be afforded a private investigator by changing an owner's settings without the owner's knowledge or permission. In essence, providing such access could expose an account owner to the risk of unknowingly reporting his whereabouts to others without his knowledge.

(2) On the other hand, what if a third-party hacker got into a party's accounts and made changes? The other party would be the first suspect that the information was intentionally altered. Even if the other party obtained legitimate information incriminating the party whose information was requested, that party might claim that the other forged or planted the evidence.

(3) It has been noted that "[t]he most common challenge to authenticating social media evidence will be from the opposing counsel objecting to the evidence as 'doctored' or 'photo-shopped.'" Gupta, "Commentary; Authenticating Social Media Evidence in California, the Social Media Capitol of the World," *Journal of the American Academy of Matrimonial Lawyers* Vol. 30, No. 2 (2018) at 344.

(4) Protecting passwords *can actually resolve potential authentication issues* further downstream in the litigation. In *People v. Valdez*, 201 Cal. App. 4th 1429 (2011), a photograph and printouts from a criminal defendant's MySpace account were properly authenticated when the investigating officer, who was admittedly not a computer forensics expert but had sufficient user experience with MySpace, testified about how a MySpace account and profile are created; how profiles can be viewed by the public; and how *only the person with the password to the account can upload and edit content on the account pages. See also, In Re KB*, 238 Cal. App. 4th 989 (2015) (a witness with user experience with Instagram such that she was sufficiently familiar with the social media account creation process, including understanding that each account is password protected, provided the court with an adequate foundation to authenticate photographs posted on the Defendant's social media account.)

In short, if the password has only been in the possession of the original owner, the argument that the data has been corrupted or compromised goes away.

3. Protecting Confidential, Privileged Material from Discovery

There are several ways that passwords can be protected. Going from the simplest to the more involved, the first option, if electronically stored information (ESI) is the only thing sought and there are no issues of privilege, the responding spouse (Husband in the *Vanderwege* case) could, instead of turning over passwords, simply download his Facebook[13] account, posts, pictures, videos, private messages and any other requested information into a zip file or onto a thumb drive and provide it to Wife in a format that is not easily modifiable, like pdf. However, where the metadata is relevant (such as metadata that records when certain actions were taken by a party either posting or deleting data from their social media site), providing hard copies of a party's posts does not give the requesting party the information they may desire. In those situations, it is possible to turn over the material in its "native format," which is to provide an exact copy of the data.[14]

This way, particularly when there is a voluminous amount of data, search programs can sift the chaff from the wheat, saving litigation costs. In either case, if the data contains an inordinate amount of material or privileged material, there are two ways to tease those items out.

1. **Traditional way**: Husband could first go through the material, create a privilege log, turn over the non-privileged material, and then, the litigants can fight over the allegedly privileged material.

2. **For more involved cases**: It is not unusual for each party to have their own forensic technology experts, who alone have the passwords and encryption codes. This approach allows the responding party to first have his expert preserve the data, restrict fishing expeditions, and then protect the privileged material;[15] the materials are then turned over to the other expert to review and examine, perhaps mining the metadata or running his own search programs.

3. **One independent gatekeeper**: Have this individual download, review, and protect privileged material identified by each party, and conduct a search using agreed upon search terms. In other situations, perhaps the gatekeeper will provide all non-

---

[13] Other platforms, such as Twitter, have the same capability.

[14] Note: Unlike discovery requests sent to a party to the litigation, when a third party is responding to a subpoena "and the subpoena does not specify the form or forms for producing electronically stored information, a person responding to a subpoena must produce the information *in a form or forms in which it is ordinarily maintained* or in a reasonably usable form or forms." Rule 45(d)(1)(A), SCRCP (emphasis added.)

[15] This need not be a tedious task, nor be used as a claim for the discovery to be unduly burdensome. *See Moore v. Publicis Groupe,* 287 F.R.D. 182, 190 (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) ("[W]hile some lawyers still consider manual review to be the 'gold standard,' that is a myth, as statistics clearly show that computerize searches are at least as accurate, if not more so, than manual review.")

privileged, relevant material that the parties will review on their own, with the ability to use the gatekeeper to conduct follow-up metadata searches or checks. Indeed, common practice among Family Court lawyers in this State who have dealt with these issues, includes appointing a qualified forensic computer analyst – either retained by one or both of the parties – who is tasked with examining the data under a strict Confidentiality Order negotiated by the parties.[16] **Form Confidentiality Order, Exhibit 7.**

Specifically, it is important that such an expert have duties that are clearly spelled out including, but not limited to:

(1) Having sole access to the devices being searched (smart phones, laptops, computers) as well as access to social media of the producing party, with passwords, encryption keys and any other information necessary to access the designated platforms being searched, with the passwords being kept strictly confidential;

(2) Review and produce, preferably in a searchable format (electronic medium), materials within the search parameters set by agreement or Order of the Court[17] (social media posts and the like, but excluding attorney-client or other privileged material), with the materials being then turned over to the producing party with the information considered confidential and proprietary to the producing party left out;

(3) After a set period of time, the unprivileged material is turned over to the requesting party; and

(4) The gatekeeper, both parties, and their counsel are placed under a confidentiality Order to not disclose the materials outside of the litigation. Where appropriate, the information (such as trade secrets) is kept under seal.[18]

---

[16] Indeed, under the new Rule 1, FRCP, counsel for the parties are encouraged to resolve discovery plans before they bring a motion to the court. *See Mancia v. Mayflower Textile Services Co.*, 253 F.R.D. 354 (D. Md. 2008) (Court held the failure of opposing counsel to cooperate and work out disputes was the biggest reason e-discovery costs were skyrocketing; the court strongly advised counsel from both sides to work together and make the e-discovery phase move more smoothly.)[16] For a well-considered and comprehensive discovery plan checklist, see Discussion of Electronic Discovery at Rule 26(f) Conferences: A Guide for Practitioners provided by the US District Court for the District of Minnesota at http://www.mnd.uscourts.gov/FORMS/Clerks_Office/eDiscovery-Guide.pdf.

[17] This may be either specific search terms or a description of information being sought, preferably limited to a specific period of time.

[18] An exception, which should also be stated in the Order, would be if the gatekeeper were to uncover illegal material such as child pornography, which would have to be turned over to the appropriate authorities.

The gatekeeper would be made a party to the Order so the Family Court could enforce confidentiality and other restrictions, or could simply be appointed as the Court's expert subject to the directives of the Court. He or she could be chosen by agreement of the parties or appointed by the Court in the same manner as a Guardian *ad Litem* (he or she is not affiliated with either party or their counsel, etc.).

Only after exhausting the foregoing procedure should the passwords, encryption keys, and other information necessary to access the accounts be obtained by the opposing party; even then, it should only be obtained by Motion of the requesting party demonstrating to the Court a compelling need based on competent evidence. This practice avoids an inadvertent failure to meet a discovery deadline, which would create a disclosure-by-default situation. An affirmative act by the requesting party requires a well-considered decision after the less intrusive options are either exhausted or discarded, before the higher burden of need is triggered.

4. Depositions:

Another way to authenticate online evidence is to ask the actual poster to admit to posting the statement or tweet during a deposition prior to trial. In addition, during the deposition, get the party to download their Facebook account, Twitter account and LinkedIn Account and email the materials to a 3rd party master so the party and the attorney can review the materials to remove any privileged information prior to sharing the non-privileged material with the requesting party.

5. Cellebrite Touch:

A new device and software created by the Israelis and used by many law enforcement groups and computer forensic experts is Cellebrite Touch. It is a product that creates images of cell phones. A one-year license costs $5,000. Once a person is properly trained to use the device, using Cellebrite allows the expert to copy a cell phone and create a verifiable copy for later use at court.

It is best for the client, not the attorney, to take the phone to the expert to protect the chain of custody. The expert will identify and note the information about the phone: serial number, owner, condition of the phone including scratches, and whether the phone was on or off when delivered. The expert will then photograph the phone.

Cellebrite Touch simply creates images. It does not analyze the actual material. Obtaining the images can take a long time. For example, it takes one hour to download images from a phone with 1Gb of memory. Most phones have at least 16 Gb of memory and many have much more. Thus, it will take Cellebrite 64 hours to download images from an iPhone 5 with 64 Gb of memory.

Cellebrite captures contacts, emails, photographs, and calendar entries. However, if contacts and calendar entries are modified, it does not keep a historical track of information.

With emails, the device is able to identify the origin of the source or transmission. Then there is the data extraction. Interestingly, experts can generally get around the passwords on iPhones, but the encryption of outdated Blackberries is solid.

Text messages are also extractable, and there will be a timeline that accurately shows the user's activity, including time and date for photos, and sometimes even the location where the photo was taken.

Relevant federal laws affecting ESI

Part of our duty to explain and educate our clients about preserving ESI is likely the duty to explain how to legally obtain ESI from their spouses. Federal and state laws specifically address this issue. Therefore, lawyers must educate themselves and their clients so that the clients do not violate any laws. Equally worrisome is the naïve attorney who attempts to introduce the illegally-obtained ESI into evidence, as both the client and the attorney could be subject to both criminal and civil penalties.

1. Federal Wiretap Act

"'[E]lectronic communication' means any transfer of signs, signals, writing, images, sounds, data...transmitted in whole or in part by a wire, radio...system that affects interstate or foreign commerce, but does not include...any communication from a tracking device..." *See* 18 U.S.C. § 2510(12)(C)(emphasis added).

2. Stored Communications Act (18 U.S.C. § 2701)

"(a) Offense. — Except as provided in subsection (c) of this section whoever —

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided..." *See* 18 U.S.C. § 2701(a)(1).

In *Jennings v. Jennings*, 401 S.C. 1, 736 S.E.2d 242 (2012), the South Carolina Supreme Court held that it was not a violation of the Stored Communication Act to access another's email account through an account provider and print copies of emails previously read by the recipient. Because emails are not temporary and are not in transmission, the emails residing on the respondent's computer were only copies of emails and could not constitute a backup of such communication. Therefore, this practice did not equal the definition of electronic storage.

3. The Computer Fraud Act (18 U.S.C. § 1030)

"(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains —
(A) information contained in a financial record of a financial institution, or a card issuer as defined in section 1602(n)(1) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. § 1601 et. seq.);

(B) information from any department or agency of the United States; or
(C) information from any protected computer..."

4. Electronic Communications Privacy Act

"Wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce...." *See* 18 U.S.C. § 2510(1).

"Oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication." *See* 18 U.S.C. § 2510(2).

AUDIENCE DISCUSSION & PARTICIPATION

TYPICAL SITUATIONS THAT MIGHT ARISE
IN YOUR LAW PRACTICE
&
HOW TO HANDLE THEM...

1. A potential client brings a number of emails that she downloaded from her husband's account.
She wants to tell you what is in the email messages.
She wants you to read the emails.
She wants you to use the emails at a temporary hearing.

HOW WOULD YOU RESPOND TO THIS SITUATION?
WHAT QUESTIONS, IF ANY, MIGHT YOU ASK OF THE POTENTIAL CLIENT?

_____

_____

_____

_____

_____

_____

_____

2. A potential client brings a number of his spouse's text messages between her and another male that H obtained.
He wants to tell you what is in the text messages.
He wants you to read the text messages.
He wants you to use them at a temporary hearing.

HOW WOULD YOU RESPOND TO THIS SITUATION?
WHAT QUESTIONS, IF ANY, MIGHT YOU ASK OF THE POTENTIAL CLIENT?

3. REAL CASE SCENARIO/QUESTION SENT TO ME:

"I've got a client who just discovered what may be some very damning texts between her current H (Plaintiff) and her Ex-H on her son's (by the Ex-H) cell phone.

W has the phone in her possession (brought over by the son) and wants to bring it to a lawyer to download all the information from it - photos, videos, texts , etc... in a manner that will preserve their integrity as evidence.

Is that something I can do without a forensic IT person?

And if the Ex-H finds out and demands that the phone be returned, is the confirmed presence of relevant evidence that he can subsequently destroy sufficient reason to withhold it, or must it be returned?

My client's Ex-H (who is close friends with client's current H) owns the phone and pays the bill. It is a hand-me-down phone that he provided for the son to use as his own. The son is 11 and brought the phone while on vacation with mom/W. My client, W, saw inappropriate texts on the phone that were not intended for child to see.

What do you advise I do?

IDENTIFY THE ISSUES:

WHAT ADVICE WOULD YOU GIVE?

If there is time..... Q & A about other sticky situations experienced by audience participants....

