NBI Presentation - How To Get Your Social Media, Email and Text Evidence Admitted (And Keep Theirs Out)[1]

Steven Clark

November 15, 2018

I. Top Admission Mistakes Made With ESI

A. Preparation, Coordination and Submission

The initial question is what is ESI? In the context of litigation, ESI is any documents or information that is stored in electronic form. It can be word processing documents, spreadsheets, digital photographs, videos, emails and attachments, text and instant messages, call logs, voicemails, information stored in databases, and electronic records of online activity, such as social media postings and other activities.

Sources of ESI include computer hard drives, company network servers, thumb (USB) drives, databases, the cloud, mobile devices (mobile phones and tablet computers), and social media websites such as Facebook, Twitter and LinkedIn.

In e-discovery, ESI is divided into five categories and grouped into two tiers based on the cost and effort needed to access and produce ESI.

The first tier is reasonable accessible ESI, and includes

1. Active online data, or ESI created, received or processed. Examples are hard drives and active network servers.

2. Near-line data, or ESI stored on removable media or accessed via automated or robotic storage systems. Examples are optical disk and magnetic tape.

[1] Much of the material is synthesized from Westlaw (Thomson Reuters) Practical Law Articles, Charts and Summaries. Some additional sources include internet articles on ESI, Metadata, and Social Media.

3. Offline storage and achives or ESI sent to storage. Unlike categories 1 & 2, offline ESI is accessed manually. Examples include magnetic tape or optical disks, referred to as JBOD.

The second tier is not reasonably accessible ESI, and consists of

4. Backup tapes, commonly using data compression. This is ESI stored for backup or disaster recovery, and is not organized for retrieval of specific files or messages. Discovery of this type of ESI requires proof that its need and relevance outweigh its retrieval and processing costs.

5. Erased, fragmented or corrupted data. This is the least accessible ESI, which may be accessed only after significant processing or might be impossible to access at all.

In the e-discovery process, there are certain functions for identifying and preserving ESI and meeting conditions such as relevancy and privilege.

The typical e-discovery process includes:

1. Creating and retaining ESI according to an enforceable electronic records and retention policy and electronic records management (ERM) program.

2. Identifying the relevant ESI, preserving it from alteration and destruction, and collecting it for further review.

3. Processing and filtering ESI to remove excess and duplicates, and for privilege which is not discoverable.

4. Producing the remaining ESI after filtering out what is irrelevant, duplicative, or privileged. Producing ESI in native format is the most common way.

5. Clawback ESI that you inadvertently disclosed to the opposing party which you should have filtered out but did not. Clawback is not unusual but opposing counsel and the court may not allow it.

6. Present at trial if the case hasn't settled.

These federal rules apply to the e-discovery process for preparing and producing ESI, as well as resolving related disputes.

- FRCP 16: Courts expect you to be ready for litigation, including being fluent in the IT and network architecture so that the pretrial conference leads to agreements on what ESI is discoverable. Sanctions under FRCP 26(f) for not obeying a scheduling order or pretrial order are a good thing to avoid.
- FRCP 26: Provides protection from excessive or expensive discovery requests.
- FRCP 26(a)(1)(C) requires you make initial disclosures no later than 14 days after the Rule 26(f) meet and confer, unless an objection (now is the time to assert it) or another time is set by stipulation or court order.
- FRCP 26(b)(2)(B) introduces the concept of not reasonably accessible ESI. It provides procedures for shifting the cost of accessing not readily accessible ESI to the requesting party.
- FRCP 26(b)(5)(B) provides courts with a clear procedure for settling claims when you produce ESI to the requesting party which you should not have.
- FRCP 26(f) is the meet and confer rule, requiring all parties to meet within 99 days of the filing of the lawsuit and at least 21 days before a scheduled conference.
- FRCP 26(g) requires an attorney to sign every e-discovery request, response or objection.
- FRCP 33 defines business records which are created or kept in electronic format as discoverable.
- FRCP 34 establishes a structured way to resolve disputes over document production.
- FRCP 34(b) establishes protocols for how documents are produced to the requesting party, who chooses the form of production. Most often, the requested form is native file, but this is a matter of negotiation between the parties.
- FRCP 37 gives judges the power to impose sanctions against a party "who fails to obey an order to provide or permit discovery (FRCP 37(f)).
- FRCP 37(e) creates a safe harbor from sanctions if you did not preserve, and therefor no longer have requested ESI provided that certain conditions and circumstances are met.
- FRCP 45 governs nonparty discovery, and protects nonparty from some of the costs and burdens of producing ESI.
- FRE 502 protects attorney client privilege and some protection against inadvertent disclosure, provided you are quick to notice the mistake and meet other conditions.
- FRE 502(b) allows clawback if you took reasonable steps to prevent the error, and responded promptly to fix the error.
- FRE 901 requires that ESI be authenticated to verify that it is what it claims to be. Metadata may be used to authenticate ESI.
- Lawyers are also subject to ethical rules relating to e-discovery imposed by the Code of Professional Responsibility.