EXHIBIT
5

STATE OF SOUTH CAROLINA	)	IN THE FAMILY COURT FOR THE NINTH JUDICIAL CIRCUIT
COUNTY OF CHARLESTON	)	
XXXXXXX,	)	Case No.: 2016-DR-XXXXX
Plaintiff,	)	
vs.	)	**CONSENT PROTECTIVE ORDER REGARDING THE FORENSIC ANALYSIS OF THE PARTIES' ELECTRONIC DEVICES**
YYYYY, and **ZZZZZ**,	)	
Defendants.	)	

WHEREAS, the parties have requested an order from this Court granting them the ability to have mirror images of the parties' electronic devices imaged and analyzed, and,

WHEREAS, the parties have agreed to provide for the analysis and exchange of such information subject to this protective order:

NOW, THEREFORE, to protect any documents or information disclosed by Mr. Gilbert as a result of his forensic investigative analysis, it is with the consent of the parties, hereby **ORDERED**:

1. Jeremy Gilbert or an equally qualified member of his staff shall inspect the hard drives and devices and shall perform specific electronic discovery tasks requested by the parties, their attorneys and the Guardian *ad Litem*.

2. Mr. Gilbert or an equally qualified member of his staff at Dixon Hughes Dixon, LLP, (DHG) shall make a copy of each of the parties' hard drives from all submitted devices from January 1, 2014 to date.

3. Mr. Gilbert and any member of DHG will not waive any applicable

privilege or other doctrine or principal assuring the confidentiality of the information on each of the parties' hard drives and other electronic devices.

4. Mr. Gilbert and his staff shall maintain all information in the strictest confidence. No information learned by Mr. Gilbert or his staff shall be disclosed except pursuant to the terms of this Order, or other direction of the Court.

5. If requested by either party, Mr. Gilbert and his staff shall make himself reasonably available for deposition or trial testimony to testify concerning their inspection and findings except as to any information that is protected by a legitimate privilege identified by each of the parties.

6. Within five (5) days, after receiving the electronic data (in its native format), records, files, or other information, Mr. Gilbert and/or his staff, shall provide each party's counsel with each of their client's information so each attorney can create a privilege log that designates all privileged material and the basis for the privilege and the date, time and type of item (ex. Email btw client and attorney, dated 8.1.16, at 10:00 am.). Once both parties create their privilege log, Mr. Gilbert or a qualified member of his staff shall produce immediately to each party's counsel and the GAL all non-privileged, responsive electronic data (in its native format), records, files, or other information. Each party's counsel shall also provide the other party and GAL with a copy of their privilege logs sufficient to allow the other to challenge any claim of privilege.

7. Plaintiff-Father and Defendant-Mother shall equally bear the costs of Mr. Gilbert of his staff's work pursuant to this Order.

8. All information obtained by and from Mr. Gilbert or his staff shall be subject to a NON-WAIVER AND CONFIDENTIALITY AGREEMENT ("Agreement") as follows:

A. Any Protected Material recovered by Mr. Gilbert or his staff shall be considered confidential and proprietary to the producing party (or the party about whom or on whose behalf the information or materials is provided). Mr. Gilbert shall hold the same in confidence and shall not use any such information other than for the purposes outlined in this Agreement; namely the search for child pornography. Moreover, Protected Material shall not be disclosed, published, or otherwise revealed to any party, person, or entity except with the specific prior written authorization of the protected party.

B. If Protected Material is used in this litigation, such records may only be disclosed to the parties; any Guardian *ad Litem* duly appointed; the attorneys (including the partners, associates, contractors, and employees of any attorney actively engaged in the conduct of this litigation); any expert witnesses retained by the parties to be used solely for the purpose of this litigation; and court officials involved in this litigation, including court reporters.

C. If Protected Material is disclosed through inadvertence or otherwise to any person not authorized to receive such information under this Agreement, the party causing such disclosure shall inform the person receiving the Protected Material that the information is covered by this Agreement, make its best efforts to retrieve the Protected Material, and such shall promptly inform the other party of the disclosure.

D. If the records that are the subject of this Order are used in any deposition, the same protection set forth in this Agreement shall apply; and the deposition tapes, exhibits, and all transcripts shall be permanently sealed and only used within the scope of this litigation.

E. All persons obtaining access to records under this Order shall use the information

only for legitimate discovery and the preparation for trial and trial of this case (including appeals and retrials). Such records shall not be used for any other purpose, and no one shall disclose such records to any person except as set forth herein. If there is an appeal in this action, appropriate action shall be taken to protect these records from public disclosure on appeal consistent with the provisions of this Order.

F. The Protected Material shall not be published outside of this litigation, nor shall it be made known to the minor child, directly or indirectly.

G. Notwithstanding any provisions of this Agreement, should any information obtained by Mr. Gilbert confirm the existence of child pornography on any of the subject devices, Mr. Gilbert, the parties, and their counsel shall be allowed to share such information with law enforcement and the Court.

AND IT IS SO ORDERED!

_____

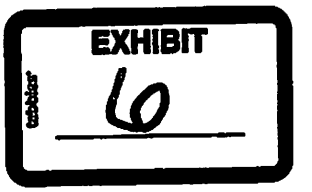
Family Court, Ninth Judicial Circuit

Charleston, South Carolina
January ____, 2017

FAILURE TO COMPLY WITH THIS ORDER WILL SUBJECT THE OFFENDER TO AN ORDER OF CONTEMPT WITH A POSSIBLE FINE, A PUBLIC WORK SENTENCE, OR BY IMPRISONMENT IN A LOCAL CORRECTIONAL FACILITY FOR ONE YEAR, A FINE OF FIFTEEN HUNDRED DOLLARS, OR A PUBLIC WORK SENTENCE OF MORE THAN THREE HUNDRED HOURS, OR ANY COMBINATION OF THEREOF, PURSUANT TO SECTION 63-3-620 OF THE CODE OF LAWS OF SOUTH CAROLINA, 1976, AS AMENDED.

Add signature blocks for parties' counsel and the pro se defendant and the GAL.

X v. Y
2018-DR-10-0001



X v. Y
Privilege Log Example

Bates No.	Description	Privilege
Def. Responses to Plaintiff's First RTP #0001	Email from Y to Minister 1/1/18 10:00 AM andMinister to Y 3/1/18 7:00 AM	Information redacted because it is protected under Priest Penitent Privilege.
Def. Responses to Plaintiff's First RTP #000349-#000422	Private Facebook messages between client and attorney	Information redacted is protected under the Attorney-Client & Work Product privileges.
Defendant's Supplemental Response to Plaintiff's First RFP Six #000466-#000662	Y's Facebook prior to date of marriage	Information is redacted as irrelevant and not reasonably calculated to lead to the discovery of relevant and/or admissible evidence.

STATE OF SOUTH CAROLINA)	IN THE FAMILY COURT FOR
)	THE NINTH JUDICIAL CIRCUIT
COUNTY OF CHARLESTON)	CASE NO.: 2015-DR-YYYYY
)	
XXXXXXX	
)	
Plaintiff,)	
)	
vs.)	**CONSENT CONFIDENTIALITY ORDER**
)	
)	
YYYYYYYY,)	
)	
)	
Defendant.)	
)	

WHEREAS, this litigation involves issues touching on child custody, visitation, child support, and attorneys' fees and costs; and,

WHEREAS, the parties anticipate that during the course of this litigation highly sensitive personal and financial information shall necessarily be exchanged and possibly provided to the Court and experts directly involved in this matter; and,

WHEREAS, given the nature of the allegations in this action as well as the total net worth of the parties, the disclosure or dissemination of personal and financial information normally exchanged in such cases may well put the safety and security of the parties' minor children at risk, and, may potentially harm the parties' ability to conduct their personal, professional, and financial dealings;

NOW, THEREFORE, to protect any documents or information provided by either party to the other, to their attorneys, to their respective experts, to the Court, or to any professional appointed to provide services during the course of this litigation, it is with the consent of the parties, hereby **ORDERED** that:

1. All such materials and information shall be deemed "Protected Material."

2. All Protected Material, shall be subject to the ***NON-WAIVER AND CONFIDENTIALITY AGREEMENT*** ("Agreement") as follows:

A. Any Protected Material disclosed in this litigation is to be considered confidential and proprietary to the producing party (or the party about whom or on whose behalf the information or materials is provided). The other party shall hold the same in confidence and shall not use any Protected Material other than for the purposes of this litigation. To that end, the parties shall limit the disclosure of all Protected Material only to those persons with a need to know the information for purposes of supporting their position in this litigation. Moreover, Protected Material will not be disclosed, published, or otherwise revealed to any other party, person, or entity except with the specific prior written authorization of the protected party. The current attorneys for the parties and any future attorneys for the parties, any experts retained by the parties or appointed by the Court, and any duly-appointed Guardian ad Litem in above-captioned matter are hereby authorized to receive "protected material" pertaining to the parties, to the extent and subject to the conditions outlined herein.

B. If Protected Material is used in this litigation, such records may only be disclosed to the parties; any Guardian ad Litem duly appointed; the attorneys (including the partners, associates, contractors, and employees of any attorney actively engaged in the conduct of this litigation); any expert witnesses retained by the parties to be used solely for the purpose of this litigation; and court officials involved in this litigation, including court reporters. Nothing herein will prohibit attorneys, parties, and experts from using the services of

professional copy shops to reproduce the documents, provided the said professional copy shops are served with a copy of this Protective Order and are advised that the Order is enforceable by this Court. Notwithstanding the foregoing, all persons who will see or otherwise review such records must sign the Acknowledgement attached to this Order, with copies of such Acknowledgements to be provided to all involved counsel before the records are seen or reviewed by such persons.

C. If Protected Material is disclosed through inadvertence or otherwise to any person not authorized to receive such information under this Agreement, the party causing such disclosure shall inform the person receiving the Protected Material that the information is covered by this Agreement, make its best efforts to retrieve the Protected Material, and shall promptly inform the other party of the disclosure.

D. If the records that are the subject of this order are used in any deposition, the same protection set forth in this Order shall apply; and the deposition tapes, exhibits, and all transcripts shall be permanently sealed and only used within the scope of this litigation.

E. All persons obtaining access to records under this Order shall use the information only for legitimate discovery and preparation and trial of this case (including appeals and retrials) and shall not use such information for any other purpose and shall not disclose such records to any person except as set forth above. If there is an appeal in this action, appropriate action shall be taken to protect these records from public disclosure on appeal consistent with the provisions of this Order.

F. The Protected Material shall not be published outside of this litigation, nor shall it be made known to the minor children, directly or indirectly.

G. The parties shall have no confidentiality obligations with respect to any information which 1) is or becomes publicly known otherwise than by the a party's breach of this Agreement; 2) is received by the requesting party without restriction from a third-party who is not under an obligation of confidentiality; 3) is approved for release by written authorization of the other party; or 4) is disclosed pursuant to court order, provided that the other party is notified at the time the request for such disclosure is made to any tribunal.

AND IT IS SO ORDERED!

_____
Family Court Judge,
Ninth Judicial Circuit

Charleston, South Carolina
November ____, 2015

FAILURE TO COMPLY WITH THIS ORDER WILL SUBJECT THE OFFENDER TO AN ORDER OF CONTEMPT WITH A POSSIBLE FINE, A PUBLIC WORK SENTENCE, OR BY IMPRISIONMENT IN A LOCAL CORRECTIONAL FACILITY FOR ONE YEAR, A FINE OF FIFTEEN HUNDRED DOLLARS, OR A PUBLIC WORK SENTENCE OF MORE THAN THREE HUNDRED HOURS, OR ANY COMBINATION OF THEREOF, PURSUANT TO SECTION 63-3-620 OF THE CODE OF LAWS OF SOUTH CAROLINA, 1976, AS AMENDED.

We move and consent:

_____
Melissa F. Brown, Esquire
Counsel for Defendant

Mark O. Andrews, Esquire
Counsel for Plaintiff

STATE OF SOUTH CAROLINA)	IN THE FAMILY COURT FOR
)	THE NINTH JUDICIAL CIRCUIT
COUNTY OF CHARLESTON)	CASE NO.: 2015-DR-XXXXX
)	
XXXXXX)	
)	
Plaintiff,)	
)	
vs.)	**PROTECTIVE ORDER**
)	
)	**ACKNOWLEDGEMENT OF RECEIPT**
YYYYYY,)	
)	
)	
Defendant.)	
)	

I acknowledge that I have received a copy of the Consent Protective Order dated November _____, 2015 and that I have read that Order, that I understand it, and that I agree to abide by its terms.

I further acknowledge that, under the terms of that Protective Order, I am forbidden to disclose to any person (other than those specified in the Order) the referenced information and documents that have been obtained in this action, and I am forbidden to use any such referenced documents for any purpose other than the conduct of Case No.: CASE NO.: 2015-DR-10-3023. I understand that all parties to CASE NO.: 2015-DR-10-3023 are direct and intended beneficiaries of my agreement to abide by the terms of the Protective Order.

I understand that if I violate the terms of that Order, I may subject to sanctions by the Court.