B. Weighing The Duty to Mitigate

By now, most of us have been told countless times about the duty to preserve and produce electronically stored information (ESI). Yet, parties continue to destroy ESI and courts continue

to hand down decisions punishing them for it. In one of the most closely watched patent cases involving two titans of the computer industry, the defendant, Samsung, was sanctioned for allowing emails to be routinely deleted after Apple met with Samsung executives and accused Samsung of infringing its patents.

By having a general understanding of what is required under the duty to preserve ESI, a lawyer can successfully navigate the spoliation minefield and reach the courthouse steps ready to try the case, free of any allegations of spoliation or the specter of a sanctions motion.

C. Duty to Produce and Preserve[2]

The mantra is "Preserve, preserve, preserve." There is a duty to preserve when a legal action is *reasonably anticipated*. Affirmative action needs to be taken to prevent the destruction or alteration of what might be relevant ESI.

Litigants have a duty to preserve "relevant" ESI. Relevance is determined by identifying "key players," people likely to have discoverable information that the disclosing party may use to support its claims or defenses. *Apple Inc. v. Samsung Elecs. Co.* (*Apple I*), 881 F. Supp. 2d 1132, 1137 (N.D. Cal. 2012), *rev'd on other grounds*, *Apple Inc. v. Samsung Elecs. Co.* (*Apple II*), 888 F. Supp. 2d 976 (N.D. Cal. 2012) (internal quotation marks omitted). Beyond key players, the duty to preserve relevant ESI "also extends to information that is relevant to the claims or defenses of any party, or which is relevant to the subject matter involved in the action." *Apple I*, 881 F. Supp. 2d at 1137(citations omitted) (internal quotation marks omitted).

The scope of the duty to preserve also includes relevant ESI the party has a "legal right" to or "practical control" of. "Practical control" merely means that the party has the "right, authority, or practical ability to obtain the documents from a non-party to the action." *See GenOn Mid-Atl.*,

[2] Taken from *Avoiding the ESI Minefield on the March to Trial*, Ben Stone, ABA Section of Litigation, August 22, 2013.

LLC v. Stone & Webster, Inc., 282 F.R.D. 346, 354 (S.D.N.Y. 2012) (citations omitted) (internal quotations marks omitted) (holding that party had a duty to preserve ESI in the possession of a third party when there was sufficient evidence to find that the party had either legal control or access to the documents). In addition, if a party is aware of relevant ESI that it has no right to or control of, the party "still has an obligation to give the opposing party notice of access to the evidence or of the possible destruction of the evidence if the party anticipates litigation involving that evidence." *Goodman v. Praxair Servs., Inc.*, 632 F. Supp. 2d 494, 514 (D. Md. 2009).

Once the locations of potentially relevant ESI have been identified, the party possessing the ESI must be told to "hold" that ESI and not delete it. *Apple I,* 881 F. Supp. 2d at 1137.The possessing party must continue to follow up with the key players throughout the litigation to ensure that they are complying with the litigation hold and preserving ESI. As one court warned,

> [o]nce a 'litigation hold' is in place, a party and her counsel must make certain that all sources of potentially relevant information are identified and placed 'on hold'. . . ." Then, "counsel must take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched." Thereafter, the duty to preserve discoverable information persists throughout the discovery process; a litigant must ensure that all potentially relevant evidence is retained.