_____

Dated: _____, 2015

ELECTRONICALLY STORED INFORMATION:
THE LAWYERS' & CLIENTS' DUTIES
PART 1
[Day 2, Morning Session]

1. **Rule of Professional Conduct 1.1:**

   a. **ABA's Model Rules 1.1, Note 8:** "[A] lawyer... [must] keep abreast of changes in law and its practice, including the benefits and risks associated with relevant technology."

   b. **SCRPC 1.1, Note 6:** "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject."

2. **E-Discovery under the Federal Rules of Civil Procedure:**

   At the heart of the rule changes to Rules 1, 16, 26, 34 and 37 is the goal to provide lawyers and judges with the practical tools to help move E-Discovery along and keep the litigation costs down. The Rules also focus on keeping discovery in line with the proportionality of the case and they require the attorneys and litigants, in addition to the courts, to keep E-Discovery litigation costs down.

3. **ETHICS OPINIONS:**

   - "[C]ounsel has a general duty to **be aware of social media** as a source of potentially useful information in litigation, to be competent to obtain that information directly or through an agent, and to know how to make effective use of that information in litigation." **N.H. 2012.**

   - Lawyers who **lack competence in e-discovery** could violate CA's ethics rules and the attorney's duty of confidentiality. **CA 2015.**

   - "Rule 1.1 requires lawyer to provide competent representation to clients. Comment [8] to the rule specifically states that a lawyer" .... [should keep abreast of **relevant technology.**] **'Relevant technology' includes social media. NC 2015.**

   - An attorney or paralegal who **misuses social media by surreptitiously** friending a represented, opposing party on Facebook is subject to discipline. **NJ 2016.**

Social media and communication via ESI are here to stay, and their impact upon family law cases continues to grow. As of 2018's second quarter, Facebook had more than 2.2 billion active, monthly users. Twitter had 336 million active, monthly users who tweeted an average of 500 million tweets per day. Instagram, which is taking over Facebook that many consider outdated, now boasts 800 million users and 60 million posts per day. Each month, new forms of social media become available in addition to familiar programs such as YouTube, LinkedIn, SnapChat, Pinterest, Vimeo and What's App.

Since social media became popular and electronically stored information (ESI) became easier to retrieve, associated platforms have provided a treasure trove of valuable evidence in family law cases. Where it was previously potentially expensive to gather certain evidence, attorneys can now search social media and other public sites from the comfort of their own office to find information publicly available about the opposing party's habits, communications, photographs, lifestyles, whereabouts, interests, friends and even their assets. On the other hand, obtaining ESI requires different methods to retrieve, and retrieval as well as the duty to preserve information that may be reasonably related to the potential litigation can become quite costly if not handled properly.

Clearly, technology's usefulness is exciting and often time-efficient, but it can also create what seems like burdensome responsibilities for the client and attorney. In addition, having to keep up with the rapid advances in technology only adds to many responsibilities faced by attorneys who are simply trying to run their practices and comply with our Rules of Professional Conduct. Nevertheless, few can live without technology in today's world, and I challenge any lawyer who can find a case where technology does not play a role, even if technology relates only to the communication between the attorney and the court.

Thus, the ABA and at least 30 states have implemented rules to their Professional Conduct requirements that specifically address a duty regarding lawyers keeping abreast of technology.[1] Specifically, the ABA's Model Rules of Professional Conduct, Rule 1.1, places a huge responsibility upon all lawyers, stating that, "a lawyer... [must] keep abreast of changes in law and its practice, including the benefits and risks associated with relevant technology."

In the April 2014 Edition of the *ABA Journal*, U.S. Magistrate James C. Francis of New York was quoted as saying that he sees technological advances like e-discovery as so critical to the courtroom that he views attorneys who are unaware of its nuances as essentially engaging in a slow career suicide. *See* Joe Dysart, *Learn or Lose: Catch Up With Tech, Judges Tell Lawyers*, ABA Journal, April 2014 at 32. Judge Francis also added, "E-discovery is pervasive. It's like understanding civil procedure.... You're not going to be a civil litigator without understanding the rules of civil procedure. Similarly, you're no longer going to be

[1] https://www.lawsitesblog.com/2015/03/11-states-have-adopted-ethical-duty-of-technology-competence.html

able to conduct litigation of any complexity without understanding e-discovery." *See id.*

Most of the cases cited in this article are opinions written by federal judges regarding cases involving millions of dollars and almost matching litigation funds. The leading case law on ESI stems from the federal cases and clearly, the trickle-down impact has affected state court decisions. However, state court litigants and particularly family court litigants vastly differ from the litigants in federal court who typically have deep pockets and huge litigation expense accounts. As time has passed, though, even the federal courts became much more concerned with the incredible costs to manage, preserve and gather ESI. Ergo, the amendments to the FRCP.

Most lawyers should understand and be familiar with how various social media platforms work, what constitutes electronically stored information (ESI), methods to obtain ESI legally, methods to obtain non-public social media material legally, methods to authenticate such evidence to introduce at trial, when the duty to preserve begins, identification of what must be preserved, and methods to properly preserve evidence. Lawyers should also be fully aware of state and federal laws that impose criminal penalties and civil sanctions on anyone who improperly, sometimes even unintentionally, obtains or handles this evidence — both for the lawyer's and the clients' sake.

SOME BASICS

1. What is Electronically Stored Information (ESI):

ESI is information created, manipulated, stored, and best utilized in digital form.

2. When did ESI come about?

While some may think that ESI is a relatively new phenomenon, it first became relevant on the national horizon during the Iran-Contra affair. In the late 1980's, United States Senate investigators were able to retrieve 758 email messages sent by Ollie North to the Contras. These emails were the smoking gun that confirmed North's involvement in that operation despite his denials to a Senate Committee while under oath. Interestingly, North was convicted, but not for his involvement with selling arms to the Contras. Instead, he was convicted for perjury — lying to the Senate Committee about the emails while under oath.

3. Where is ESI located?

ESI is found on devices with electrical, digital, magnetic, wireless, optical or electromagnetic capabilities such as laptops, iPads, iPhones, iPods, tablets, Android Smartphones, etc. The devices, apps, and programs containing ESI are constantly evolving and the potential for their use in future litigation is limitless.

4. Why is ESI so important to the practice of family law aside from potential ethics violations?

Today, people use these various devices to communicate with others through emails, texts, pictures, videos, posts, tweets and the like. As such, these communications are often key evidence in family court cases.

CASES THAT ADDRESS THE IMPORTANCE OF LAWYERS UNDERSTANDING THE CLIENT'S DUTY TO PRESERVE

FEDERAL COURT CASES

1. *Zubalake v. UBS Warburg*, 216 F.R.D. 280, 283 n. 30 (S.D.N.Y. 2003):

As the law has evolved to keep up with technology, more judges have held attorneys liable for not properly advising their clients about how to preserve ESI. In 2003, Judge Shira A. Scheindlin, a federal judge in New York well known for her knowledge of technology and the use and abuse of e-discovery, cited the civil discovery standards and the scope of a litigant's duty to preserve electronic documents in her seminal decision, *Zubalake v. UBS Warburg*,. Now, most states have enacted e-discovery rules, and ESI is an explicit part of the last several round of amendments to the Federal Rules of Civil Procedure. The American Bar Association has written a good primer on these amendments.[2]

2. *Qualcomm Inc. v. Broadcom Corp.*, No. 05CV1958-B (BLM), 2008 WL 66932, at *9 (S.D. Cal. Jan. 7, 2008), *vacated in part*, No. 05CV1958-RMB (BLM), 2008 WL 638108 (S.D. Cal. Mar. 5, 2008):

In 2008, Magistrate Judge Barbara Major sanctioned Qualcomm and some of its retained attorneys for destroying tens of thousands of emails. *Qualcomm v. Broadcomm*, 2008 WL 66932 (S.D. Cal. Jan. 7, 2008).

3. *Sekisui America Corp. v. Hart*, 945 F.Supp.2d 494 (S.D.N.Y. Aug. 15, 2013):

Ten years after *Zubalaki*, Judge Scheindlin issued a scathing opinion and jury charge and held the Plaintiff's attorneys liable for not properly advising their client, Sekisui America Corporation, about how to preserve ESI data and for not ensuring that their client properly complied when responding to an e-discovery request. *Sekisui America Corp. v. Hart*. Judge Scheindlin also granted the Defendant's jury instruction request and charged the jury to assume that the Plaintiff's actions in deleting electronic documents were detrimental to the Defendant and that sanctions were appropriate.

---

[2]https://www.americanbar.org/publications/law_practice_home/law_practice_archive/lpm_magazine_articles_v32_is8_an7/

4. ***Green v. McClendon*, 2009 U.S. Dist. LEXIS 71860 (S.D.N.Y. Aug. 13, 2009):**

While the Plaintiff was punished in *Sekisui*, the Defendant's attorney was slammed in *Green v. McClendon*,. In *Green*, the judge held that the "litigation hold duty" *first runs to the lawyer* and only then attaches to the client. In that case, the court found that the lawyer failed to properly instruct the client to preserve relevant evidence and was thus personally liable—scary stuff for family court attorneys.

STATE COURT CASES & RULES

1. ***Allied Concrete Co. v. Lester*, 736 S.E.2d 699 (Va. 2013):**

Here, a Virginia personal injury lawyer learned the hard way that the consequences for not properly advising a client about the preservation of social media posts are severe. Here, the lead attorney's paralegal told the attorney that the personal injury client had pictures on his Facebook page that would be detrimental to his case. The attorney told the paralegal to take care of it. Later, it was discovered by the Defendant that the Facebook pictures were deleted. (The Defendant obtained copies of the photos before the Plaintiff deleted them.)

The real problem, though, was not the attorney's instruction to his paralegal to "clean up" the problem. The actions that resulted in the lead attorney being disbarred for 5 years was a result of him telling the opposing party that the pictures never existed when he knew they had existed and had advised his paralegal to tell the client to "clean up" the problem. Both the attorney and client were sanctioned by the trial court (lawyer $542,000 and client $180,000), and the trial court's ruling was affirmed by the Virginia Supreme Court.

The sanctions were extraordinarily harsh, but hopefully other attorneys will take note to avoid finding themselves in a similar predicament.

2. ***Carlucci v. Piper Aircraft Corp*, 102 F.R.D. 472, 486 (S.D. Fla. 1984):**

Here, the Court noted that a "reasonable" document retention program might survive judicial review and suggesting that "the good faith disposal of documents pursuant to a *bona fide*, consistent and reasonable document retention policy" might provide a justification for failing to produce documents in response to discovery requests.

3. **Rule 37(f), SCRCP:**

"Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as result of the routine, good-faith operation of an electronic information system."

4. ***Compare*** **ABA Litigation Task Force on Electronic Discovery, Standard 29(a)(iii) (Aug. 1999):**

"Unless a requesting party can demonstrate a substantial need for it, a party does not ordinarily have a duty to take steps to try to restore electronic information that has been deleted or discarded in the regular course of business but may not have been completely erased from computer memory"), with ABA Litigation Task Force on Electronic Discovery, November 2003 Draft Amendments to Electronic Discovery Standards, Standard 29(a)(iii) (Nov. 17, 2003) ("Electronic data as to which a duty to preserve may exist includes data that may have been deleted but can be restored", both available at http://www.fjc.gov/public/pdf.nsf/lookup/ElecDi12.pdf/$file/ElecDi12.pdf.

IMPORTANT TAKE-AWAYS

1. Before the Initial Consultation:

Lawyers should send a packet of materials to potential client materials to fill out before the initial consultation and that packet should include a form about Social Media, ESI & Cloud Based Services (Security Systems, Thermostats, Cameras, Locks, Music & the like) that can be controlled remotely from a Smart Phone. **FORM: SOCIAL MEDIA, ESI & CLOUD BASED SERVICES, EXHIBIT 1.**

2. At the Initial Consultation:

a. **Passwords:** Discuss the potential client's security measures regarding passwords on all electronic devices (smart phones, desk top computers, lap tops, iPads, gaming devices, digital recorders, video recorders, WiFi devices, digital cameras) social media platforms, Apple ID, cloud services and others.

(1) Discuss whether or not changing passwords would "tip" the opposing party about potential separation/litigation;

(2) Whether the OP knows the potential client's passwords or could easily guess them or knows the answers to security questions.

b. **Preservation of Evidence:** Begin at the IC and advise potential clients to preserve any information that might possibly be relevant to a future or ongoing action. In fact, Rule 3.4 of the South Carolina Rules of Professional Conduct makes this responsibility clear:

> **Rule 3.4** states in relevant part that **a lawyer** shall not "**unlawfully obstruct another party's access to evidence or unlawfully alter, destroy or conceal a document or other material having potential evidentiary value. A lawyer shall not counsel or assist another person to do any such act.**"

Clearly, since electronically stored information ("ESI") is as ephemeral as the arrangement of electrons of which it is comprised, extraordinary care is required to preserve this information **even before** the lawyer can review it.

3. When does the client's Duty to Preserve Evidence Arise?

a. The duty to preserve arises when a party knows or should have known that litigation is reasonably foreseeable. *Rimkus Consulting Group, Inc. v. Cammarata*, 688 F. Supp. 2d 598, 612-613 n. 7 (S.D. Tex. 2010)[3]. The test for "reasonable anticipation of litigation" varies state to state, but most cases from various jurisdictions hold that reasonable anticipation of litigation arises when a party knows there is a credible threat that it will become involved in litigation. *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 217 (S.D.N.Y. 2003).

b. South Carolina family law practitioners should expect courts to broadly apply these rules. In *King v. American Power Conversion Corp.*, 181 Fed. Appx. 363 (4th Cir. 2006), the Fourth Circuit Court of Appeals held the plaintiffs responsible for the destruction of evidence by a third party *despite the fact that they had themselves* had made efforts to preserve evidence. The court based its decision on the fact that the loss of evidence irreparably prejudiced the defendants. This case should serve as a reminder that attorneys should take special care to preserve and/or identify all evidence that they possess or even know about.

By sending a preservation letter, a party can definitively establish a date that serves as the very latest date that the duty to preserve could arise.

4. How does the lawyer ensure that the client's social media and ESI are preserved?

a. Assume that all clients' Social Media posts and ESI will be the subject of discovery. as part of the litigation. Therefore, **at the initial consultation** instruct the potential client about the importance of preserving evidence that is *reasonably expected to be relevant to the matter at hand*, and advise the potential client not to delete anything unless it is in the normal course of business.

b. Include ***in your notes*** and ***in a follow-up Preservation Letter*** to the potential client/client that the attorney orally instructed the party to preserve all evidence that might be relevant to the potential matter. **See *Electronic***

---

[3] See also *Bagley v. Yale University*, Civ. No. 3:13-CV-1890 (D. Conn. Dec. 22, 2016) (Duty arose before filing of suit and arguably when university staff exchanged emails noting plaintiff's threat of legal action). *Jones v. Bremen High Sch. Dist. 228*, No. 08-CV-3548 (N.D. Ill. May 25, 2010) (Duty arises when a par receives EEOC charges). *D'Onofrio v. SFZ Sports Group, Inc.*, No. 06-687 (D.D.C. Aug. 24, 2010) (Duty arises with receipt of a letter stating that the sender intended to initiate litigation).

Evidence for Family Law Attorneys, **Conlon J. Timothy and Hughes, Aaron (2017), Exhibit 1 "Preservation Letter" 139.**

5. What advice does the attorney give to potential and current clients about future social media posts, emails and texts that they are bound to make?

While many family law attorneys often advise clients to stop posting publicly on social media sites, such advice can also have **an underappreciated adverse effect**. In today's world, suggesting that a client change their lifestyle by not using social media is like suggesting that they not use their phones. Advising a party to "go dark" do more than cut the person off from friends, family, social groups, professional networking, hobbyist sites, and other interests. It can add unnecessary stress to the already huge amount of stressed caused by the divorce case.

Advise the client to observe their normal routines, but assume their worst enemy is reading every future post/text/email & imagine how it would look if this material was introduced as evidence in court.

6. How does the attorney advise the potential client/client to preserve material that might be relevant to the potential/pending action?

Despite many parties' best efforts, some evidence may nonetheless be destroyed, whether intentionally or unintentionally. Clearly, destruction could come from the unscrupulous litigant erasing posts or suddenly "losing" their phone or, after turning it over, using "Find My iPhone" to remotely wipe it clean.[4]

Less well known is the **unintentional destruction of evidence**: iPhones, for example, can be set to automatically delete all emails over thirty days old.

7. Four traditional ways to recover ESI and social media that has been destroyed:

When this evidence is intentionally destroyed, the four traditional ways to recover it are not always effective.

a. A criminal warrant for the device requires a showing of probable cause, and the device or devises will be in the custody of the police and not available for civil litigation.

---

[4] This can be prevented by having the phone dropped into a "Faraday Bag," an enclosure that isolates the phone from radio waves named after the English scientist Michael Faraday. Essentially, it is a sandwich bag made of aluminum foil that is cheap, lightweight and easy to use. *Riley v. California, 134 S. Ct. 2473, 2487* (2014).

b. A discovery subpoena to a third-party platform such as Facebook or Twitter under Rule 45, SCRCP, could be issued, but the responding party is entitled to at least 10 days' notice.[5]

c. A Request to Produce the physical device or an Interrogatory requesting the account information and password (such as in the *Vanderwege v. Vanderwege*—now pending before the South Carolina Supreme Court) would allow the receiving party to go straight to the platform and access the data directly. However, the responding party has a minimum of thirty (30) days within which to respond.

d. An *Ex Parte* Order prohibiting destruction of ESI along with an Order to bring a device to an emergency hearing, would require, at a minimum, an affidavit or verified pleading showing a substantial risk of irreparable injury, loss or harm that will result from the delay required to effect notice, and/or that notice itself will precipitate adverse action before an Order can be issued.

Such a high burden is difficult to meet, particularly at the beginning of a case; if it is attempted during the case after counsel has been retained, there will be the additional burden of issuing the Order without notice to opposing counsel or, if opposing counsel is notified, addressing whether that counsel can or cannot tell his client that his device will be inspected.

ANTI-SPOLIATION, LITIGATION HOLD & PRESERVATION WARNING LETTERS

Anti-Spoliation, Litigation Hold & Preservation Warning letters are a means to put the other side on notice to preserve and refrain from destroying any ESI evidence that might be related in any way to the litigation. The letters should remind opposing counsel of his duties under SCRPC 3.4 demand that counsel instruct his client not to change or destroy any ESI contained in any form.

Thus, it is common practice for a requesting party, as soon as it is determined that ESI will be an issue, to send the responding party an **anti-spoliation letter,**[6] putting the responding party on notice that ESI will be requested and that all past and future activity, whether through the use of online or cellular methods, be

---

[5] Even more complicated, many platforms refuse to comply with such subpoenas under the federal Secured Communications Act. *See e.g. J.T. Shannon Lumber Co. v. Gilco Lumber Inc.*, No. 2:07-cv-119, 2008 WL 3833216 (N.D. Miss. 2008), *reconsideration denied*, 2008 WL 4755370, at *1 (N.D. Miss. 2008) (The court found the "statutory language clear and unambiguous" and ruled that a Rule 45 subpoena does not constitute an exception to the SCA allowing an ECS provider to divulge the contents of communications. Having a court order a party to sign a waiver is likewise problematic as many platforms such as Facebook include in their terms of use a clause that provides the user will not share his or her user name and password.)

[6] The term Anti-Spoliation letter is sometimes referred to as a "Litigation Hold letter" or a "Duty to Preserve letter."

preserved, including disabling any automatic deletion protocols. **FORM ANTISPOLIATION, LITIGATION HOLD LETTER, EXHIBIT 2. See also, *Electronic Evidence for Family Law Attorneys*, Conlon J. Timothy and Hughes, Aaron (2017) Exhibit 2, "Preservation Letter (Opposing Party)" P. 139.**

When all South Carolina lawyers already have the ethical obligation to advise clients to preserve all materials that might potentially be relevant to the potential or pending litigation, *why would it help to send such letters to the opposing party?*

1. **Failure to comply with an anti-spoliation notice**: Failure to comply can carry substantial risks such as:

a. The risk to the case itself: in some situations, the timing of any smashing of hard drives or deletions and over-writing of emails can be reconstructed but,

b. Even if not, the fact such destruction took place at all after notification raises problems for the responding party during the discovery phase of the case and opens that party to impeachment at trial.

c. More significantly, where parties and sometimes their attorneys are found guilty of deleting evidence, courts have considered **a range of consequences ranging from financial sanctions to disbarment**, *Lester at* 285 Va. 295, 736 S.E.2d 699, to a negative inference sanction, *Zubulake v. UBS Warburg LLC,* 217 F.R.D. 309, 311 (S.D.N.Y. 2003). *Cf. Hawkins v. Coll. of Charleston,* No. 2:12-CV-384-DCN, 2013 WL 6050324 (D.S.C. Nov. 15, 2013), where the Court declined to dismiss the Plaintiff's case for deleting some of his Facebook pages because the Court found the Plaintiff's actions did not prejudice the Defendant.

2. **What other benefits might result from sending an anti-spoliation letter?**

a. *Notice* has even more horsepower if anti-spoliation language is included in a Temporary Order or even an *Ex Parte* Order granting an emergency hearing.

b. Among the protections available to both parties would be a provision that the requesting party have a forensic computer expert at the hearing who is able to take possession, perhaps immediately, of the opposing party's phone to download its data and safekeep it *without examination* and then return the device so it can be used by the owner.[7]

---

[7] A common practice, at least with respect to information stored on devices such as computers with hard drives, is for a technician to copy, or "ghost," all the information onto a second and third hard drive and then return the original to the owner so the owner does not lose use of it. The second hard drive is preserved unmolested as a safety and the third is then inspected using appropriate programs, particularly useful when there is so much data as to be impossible to manually search, similar to doing computerized legal

3. What entails a showing of good faith?

A showing of good faith has always been necessary when responding to discovery or any other court-ordered instruction; however, the **burden of showing good faith is now significantly greater** on the responding party.

Attorneys cannot claim, for example, that they did not know about those backup tapes stored in a closet because they lacked access to relevant IT personnel. Instead, attorneys must have proactive conversations with ESI custodians and IT stewards to create and maintain documentation regarding what preservation actions were taken when the obligation arose, how the chain of custody was assured, and how both custodians and relevant ESI repositories were systematically identified.

4. Facebook spoliation cases and contrasting rulings by different state and federal courts:

a. *Examples Where Parties Were Sanctioned for Spoliation of Facebook evidence:*

(1) In *Gatto v. United Air Lines, Inc.*, No. 10-CV-1090-ES, 2013 WL 1285285 (D.N.J. March 25, 2013), the Plaintiff argued that he did not destroy his Facebook account but had instead merely deactivated it. However, the record included additional evidence indicating that he did take additional steps *to permanently delete* his account.

As a sanction, the court gave an adverse inference instruction, finding that the sanction was appropriate (i) the evidence was in Gatto's control; (ii) there was an actual suppression or withholding of evidence; (iii) the destroyed evidence was relevant to the claims in the matter; and (iv) it was reasonably foreseeable that the evidence was discoverable. The court, however, denied the defendant's request for an award of attorneys' fees and costs.

(2) See also Allied Concrete Co. v. Lester, 736 S.E.2d 699 (Va. 2013) discussed earlier in the article.

b. *Cases Where Parties Were Not Sanctioned for Spoliation of Facebook Evidence:*

(1) In *Hawkins v. College of Charleston*, No. 2:12-CV-384 DCN (D.S.C. November 15, 2013), the court denied the Defendant's motion to dismiss as a sanction for the Plaintiff, a former College of Charleston student,

---

research for specific terms rather than manually going through the entire contents of a law library.

deleting some of his Facebook pages. Although it was clear that the destruction of the ESI was intentional, the court concluded that any prejudice suffered by the Defendant was slight.

(2) In *Osburn v. Hagel*, 2013 WL 6069013 (MD Ala. Nov. 18, 2013), the court determined that sanctions were not appropriate where the Facebook account holder normally deleted her conversations and that her actions were in her normal course of behavior prior to receiving discovery requests for this information.

WHY ISN'T THE LAW KEEPING UP WITH ADVANCEMENTS IN TECHNOLOGY?

To date, the federal courts are typically the first to address issues related to the many advances in technology. In fact, the trickle down effect is a historical fact given so many states adopt the federal rules such that their state rules are identical or substantially similar to the Federal Rules.

Given the challenges involved with E-Discovery, which include the costs of preservation and the costs of gathering the materials from the other party, the federal courts created Committees to study amendments to the Federal Rules of Civil Procedure.

On December 1, 2015, amendments to Federal Rules of Civil Procedure 1, 16, 26, 34 and 37 were implemented. Much thought and study were put into these amendments and this author's opinion is that state court attorneys should become aware of the dramatic changes in the rules specific to E-Discovery because history shows that it will not be long before South Carolina adopts the federal court's amendments to our Rules of Civil Procedure. In fact, state courts have routinely used the Federal Rules to fill any gap in their own rules. Such gap-filling has occurred in most areas of the law, and family law attorneys should know the rules so that they can use them as a sword or shield if presented with a situation not immediately resolvable by reference to the state rules.

SUMMARY OF THE MOST IMPORTANT CHANGES TO THE FEDERAL RULES OF CIVIL PROCEDURE 1, 16, 26, 34 & 37

1. **Rule 1** was amended to make it so that *parties*, as well as the courts, now have a duty to interpret and use the rules to "to secure the just, speedy, and inexpensive determination of every action and proceeding." The Advisory Committee Notes state that: "Effective advocacy is consistent with — and indeed depends upon — **cooperative** and **proportional use of procedure**."

2. **Rule 16** amendments are made to reduce the time to enter scheduling orders to the earlier of 90 days (previously 120 days) after a defendant has been served or 60 days (previously 90 days) after a defendant has made an appearance. The rules allow scheduling orders to include preservation provisions and clawback agreements.

3. Rule 26 is significantly changed in several key respects.

a. Rule 26(b)(1) is changed in four major respects.

(1) Proportionality requirements have been restored. The factors identify what factors must be considered in determining whether discovery is proportional to the needs of the case. They include the importance of issues at stake, 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.

(2) The amendment eliminates language regarding the discovery of sources of information, but the Notes make clear that such information is discoverable where appropriate.

(3) The new rule does not contain a provision allowing a court to order discovery on matters "relevant to the subject matter involved in the action." The Notes state that such language is unnecessary given the addition of proportional discovery.

(4) The phrase "reasonably calculated to lead to the discovery of admissible evidence" is eliminated. Under the new rule, an objection based on the "reasonably calculated" language is no longer a basis for objecting to discovery requests as being overly broad.

b. Rule 26(d)(2) no longer prevents parties from issuing discovery requests prior to the Rule 26(f) conference. Under the amendment, the parties may issue requests for documents 21 days after service of the summons and complaint, although such early requests are not deemed served until the Rule 26(f) conference takes place. This amendment relates to the duty of preservation because it will be difficult for a party to claim that it could not have reasonably foreseen the relevance of the information if it has actually been placed on notice that the opposing party seeks production of the information.

c. Rule 26(f)(3) now requires that a discovery plan must state the parties' views on disclosure, discovery, or preservation of ESI. The significant change is the addition of the word "preservation." The rule further states that the discovery plan must indicate whether the parties want the court to enter an order containing any agreements they have reached under Rule of Evidence 502 regarding limitation on waivers due to the inadvertent disclosure of attorney work product or attorney-client communications. The incorporation of a Rule 502 order may expand the court's reach with respect to third parties and other actions.

4. Rule 34(b), as amended, sets forth the procedures that a party must use in responding to ESI requests and objecting to such requests.

a. The amendment states that objections must be made "with specificity." No boilerplate objections will be allowed. This change reflects the language in Rule 33 dealing with responses to interrogatories. Further, the new rule requires an objecting party to disclose whether it is withholding documents based on the objection. This amendment seeks to prevent a party from making a general objection and simultaneously producing documents, leaving the other party to wonder whether additional documents are being withheld on the basis of the objection.

b. Another important change relates to *how* ESI may be produced. This change addresses the common practice of producing information rather than allowing inspection but makes clear that a party that designates that it will produce rather than allow inspection must produce the information by the deadline set forth in the request, or by a reasonable deadline set forth in the response. This change is intended to curb the practice of promising to deliver the information "in due course" by setting firm dates for production.

5. Rule 37(e), as amended, deals with the loss of ESI and establishes a clear standard for spoliation sanctions and curative measures, distinguishing between the negligent and intentional loss of information.

a. The new rule deals with ESI "that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery." If another party is prejudiced by the loss of ESI, a court "may order measures no greater than necessary to cure the prejudice.

b. *But* if the party acted with *specific intent* to deprive the other party of the information, the court may (1) "presume that the lost information was unfavorable to the party"; (2) "instruct the jury that it may or must presume the information was unfavorable to the party"; (3) "dismiss the action or enter a default judgment." The Committee states that the rule "recognizes that 'reasonable steps' to preserve suffice; it does not call for perfection."

c. It should be emphasized that even the intentional destruction of ESI does not justify one of the three harsh sanctions unless the destruction was done *for the purpose* of depriving the other party of the information. For example, a party may intentionally delete information on a hard drive for the purpose of freeing up memory, and such action would only justify proportional remedial measures because the deprivation would be negligent even though the destruction was intentional. However, if the destruction was done to keep the other party from getting the information, the court may order one of the three punitive measures.

See the following materials that include more detailed explanation of the amendment to the E-Discovery sections of the Federal Rules of Civil Procedure as well as many forms and checklists.

E-Discovery Guide to FRCP from Kroll, EXHIBIT 3.

Minnesota Federal Courts Checklists regarding the new amendments about E-Discovery to FRCP, EXHIBIT 4.

LUNCH TIME HOMEWORK

1. **Is this a proper Interrogatory request? Why or Why Not?**

   Identify all social media accounts to which you have had access in the last three years. For each account, include the username and password you used to access each account.

   _____

   _____

   _____

   _____

   _____

2. **Is this a proper objection to the Interrogatory request? Why or Why Not?**

   Defendant objects to Interrogatory No. 18. The information sought is not relevant to the subject matter of the pending action, or if so, does not outweigh the prejudice to Defendant's constitutional right to privacy. Further, the information sought does not appear calculated to lead to the discovery of admissible evidence.

   _____

   _____

   _____

   _____

TECHNOLOGY, THE INTERNET, THE CLOUD, SOCIAL MEDIA & ELECTRONICALLY STORED INFORMATION (ESI)

****

#1: Do you know your home WiFi Name & Password?

Name: _____

Password: _____

****

If you do not know this information, it is very important that you find out the answer from the person who set up your home system.

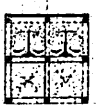
Why important? If you and your spouse are separated and your spouse set up the WiFi in the marital home where you remain, your spouse can still control any cloud based system in your home remotely using the original logins.

What systems do you mean? Cloud based security systems, thermostat systems, sound systems, alarm systems, door locking systems, camera systems, etc can be controlled by your spouse. This means that your spouse may be able to watch you, film you, record you, lock & unlock your doors, enter the home when you are present, watch your & your guests' comings and goings.

1st step: Change your home's WiFi username & password.

2. If you do not know your home WiFi password, immediately unplug your system to cut off all the cloud based systems' access through the current WiFi and do not plug in or turn on your current WiFi until you have changed the user name and password. If you cannot change the WiFi username and password (perhaps, for example, your cable company is the provider and this service is still in your spouse's name). Then, another option is to purchase a different WiFi device for your home.

3. Given the many other options, we will discuss other options during our meeting.

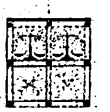


Please list all devices owned by you that are capable of accessing the Internet, GPS capability, sending text messages and emails. (Exs. Smart Phone, iPad, tablet, laptop, desktop, Alexa, Google Device, Smart Watch, & the like.)

DEVICE	OWNER	PROVIDER	WHO PAYS BILL	PASSWORD PROTECTED	WHO KNOWS PASSWORD?	ANYONE ELSE HAVE ACCESS TO DEVICE?
EX. iPhone	*W*	*AT&T*	*H*	*Yes*	*W & children*	*Children*

Please list all devices capable of taking pictures, videos and audios that you use or are set up at your home or office. (Exs. Smart Home Security Systems, Remotely Controlled ThermoStat device, theNest, Ring, Camera, Video Equipment, Audio Equipment, Nanny Cam, and the like.)

DEVICE	OWNER	PROVIDER	WHO PAYS BILL	PASSWORD PROTECTED	WHO KNOWS PASSWORD	WHO RECEIVES NOTICES
EX. Ring	*W*	*Ring*	*W*	*Yes.*	*W*	*W&H*



Please list all Social Media Sites, Platforms and Professional sites that you have signed up for in the past whether or not the account still exists. (Exs: Facebook, Professional Facebook, Instagram, SnapChat, YouTube, Twitter, LinkedIn, AVVO, Martindale Hubbell, Google, Pinterest, and the like.)

PLATFORM	DATE OPENED	USERNAME	PASSWORD PROTECTED	WHO KNOWS PASSWORD	DATE CLOSED
EX. Facebook	*DEC 2012*	*MelissaFullerBrown*	*Yes*	*W*	*Open*

Please list all dating sites that you have used in the past. (Ex. Match, POF, EliteSingles, Tinder, Bumble, MillionaireMatch, etc)

DATE OPENED	ONLINE NAME	WHO PAYS BILL	PASSWORD PROTECTED	WHO KNOWS PASSWORD	NOTICES SENT? & IF SO, WHERE & DEVICES
June 2018	*SCMan*	*H*	*Yes.*	*H*	*Yes. To my email account, [redacted], which goes to my iPhone, laptop & iPad.*

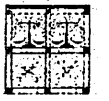


EXHIBIT
tabbies
2

Melissa Fuller Brown, Esquire
56 Wentworth St., Suite 100
Charleston, SC 29401

Melissa F. Brown, LLC
Attorney at Law

843-722-8900 (T)
843-722-8922 (F)
melissa@melissa-brown.com

June 7, 2018

SENT VIA EMAIL & US MAIL
ATTORNEY
Street
Charleston, SC 29401

Re:
Case No.:

Dear Attorney:

As you know, in the course of handling family law cases, we sometimes run into situations where one party destroys (or spoliates) relevant evidence. I hope no destruction of evidence has already occurred in this matter. Based upon some of your client's allegations, we have reason to believe that he and, possibly you, are in possession of materials and information pertinent to our representation of Mrs. Deleot. Accordingly, in connection with our ethical and legal obligations, I am required to send this letter to you and thereby make the requests outlined below. I certainly trust that you understand our position in this matter, and we hope we can all proceed in a business-like fashion in such respects.

Therefore, this letter relates to the potential spoliation of documents, records, memorializations, tangible things, electronically stored information, data, storage systems, computers, hard drives, storage devices, and/or other material that may be discoverable and/or relevant in connection with legal matters, which may potentially involve you and/or others with whom you may have business and/or personal relations. Our representation and the associated legal and equitable matters may involve, among others, issues related to family law, accounting finances, and/or the preservation of assets and information. Accordingly, it is critically important that any and all documents, records, memorializations, tangible things, electronically stored information, data, and/or other material, regardless of form or format, which may be discoverable and/or relevant, be preserved inviolate until a Court of competent jurisdiction permits the alteration or destruction of such.

Therefore, we hope that Mr. Deleot will preserve and retain any and all documents, records, memorializations, tangible things, electronically stored information, data, storage

systems, computers, hard drives, storage devices, and/or all other material, regardless of form or format, which may be discoverable and/or relevant in connection with any claims and/or potential claims which our clients may have involving these matters.

This letter is intended to reach not only those named specifically above but also all businesses, enterprises, companies, partnerships, corporations, limited liability companies, and/or any and all other entities controlled or operated by the aforementioned persons and/or entities, or in which they have any interest of any nature, and any predecessors, successors, parents, subsidiaries, divisions, or affiliates, and its respective officers, directors, agents, attorneys, accountants, employees, partners, or other persons occupying similar positions or performing similar functions as it relates to the pending action between the parties.

This letter is also intended to reach all documents, records, memorializations, tangible things, electronically stored information, data, storage systems, computers, hard drives, storage devices, and/or other material of any and every nature, regardless of form or format that may be discoverable and/or relevant pursuant to Rules of Court. But, we hope that this letter should not be parsed or dissected in an attempt to circumvent or undermine its meaning. Instead, it is intended to be all encompassing; any doubt or question as to its reach or intent should be resolved in favor of preservation and retention. Therefore, no part or portion of such materials may be destroyed, altered, hidden, discarded, written over, mutilated, alienated, hypothecated, encumbered, sold, donated, given to others, secreted, diminished, decreased in value, deleted, erased, or otherwise rendered unproducable to any extent whatsoever.

You should anticipate that some of the information subject to disclosure or responsive to discovery in this matter may be stored on Mr. Deleot current and former computer/s, computer systems, online repositories, hard drives (external and/or internal), digital or other cameras, PDAs, smart phones, iPhones and all generations of iPhones, iPads and all generations of iPads, iPod and all generations of iPod's, iTouch and all generations of iTouch, other electronic devices, telephones, and/or cell/wireless phones. Such may also be stored, preserved, and/or maintained in some other form or format, e.g., paper, and such may or may not be stored, retained, and/or maintained off site in the past, currently, or in the future.

Electronically stored information (hereafter "ESI") should be afforded the broadest possible definition and includes (by way of example and not as an exclusive list) potentially relevant information electronically, magnetically, or optically stored as:

1. Digital communications (e.g. e-mail, voicemail, instant messaging, texting), including, but not limited to, any and all email messages to and/or from your client; Word processing documents, including drafts and metadata (created by and/or stored in Word or WordPerfect or other word processing programs);
2. Spreadsheets and Tables (e.g., Excel or Lotus 123 worksheets);
3. Accounting Application Data (e.g., Quickbooks, Money, Peachtree Data

Files);

4. Image and Facsimile Files (e.g., .PDF, .TIFF, .JPG, .GIF images);
5. Sound Recordings (e.g.,.WAV and .MP3 files);
6. Video and Animation (e.g., .AVI, .MOV files);
7. Databases (e.g., Access, Oracle, SQL Server data, SAP);
8. Contact and Relationship management Data (e.g., Outlook and ACT!);
9. Presentations (e.g., Powerpoint, Corel Presentations);
10. Network Access and Server Activity Logs;
11. Project Management Application Data;
12. Computer Aided Design/Drawing Files; and/or,
13. Backup and Archival Files (e.g., Zip, .GHO).

ESI may be located not only in areas of electronic, magnetic, and optical storage media reasonably accessible to you, but also in areas you may deem not reasonably accessible. You are obligated to preserve potentially discoverable evidence from all sources and locations of ESI even if you do not anticipate producing such ESI.

The request contained herein that you preserve both accessible and inaccessible ESI is reasonable and necessary. Please be aware that even ESI that you deem reasonably inaccessible must be preserved in the interim so as to avoid depriving my client of his right to secure evidence or the Court of its right to adjudicate the issue.

In addition to the above, regardless of format or form or manner of storage, and without limitation, you should immediately undertake to preserve for the period commencing **from the time you first contemplated a family court action** and proceeding forward in time and continuing until released by Court Order, all itineraries, calendars, debit and/or credit card statements and/or bills and/or invoices, airline and/or other common carrier tickets, receipts, boarding passes, invoices, bills, charges, and the like; private transportation tickets, receipts, boarding passes, in voices, bills, charges, and the like; hotel/motel and other similar accommodation bills, invoices, charges, receipts, and the like; all banking and/or financial institution statements, records, notifications, checks, registers, stubs, data entries, drafts, draft records, communications, and the like. All social media pages, including, but not limited to, Facebook, LinkedIn, MySpace, Instagram, Twitter, YouTube, chatrooms, message boards, instant messaging, and the like.

Preservation Requires Immediate Intervention

This requires immediate action on your part to preserve potentially discoverable and/or relevant evidence, including, but not limited to, ESI, which in any way may relate to our client's potential claim(s). You must maintain all computers and any and all component parts, internal and/or external.

Adequate preservation of evidence, especially, but not limited to, ESI, requires more than simply refraining from efforts to destroy or dispose of such evidence. You must also intervene to prevent loss due to routine operations and employ proper techniques and protocols suited to protection of all such evidence, including, but not limited to, ESI. Please

be advised that sources of ESI are altered and erased by continued use of your computers and other devices. Booting a drive, examining its contents, or running any application will irretrievably alter the evidence it contains and may constitute unlawful spoliation of evidence. Consequently, alteration and erasure may result from failing to act diligently and responsibly to prevent loss or corruption of ESI.

Nothing in this demand for preservation for ESI should be understood or construed to diminish your concurrent obligation to preserve documents, tangible things, and/or all other potentially discoverable and/or relevant evidence.

Suspension of Routine Destruction

It is advisable to initiate immediately a litigation hold for potentially relevant ESI, documents, and tangible things, and to act diligently and in good faith to secure and audit compliance with such litigation hold. It is also advisable immediately to identify and modify or suspend features of your information systems and devices that, in routine operation, operate to cause the loss of potentially discoverable and/or relevant ESI. Examples of such features and operations include:

1. Purging the contents of e-mail repositories by age, capacity, and/or other criteria;
2. Using data or media wiping, disposal, erasure, or encryption utilities, and/or devices;
3. Overwriting, erasing, destroying, and/or discarding back up media;
4. Re-assigning, re-imaging, or disposing of systems, servers, devices, and/or media;
5. Running antivirus or other programs effecting wholesale metadata alteration;
6. Releasing and/or purging online storage repositories;
7. Using metadata stripper utilities;
8. Disabling server and/or IM logging; and/or
9. Executing drive and/or file defragmentation and/or compression programs.

Guard Against Deletion

Unfortunately, employees, officers, co-workers or others may seek to hide, destroy, and/or alter ESI and/or act to prevent and/or guard against preservation, retention, and/or disclosure. Especially where company machines have been used for internet access or personal communications, users may seek to delete and/or destroy information that they regard as personal, confidential, and/or embarrassing and, in so doing, may violate the duty to retain and preserve; discoverable and/or relevant material and/or information is not necessarily rendered undiscoverable and/or irrelevant simply because it may be regarded as personal or embarrassing. Compounding the potential problem, deleting and/or destroying such allegedly personal material and/or information may also delete or destroy potentially relevant ESI that is not personal. This concern is not one unique to you or your employees and officers. It is simply an event that occurs with such regularity in electronic discovery efforts that any custodian of ESI and counsel are obliged to anticipate and guard against its occurrence.

Servers

With respect to servers like those used to manage electronic mail (e.g., Microsoft Exchange Lotus Domino) or network storage (often called a user's "network share"), the complete contents of each user's network share and e-mail account should be preserved. There are several ways to preserve the contents of a server depending upon its RAID configuration and whether it can be shut down or must be online 24/7. If you question whether the preservation method you pursue is one that is sufficient, please understand the duty to preserve is inviolate.

Home Systems, Laptops, Online Accounts, and Other ESI Venues

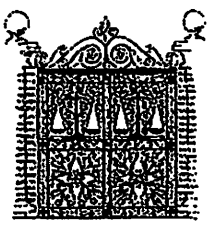
Although swift action to preserve data on office workstations and servers must be taken, you should also determine if any home or portable systems may contain potentially relevant data. To the extent that officers, board members, employees, accountants, or attorneys have sent or received potentially relevant e-mail messages or created or reviewed potentially relevant documents away from the office, you must preserve the contents of systems, devices, and media used for these purposes (including not only potentially relevant data from portable and home computers, but also from portable thumb drives, CD-R disks, and the user's PDA, telephones, smart phone, iPhones and all generations of iPhones, iPads and all generations of iPads, iPod and all generations of iPod's, iTouch and all generations of iTouch, voice mailbox, and/or other form of ESI storage). Similarly, if employees, officers, accountants, attorneys, or board members used online or browser-based-e-mail accounts and services (such as AOL, Gmail, Yahoo, or the like) to send or receive potentially relevant messages and attachments, the contents of these account mailboxes (including by way of example, Sent, Deleted, and Archived Message folders) should be preserved.

Ancillary Preservation

It is important and imperative to preserve the documents and other tangible items that may be required to access, interpret, and/or search potentially relevant ESI including, but not limited to, logs control sheets, specification, indices, naming protocols, file lists, network diagrams, flow charts, instruction sheets, data entry forms, abbreviation keys, user ID, and/or password rosters, key codes, access codes, or the like.

It is also important and imperative to preserve any passwords, keys, or other authenticators required to access encrypted files or standard CD or DVD optical disk drive if needed to access the encrypted files or run applications, along with installation disks, user manuals, and license keys for applications required to access the ESI.

It is also important and imperative to preserve any cabling, drivers and hardware, floppy disk drive, and/or standard CD or DVD optical disk drive, if needed to access or interpret devices on which ESI is stored. This includes tape drives, bar code readers, Zip drives, and other legacy or proprietary devices.



Melissa F. Brown, LLC
Attorney at Law
www.melissa-brown.com

Preservation Protocols

A successful and compliant ESI preservation effort requires expertise and the implementation of efficacious forensic protocols. If you do not currently have such expertise at your disposal, we urge you to engage the services of an expert in electronic evidence and computer forensics.

Do Not Delay Preservation

Please proceed promptly to implement appropriate protocols for the retention and preservation of discoverable and/or relevant evidence, regardless of form or format. Again, in order to be safe and compliant, it is best to conclude that all material is discoverable and relevant. Your implementation of such protocols will likely avoid spoliation of evidence, a result all involved should advocate and endorse.

Confirmation of Compliance

Please confirm that you have taken the steps to preserve ESI, tangible documents, and all other evidence, and materials, regardless of form or format, which is potentially discoverable and/or relevant to our client's potential claims. Thank you for your attention to this matter.

Of course, my client agrees to abide by these same preservation of evidence procedures. We look forward to receiving your confirmation of compliance as well as that of your client's and any of his representatives or others who have assisted her including but not limited to your staff and anyone else acting on her behalf or providing advice to him in this matter.

With kindest regards, I am

Very truly yours,

Melissa F. Brown

MFB/jw
cc: Client, *via email only*

Melissa F. Brown, LLC
Attorney at Law
www.melissa-brown.com

Featuring December 2015 Amendments

Federal Rules of Civil Procedure

Ediscovery Guide

Practical Analysis for Organizations and Legal Teams

Brought to you by KLDiscovery

KLDiscovery™

First Edition: December 2015
Minneapolis, MN

Federal Rules of Civil Procedure

Ediscovery Guide

Practical Analysis for Organizations and Legal Teams

Brought to you by KLDiscovery

KLDiscovery

Introduction

On December 1, 2015, significant changes to the Federal Rules of Civil Procedure (Rules) affecting the legal discovery of electronically stored information (ESI) became effective for cases then pending or thereafter commenced. At the heart of the amendments is a renewed effort to provide judges and lawyers with practical tools to help move the discovery process along and keep costs in control. The amendments, including revisions to Rules 1, 16, 26, 34, and 37, are intended to provide new guidelines on the scope of discovery and the spoliation of ESI while emphasizing the need for proportionality and cooperation between parties.

Now, more than ever, both counselor and client will need to familiarize themselves with the rules changes and prepare for their impact on ediscovery. To that end, this guide provides the text of the major rules amendments and the accompanying Committee Notes. It also examines their impact on key ediscovery rule provisions, along with analysis for organizations and their legal teams.

For the latest ediscovery case law and statutory updates, visit www.KLDiscovery.com.

RULE 1

Scope and Purpose

New Rule Provisions

These rules govern the procedure in all civil actions and proceedings in the United States district courts, except as stated in Rule 81. They should be construed, ~~and~~ administered, and employed by the court and the parties to secure the just, speedy, and inexpensive determination of every action and proceeding.

Committee Note

Rule 1 is amended to emphasize that just as the court should construe and administer these rules to secure the just, speedy, and inexpensive determination of every action, so the parties share the responsibility to employ the rules in the same way. Most lawyers and parties cooperate to achieve these ends. But discussions of ways to improve the administration of civil justice regularly include pleas to discourage overuse, misuse, and abuse of procedural tools that increase cost and result in delay. Effective advocacy is consistent with—and indeed depends upon—cooperative and proportional use of procedure.

This amendment does not create a new or independent source of sanctions. Neither does it abridge the scope of any other of these rules.

Amendment Analysis

Courts and Parties Share Responsibility for Effective Litigation

The amendment to Rule 1 is subtle, but important. The added language emphasizes that litigants and their attorneys, not just the courts,

have a responsibility to make litigation as efficient as possible. The Committee Note recognizes the balancing act between the adversarial nature of litigation and necessary cooperation throughout the litigation process. While the Committee Note states that this amendment does not mandate cooperation, it does highly encourage it and it foreshadows the emphasis on proportionality that runs throughout the amendments.

Impact for Corporations and Law Firms

Cooperation is Key in Discovery

Litigation by its very nature is adversarial. Nonetheless, even the most cutthroat lawyers understand the importance of cooperation and the impact that collaboration can have on the case budget and the overall outcome of the matter. When it comes to ediscovery, moreover, the case for cooperation is even more compelling given the complicated technical protocols and intersecting roles amongst inside counsel, law firms and service providers. The open question that organizations and counsel will need to deliberate going forward is how this renewed focus on cooperation will best translate into effective arrangements with the opposing party.

RULE 16

Pretrial Conferences; Scheduling; Management

New Rule Provisions

(b) Scheduling.

(1) *Scheduling Order.* Except in categories of actions exempted by local rule, the district judge—or a magistrate judge when authorized by local rule—must issue a scheduling order:

(A) after receiving the parties' report under Rule 26(f); or

(B) after consulting with the parties' attorneys and any unrepresented parties at a scheduling conference ~~by telephone, mail, or other means~~.

(2) *Time to Issue.* The judge must issue the scheduling order as soon as practicable, but ~~in any event~~ unless the judge finds good cause for delay, the judge must issue it within the earlier of ~~120~~90 days after any defendant has been served with the complaint or ~~90~~60 days after any defendant has appeared.

(3) Contents of the Order.

* * * * *

(B) Permitted Contents. The scheduling order may:

* * * * *

(iii) provide for disclosure, or discovery, or preservation of electronically stored information;

(iv) include any agreements the parties reach for asserting claims of privilege or of protection as trial-preparation material after information is produced, including agreements

16

reached under Federal Rule of Evidence 502;

(v) direct that before moving for an order relating to discovery, the movant must request a conference with the court;

(vvi) set dates for pretrial conferences and for trial; and

(vivii) include other appropriate matters.

Committee Note

The provision for consulting at a scheduling conference by "telephone, mail, or other means" is deleted. A scheduling conference is more effective if the court and parties engage in direct simultaneous communication. The conference may be held in person, by telephone, or by more sophisticated electronic means.

The time to issue the scheduling order is reduced to the earlier of 90 days (not 120 days) after any defendant has been served, or 60 days (not 90 days) after any defendant has appeared. This change, together with the shortened time for making service under Rule 4(m), will reduce delay at the beginning of litigation. At the same time, a new provision recognizes that the court may find good cause to extend the time to issue the scheduling order. In some cases it may be that the parties cannot prepare adequately for a meaningful Rule 26(f) conference and then a scheduling conference in the time allowed. Litigation involving complex issues, multiple parties, and large organizations, public or private, may be more likely to need extra time to establish meaningful collaboration between counsel and the people who can supply the information needed to participate in a useful way. Because the time for the Rule 26(f) conference is geared to the time for the scheduling conference or order, an order extending the time for the scheduling conference will also extend the time for the Rule 26(f) conference. But in most cases it will be desirable to hold at least a first scheduling conference in the time set by the rule.

Three items are added to the list of permitted contents in Rule 16(b)(3)(B).

The order may provide for preservation of electronically stored information, a topic also added to the provisions of a discovery plan under Rule 26(f)(3)(C). Parallel amendments of Rule 37(e) recognize that a duty to preserve discoverable information may arise before an action is filed.

The order also may include agreements incorporated in a court order under Evidence Rule 502 controlling the effects of disclosure of information covered by attorney-client privilege or work-product protection, a topic also added to the provisions of a discovery plan under Rule 26(f)(3)(D).

Finally, the order may direct that before filing a motion for an order relating to discovery the movant must request a conference with the court. Many judges who hold such conferences find them an efficient way to resolve most discovery disputes without the delay and burdens attending a formal motion, but the decision whether to require such conferences is left to the discretion of the judge in each case.

Amendment Analysis

More Effective Scheduling Conferences

The first amendment to 16(b)(1)(B) concerns logistics at the outset of litigation. The new rule deletes the language allowing the judge to issue a scheduling order after parties communicate by phone, mail or other means. Instead, the rule is intended to encourage parties to communicate directly at the scheduling conference or other circumstances where a live conversation can take place. The Committee Note explains that simultaneous conversation via in-person meetings, teleconferences or other electronic meeting forums is recommended. The change is intended to make scheduling conferences more effective by reducing delay and misunderstandings that are more commonplace via indirect communication methods.

Shorter Time Limits

Continuing with amendments to effectuate efficient litigation, the second amendment to Rule 16 reduces the time for courts to issue scheduling orders. Rule 16(b)(2) requires the judge to issue a scheduling order 90 days after any defendant has been served or 60 days after any defendant has appeared, whichever is earlier. The Committee Note, however, recognizes that in some complex cases, the court may extend a scheduling order if there is good cause for delay.

More Comprehensive Scheduling Orders

The final changes to Rule 16 allow for a more inclusive scheduling order, adding three key ediscovery topics. Courts are empowered to address the following new items in their scheduling orders:

- The preservation of electronically stored information;
- Clawback agreements reached under Federal Rule of Evidence 502; and
- A required discovery conference before either party moves for a discovery order.

The Committee Note highlights that two of these topics—preservation and privilege protection—are stressed several times throughout the 2015 rule amendments, emphasizing the importance of these areas.

Impact for Corporations and Law Firms

Litigants Should Be Ready for Discovery Because There Is No Time to Waste

Active case management is a prominent theme throughout the rule amendments. The reduction of time for courts to issue a scheduling order is intended to reduce delays at the outset of litigation. This will make early case assessment even more important. Practically speaking, as soon as possible, litigants need to know:

- Where their data lie and on what data sources
- What types of data are implicated
- How many custodians are relevant
- What timelines are involved

16

- Whether international data is involved
- What types of legal hold protocols are in place
- How data will be reviewed and produced

The changes also underscore the importance of deploying strong information governance policies in advance of litigation. Understanding the data landscape in advance of litigation will make everything more efficient downstream. Further, parties should develop an approach to ediscovery—even if they have never had to produce ESI in litigation before. Having a formal discovery protocol for managing data, coordinating personnel (such as IT departments, international offices, etc.) and leveraging outside help (such as consultants and technology providers) will be increasingly important to be better prepared with ever shortening timeframes.

Parties Should Meet Early and Often

Beyond shortened timeframes, the amendments are intended to discourage "drive-by" meet and confers. In the past, courts have frequently voiced dismay when ruling on ediscovery issues raised by parties that failed to meet and confer. Instead, the new rules require that parties communicate and be upfront; likewise, the amendments further clarify that judges will not tolerate foot-dragging or game-playing among parties during discovery.

Specifically, litigants should be prepared to:

- Engage in direct face-to-face or voice-to-voice communications at the scheduling conference
- Address more comprehensive scheduling orders from the court
- Resolve concerns upfront via discovery conferences before engaging in burdensome motion practice

Consider, for example, the need to discuss search protocols. If a proactive producing party solicits the requesting party for input over its tentative search protocol and its intent to use technology assisted review or predictive coding technologies, the requesting party has an incredible incentive to speak up. In fact, some courts will see this early communication as the requesting party's exclusive opportunity to offer feedback or raise objections. The bottom line: by encouraging the parties to discuss discovery prior to the Rule 26(f) conference, amended Rule 16 incentivizes parties to be prepared earlier than ever before.

Under those conditions, disputes over "discovery about discovery" would never need to be presented to the court, because counsel would have reduced, early in the case, the potential for disagreements about proper discovery protocols and would have actively sought to avoid such agreements through cooperation. This is reinforced by the amendment to Rule 26(f), which requires the parties to have an enhanced "discovery plan" reflecting issues about ediscovery. Amended Rule 16 demonstrates an attempt to encourage courts to get parties to address their discovery concerns early on and not down the road.

Counsel Should Consider Clawbacks More Closely

Both judges and commentators have spoken at length about the importance of clawback agreements, which take advantage of Fed.R.Evid. 502. The basic fact is that just as man and machine will probably never be able to perfectly separate what is relevant from what is not, the same holds true for identifying and isolating privileged information. Mistakes happen in document review and production -- and they always will.

While this does incentivize proper protocols, it also stresses the importance of carving out an escape plan, such as a clawback agreement. The amendments to Rules 16 and 26(f) emphasize the importance of including a Fed.R.Evid. 502 agreement in order to recoup mistakenly produced privileged documents by allowing courts to address them in their scheduling orders. Without such an agreement, parties must show they took "reasonable steps" to prevent disclosure, among other requirements found in Rule 502. However, parties can modify these requirements, or eliminate them altogether, if they arrive at a properly worded Fed.R.Evid. 502 clawback agreement before discovery begins. What does this mean for parties? Under the new rules, there will be more pressure than ever before to enter into a clawback agreement—something most litigating parties often refuse.

16

26

RULE 26

Duty to Disclose; General Provisions; Governing Discovery

New Rule Provisions

(b) Discovery Scope and Limits.

(1) *Scope in General.* Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible in evidence to be discoverable. ~~Including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter. For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence. All discovery is subject to the limitations imposed by Rule 26(b)(2)(C).~~

(2) *Limitations on Frequency and Extent.*

• • • • •

(C) When Required. On motion or on its own, the court must limit the frequency or extent of discovery

otherwise allowed by these rules or by local rule if it determines that:

• • • • •

(iii) the ~~burden or expense of the~~ proposed discovery is outside the scope permitted by Rule 26(b)(1) ~~outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues.~~

• • • • •

(c) Protective Orders.

(1) ***In General.*** A party or any person from whom discovery is sought may move for a protective order in the court where the action is pending—or as an alternative on matters relating to a deposition, in the court for the district where the deposition will be taken. The motion must include a certification that the movant has in good faith conferred or attempted to confer with other affected parties in an effort to resolve the dispute without court action. The court may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense, including one or more of the following:

• • • • •

(B) specifying terms, including time and place or the allocation of expenses, for the disclosure or discovery;

• • • • •

(d) Timing and Sequence of Discovery.

• • • • •

(2) ***Early Rule 34 Requests.***

(A) Time to Deliver. More than 21 days after the summons and complaint are served on a party, a request under Rule 34 may be delivered:

(i) to that party by any other party, and

(ii) by that party to any plaintiff or to any other party that has been served.

(B) When Considered Served. The request is considered to have been served at the first Rule 26(f) conference.

(23) ***Sequence.*** Unless~~, on motion,~~ the parties stipulate or the court orders otherwise for the parties' and witnesses' convenience and in the interests of justice:

(A) methods of discovery may be used in any sequence; and

(B) discovery by one party does not require any other party to delay its discovery.

• • • • •

(f) Conference of the Parties; Planning for Discovery.

• • • • •

(3) ***Discovery Plan.*** A discovery plan must state the parties' views and proposals on:

• • • • •

(C) any issues about disclosure, or discovery, or preservation of electronically stored information, including the form or forms in which it should be produced;

(D) any issues about claims of privilege or of protection as trial-preparation materials, including—if the parties agree on a procedure to assert these claims after production—whether to ask the court to include their agreement in an order under Federal Rule of Evidence 502;

• • • • •

Committee Note

Rule 26(b)(1) is changed in several ways.

Information is discoverable under revised Rule 26(b)(1) if it is relevant to any party's claim or defense and is proportional to the needs of the case. The considerations that bear on proportionality are moved from present Rule 26(b)(2)(C)(iii), slightly rearranged and with one addition.

Most of what now appears in Rule 26(b)(2)(C)(iii) was first adopted in 1983. The 1983 provision was explicitly adopted as part of the scope of discovery defined by Rule 26(b)(1). Rule 26(b)(1) directed the court to limit the frequency or extent of use of discovery if it determined that "the discovery is unduly burdensome or expensive, taking into account the needs of the case, the amount in controversy, limitations on the parties' resources, and the importance of the issues at stake in the litigation." At the same time, Rule 26(g) was added. Rule 26(g) provided that signing a discovery request, response, or objection certified that the request, response, or objection was "not unreasonable or unduly burdensome or expensive, given the needs of the case, the discovery already had in the case, the amount in controversy, and the importance of the issues at stake in the litigation." The parties thus shared the responsibility to honor these limits on the scope of discovery.

The 1983 Committee Note states that the new provisions were added "to deal with the problem of over-discovery. The objective is to guard against redundant or disproportionate discovery by giving the court authority to reduce the amount of discovery that may be directed to matters that are otherwise proper subjects of inquiry. The new sentence is intended to encourage judges to be more aggressive in identifying and discouraging discovery overuse. The grounds mentioned in the amended rule for limiting discovery reflect the existing practice of many courts in issuing protective orders under Rule 26(c). . . . On the whole, however, district judges have been reluctant to limit the use of the discovery devices."

The clear focus of the 1983 provisions may have been softened, although inadvertently, by the amendments made in 1993. The 1993 Committee Note explained: "[F]ormer paragraph (b)(1) [was] subdivided into two paragraphs for ease of reference and to avoid renumbering of paragraphs (3) and (4)." Subdividing the paragraphs, however, was done in a way that could be read to separate the proportionality provisions as "limitations," no longer an integral part of the (b)(1) scope provisions. That

appearance was immediately offset by the next statement in the Note: "Textual changes are then made in new paragraph (2) to enable the court to keep tighter rein on the extent of discovery."

The 1993 amendments added two factors to the considerations that bear on limiting discovery: whether "the burden or expense of the proposed discovery outweighs its likely benefit," and "the importance of the proposed discovery in resolving the issues." Addressing these and other limitations added by the 1993 discovery amendments, the Committee Note stated that "[t]he revisions in Rule 26(b)(2) are intended to provide the court with broader discretion to impose additional restrictions on the scope and extent of discovery. . . ."

The relationship between Rule 26(b)(1) and (2) was further addressed by an amendment made in 2000 that added a new sentence at the end of (b)(1): "All discovery is subject to the limitations imposed by Rule 26(b)(2)(i), (ii), and (iii) [now Rule 26(b)(2)(C)]." The Committee Note recognized that "[t]hese limitations apply to discovery that is otherwise within the scope of subdivision (b)(1)." It explained that the Committee had been told repeatedly that courts were not using these limitations as originally intended. "This otherwise redundant cross-reference has been added to emphasize the need for active judicial use of subdivision (b)(2) to control excessive discovery."

The present amendment restores the proportionality factors to their original place in defining the scope of discovery. This change reinforces the Rule 26(g) obligation of the parties to consider these factors in making discovery requests, responses, or objections.

Restoring the proportionality calculation to Rule 26(b)(1) does not change the existing responsibilities of the court and the parties to consider proportionality, and the change does not place on the party seeking discovery the burden of addressing all proportionality considerations.

Nor is the change intended to permit the opposing party to refuse discovery simply by making a boilerplate objection that it is not proportional. The parties and the court have a collective responsibility to consider the proportionality of all discovery and consider it in resolving discovery disputes.

The parties may begin discovery without a full appreciation of the factors that bear on proportionality. A party requesting discovery, for example, may have little information about the burden or expense of responding. A party requested to provide discovery may have little information about the importance of the discovery in resolving the issues as understood by the requesting party. Many of these uncertainties should be addressed and reduced in the parties' Rule 26(f) conference and in scheduling and pretrial conferences with the court. But if the parties continue to disagree, the discovery dispute could be brought before the court and the parties' responsibilities would remain as they have been since 1983. A party claiming undue burden or expense ordinarily has far better information—perhaps the only information—with respect to that part of the determination. A party claiming that a request is important to resolve the issues should be able to explain the ways in which the underlying information bears on the issues as that party

26

understands them. The court's responsibility, using all the information provided by the parties, is to consider these and all the other factors in reaching a case-specific determination of the appropriate scope of discovery.

The direction to consider the parties' relative access to relevant information adds new text to provide explicit focus on considerations already implicit in present Rule 26(b)(2)(C)(iii). Some cases involve what often is called "information asymmetry." One party—often an individual plaintiff—may have very little discoverable information. The other party may have vast amounts of information, including information that can be readily retrieved and information that is more difficult to retrieve. In practice these circumstances often mean that the burden of responding to discovery lies heavier on the party who has more information, and properly so.

Restoring proportionality as an express component of the scope of discovery warrants repetition of parts of the 1983 and 1993 Committee Notes that must not be lost from sight. The 1983 Committee Note explained that "[t]he rule contemplates greater judicial involvement in the discovery process and thus acknowledges the reality that it cannot always operate on a self-regulating basis." The 1993 Committee Note further observed that "[t]he information explosion of recent decades has greatly increased both the potential cost of wide-ranging discovery and the potential for discovery to be used as an instrument for delay or oppression." What seemed an explosion in 1993 has been exacerbated by the advent of ediscovery. The present amendment again reflects the need for continuing and close judicial involvement in the cases that do not yield readily to the ideal of effective party management. It is expected that discovery will be effectively managed by the parties in many cases. But there will be important occasions for judicial management, both when the parties are legitimately unable to resolve important differences and when the parties fall short of effective, cooperative management on their own.

It also is important to repeat the caution that the monetary stakes are only one factor, to be balanced against other factors. The 1983 Committee Note recognized "the significance of the substantive issues, as measured in philosophic, social, or institutional terms. Thus the rule recognizes that many cases in public policy spheres, such as employment practices, free speech, and other matters, may have importance far beyond the monetary amount involved." Many other substantive areas also may involve litigation that seeks relatively small amounts of money, or no money at all, but that seeks to vindicate vitally important personal or public values.

So too, consideration of the parties' resources does not foreclose discovery requests addressed to an impecunious party, nor justify unlimited discovery requests addressed to a wealthy party. The 1983 Committee Note cautioned that "[t]he court must apply the standards in an even-handed manner that will prevent use of discovery to wage a war of attrition or as a device to coerce a party, whether financially weak or affluent."

The burden or expense of proposed discovery should be determined in a realistic way. This

includes the burden or expense of producing electronically stored information. Computer-based method of searching such information continue to develop, particularly for cases involving large volumes of electronically stored information. Courts and parties should be willing to consider the opportunities for reducing the burden or expense of discovery as reliable means of searching electronically stored information become available.

A portion of present Rule 26(b)(1) is omitted from the proposed revision. After allowing discovery of any matter relevant to any party's claim or defense, the present rule adds: "including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter." Discovery of such matters is so deeply entrenched in practice that it is no longer necessary to clutter the long text of Rule 26 with these examples. The discovery identified in these examples should still be permitted under the revised rule when relevant and proportional to the needs of the case. Framing intelligent requests for electronically stored information, for example, may require detailed information about another party's information systems and other information resources.

The amendment deletes the former provision authorizing the court, for good cause, to order discovery of any matter relevant to the subject matter involved in the action. The Committee has been informed that this language is rarely invoked. Proportional discovery relevant to any party's claim or defense suffices, given a proper understanding of what is relevant to a claim or defense. The distinction between matter relevant to a claim or defense and matter relevant to the subject matter was introduced in 2000. The 2000 Note offered three examples of information that, suitably focused, would be relevant to the parties' claims or defenses. The examples were "other incidents of the same type, or involving the same product"; "information about organizational arrangements or filing systems"; and "information that could be used to impeach a likely witness." Such discovery is not foreclosed by the amendments. Discovery that is relevant to the parties' claims or defenses may also support amendment of the pleadings to add a new claim or defense that affects the scope of discovery.

The former provision for discovery of relevant but inadmissible information that appears "reasonably calculated to lead to the discovery of admissible evidence" is also deleted. The phrase has been used by some, incorrectly, to define the scope of discovery. As the Committee Note to the 2000 amendments observed, use of the "reasonably calculated" phrase to define the scope of discovery "might swallow any other limitation on the scope of discovery." The 2000 amendments sought to prevent such misuse by adding the word "Relevant" at the beginning of the sentence, making clear that "'relevant' means within the scope of discovery as defined in this subdivision . . . ." The "reasonably calculated" phrase has continued to create problems, however, and is removed by these amendments. It is replaced by the direct statement that "Information within the scope of discovery need not be admissible in evidence to be discoverable." Discovery of nonprivileged information not admissible in evidence remains

available so long as it is otherwise within the scope of discovery.

Rule 26(b)(2)(C)(iii) is amended to reflect the transfer of the considerations that bear on proportionality to Rule 26(b)(1). The court still must limit the frequency or extent of proposed discovery, on motion or on its own, if it is outside the scope permitted by Rule 26(b)(1).

Rule 26(c)(1)(B) is amended to include an express recognition of protective orders that allocate expenses for disclosure or discovery. Authority to enter such orders is included in the present rule, and courts already exercise this authority. Explicit recognition will forestall the temptation some parties may feel to contest this authority. Recognizing the authority does not imply that cost-shifting should become a common practice. Courts and parties should continue to assume that a responding party ordinarily bears the costs of responding.

Rule 26(d)(2) is added to allow a party to deliver Rule 34 requests to another party more than 21 days after that party has been served even though the parties have not yet had a required Rule 26(f) conference. Delivery may be made by any party to the party that has been served, and by that party to any plaintiff and any other party that has been served. Delivery does not count as service; the requests are considered to be served at the first Rule 26(f) conference. Under Rule 34(b)(2)(A) the time to respond runs from service. This relaxation of the discovery moratorium is designed to facilitate focused discussion during the Rule 26(f) conference. Discussion at the conference may produce changes in the requests. The opportunity for advance scrutiny of requests delivered before the Rule 26(f) conference should not affect a decision whether to allow additional time to respond.

Rule 26(d)(3) is renumbered and amended to recognize that the parties may stipulate to case-specific sequences of discovery.

Rule 26(f)(3) is amended in parallel with Rule 16(b)(3) to add two items to the discovery plan—issues about preserving electronically stored information and court orders under Evidence Rule 502.

Amendment Analysis

Scope of Discovery and Proportionality

The changes to Rule 26(b)(1) are intended to emphasize that parties may obtain discovery of non-privileged information, including ESI, that is both relevant and proportional to the needs of the case. In order to make that point, the amendment relocates and rearranges the proportionality considerations from Rule 26(b)(2)(C)(iii) into Rule 26(b)(1). In response to public comments, it also adds a new consideration—the parties' relative access to information—and explains in a revised Committee Note that these changes simply restore the emphasis on proportionality to Rule 26(b)(1).

In addition, a number of important deletions are made from Rule 26(b)(1). The amended rule removes the previous "reasonably calculated to lead to the discovery of admissible evidence" language, in favor of an emphasis on the

parties' obligations to consider proportionality throughout the discovery process. It also deletes the authority to seek discovery relevant to the subject matter involved and omits the (unnecessary) list of examples, thereby shortening the rule.

Under the amended Rule 26(b)(1), the relevant considerations in determining whether discovery is proportional to the needs of the case include:

- The importance of the issues at stake;
- 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 outweighs its likely benefit.

These factors have been slightly reordered from their previous location in response to public comments, with "amount in controversy" being moved behind the "importance of issues at stake" factor to the first position in the list. As noted, the amended list now includes a new factor in the third position, "parties' relative access to relevant information." The Committee Note emphasizes that moving the proportionality standard from Rule 26(b)(2)(C)(iii) to its prominent position in Rule 26(b)(1) "does not change the existing responsibilities of the court and parties to consider proportionality." Rather, the court and the parties have a continuing, "collective responsibility to consider the proportionality of all discovery and consider it in resolving discovery disputes."

Protective Orders for Costs

Rule 26(c)(1)(B) is amended to explicitly acknowledge that a protective order issued for good cause may allocate costs amongst the parties. The Committee Note explains that the "[a]uthority to enter such orders [shifting costs] is included in the present rule" and courts are coming to exercise this authority.

In response to public comments, the Committee Note further clarifies that "[r]ecognizing the authority to shift the costs of discovery does not mean that cost-shifting should become a common practice" and that "[c]ourts and parties should continue to assume that a responding party ordinarily bears the costs of responding." While the Rules Committee intends to take a look at more comprehensive cost-shifting proposals at some point, it has signaled that it wants to see what impact the renewed emphasis on proportionality has before undertaking that task.

Discovery Requests Prior to Meet and Confer

A new provision (Rule 26(d)(2)("Early Rule 34 Requests")) will be added to allow "delivery" of discovery requests prior to the "meet and confer" required by Rule 26(f). The intent of this relaxation of the existing "discovery moratorium" is "designed to facilitate focused discussion during the Rule 26(f) conference," since discussion may produce changes in the requests.

26

However, if that option is exercised, the response time will not commence, however, until after the first Rule 26(f) conference—these requests are deemed served at the time of the conference. Rule 34(b)(2)(A) will be amended by a parallel provision as to the time to respond "if the request was delivered under 26(d)(2) – within 30 days after the parties' first Rule 26(f) conference."

Discovery Plan Proposals for Preservation and Clawbacks

As noted in connection with the discussion of enhanced Rule 16 (b), a parallel amendment to Rule 26(f)(3)(D) requires that a discovery plan must include a statement of the parties' views and proposals on preservation of ESI as well as issues about claims of privilege, including whether to ask the court for an order under Fed.R.Evid. 502. The Committee Note also alludes to the wisdom of consideration of the potential use of more sophisticated document sorting and collection tools.

Impact for Corporations and Law Firms

More Than Ever Before Litigants Need to Understand Proportionality

The changes to Rule 26 are intended to restore the proportionality factors to a prominent consideration by both requesting and producing parties, and to encourage a dialogue between the parties—and the court, if necessary—regarding the amount of discovery reasonably needed in light of the claims and defenses in the case. This shift to an emphasis on proportionality is accompanied by elimination of an often-cited basis for allowing virtually unlimited discovery—the "reasonably calculated to lead to the discovery of admissible evidence" language. However, it should be noted that at the end of the proportionality factors in Rule 26(b)(1), the new rule does include the following language, "Information within this scope of discovery need not be admissible in evidence to be discoverable."

The Committee Note explains that these amendments do not alter existing responsibilities to consider proportionality and that the parties and the court have a collective responsibility to address proportionality. Practically speaking, this focus on proportionality may oblige parties to compromise more frequently when it comes to number of custodians, timeframes, data locations, search terms and other discovery parameters.

Parties that believe something is not proportional should raise the issue (i.e., by way of objection or a motion for a protective order) as early as possible if it is not possible to secure agreement to restrict discovery requests. Information cannot be withheld solely on the basis of proportionality, so parties should not sit on their hands. Instead, they should be up front about their objections, which now must be stated with specificity under amended Rule 34.

It remains to be seen if the addition of the new factor involving the relative access to information will be interpreted to diminish objections based on burden. The Committee Note declares that the burden is "heavier on the party who has more information, and properly so." Courts may expect parties with broad sources of information

to be prepared to retrieve their information quickly and efficiently. This will be especially true for corporations, which puts an emphasis on solid information governance protocols and ediscovery collection techniques. Moreover, while it remains unclear as to the extent the new Rule 26(b)(1) will limit discovery, this amendment makes it even more important to start planning for potential litigation up front. Managing the litigation more efficiently while working with critical actors such as IT departments or vendors will result in time and money saved in the long run.

Parties Should Be Prepared for an Ever-Expanding Meet and Confer

The amendments to Rule 26—along with the previously discussed amendments to Rule 16—seek to encourage earlier communication between the parties to facilitate meaningful discussions about the scope of preservation and clawback agreements at the 26(f) conference. While the new rules seem to reflect an increased expectation on the parties, the Committee Note also states that the 2015 amendments reflect "the need for continuing and close judicial involvement in the cases that do not yield readily to the ideal of effective party management." Anytime there is a major discovery dispute after the meet and confer, parties can expect a judge to require them to go back and do it again.

By allowing Rule 34 delivery (not service) of requests for production prior to the 26(f) conference, the revised rule hopes to encourage more meaningful discovery discussion between the parties at the 26(f) conference. Some pushback among commentators has been that this risks taking away from the importance of early discussions about preservation. Others see that as enhancing the discussion. In any event, the coordinated amendments portent, for courts and parties willing to do so, the need for greater urgency to get discovery issues worked out early before collection, review and production.