Richard Green (Fine Paintings) v. McClendon, 262 F.R.D. 284, 289 (S.D.N.Y. 2009) (citations omitted).

Failure to conduct adequate follow-up with the key players can, as discussed more below, result in sanctions (even if a suitable hold was initially issued by that party). *Apple I,*881 F. Supp. 2d at 1147.

The duty to preserve relevant ESI arises once litigation has commenced. It may attach earlier if litigation can be reasonably anticipated or if a party has notice that ESI may be relevant to future litigation. *Rimkus Consulting Grp. v. Cammarata*, 688 F. Supp. 2d 598, 612 (S.D. Tex.

2010); *Apple I*, 881 F. Supp. 2d at 1136. As the *Rimkus* court noted, this concept, while easy to state, can be difficult to apply:

These general rules are not controversial. But applying them to determine when a duty to preserve arises in a particular case and the extent of that duty requires careful analysis of the specific facts and circumstances. It can be difficult to draw bright-line distinctions between acceptable and unacceptable conduct in preserving information and in conducting discovery, either prospectively or with the benefit (and distortion) of hindsight. *Rimkus*, 688 F. Supp. 2d at 613.

Fortunately, however, a robust body of case law in this arena lays out a general framework that attorneys can use to figure out whether a duty to preserve has attached. A duty attaches, for example, once a party has met with an attorney and decided to bring a lawsuit. *Turner v. Hudson Transit Lines, Inc.*, 142 F.R.D. 68, 72–73 (S.D.N.Y. 1991). A duty also arises once someone is told that he or she has committed a legal wrong. In the *Apple* cases, for instance, the court held that the duty by Samsung to preserve ESI attached once Apple told Samsung that it was infringing Apple's patents. *Apple I*, 881 F. Supp. 2d at 1134; *see also Bayoil, S.A. v. Polembros Shipping Ltd.*, 196 F.R.D. 479, 483 (S.D. Tex. 2000) ("Notice does not have to be of actual litigation, but can concern 'potential' litigation. Otherwise, any person could shred documents to their heart's content before suit is brought without fear of sanction."). Similarly, in the employment context, the duty has been held to arise as soon as an employee files a charge of discrimination with the Equal Employment Opportunity Commission. *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216–17 (S.D.N.Y. 2003).

D. Spoilation Pitfalls[3]

[3] See note 2, infra.

The law of spoliation is a minefield for the unwary. But an attorney who understands the law and acts quickly to preserve potentially relevant ESI will insulate his or her client from any claim of spoliation later on in the litigation.

Culpable State of Mind

If a party deletes ESI that he or she had a duty to preserve, the opposing party must prove that the destruction was with a "culpable state of mind" for sanctions to be imposed. Culpable states of mind vary, from bad faith, recklessness, and willfulness and conscious disregard, to the least culpable, gross negligence, and negligence. Whether a party's conduct constitutes one state of mind or another is highly fact dependent as the "varieties of efforts and failures is infinite." *Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec.*, 685 F. Supp. 2d 456, 465 (S.D.N.Y. 2010), *rev'd on other grounds, Chin v. Port Auth. of N.Y. & N.J.*, 685 F.3d 135 (2d Cir. 2012). What complicates matters further is that courts have disagreed about what constitutes one state of mind or another. *See Pension Comm.*, 685 F. Supp. 2d at 464 ("It is . . . a call that cannot be measured with exactitude and might be called differently by a different judge.").

Bad faith is relatively easy to define and limited to instances where a party has intentionally deleted ESI so that the ESI could not be used by an adversary in litigation. *See, e.g.*, *Rimkus*, 688 F. Supp. 2d at 644.

Less clear is what constitutes gross negligence and negligence. Fortunately, in the 2010 *Pension Comm.* decision, Judge Scheindlin, the New York federal judge who, earlier, had issued the influential *Zubulake* line of ESI-related decisions, provided guidance. Citing the definition of gross negligence from torts, Judge Scheindlin concluded that gross negligence included failing to institute a litigation hold, failing to collect relevant ESI from key players, or preventing the routine destruction of ESI after the duty to preserve has attached. *Pension Comm.*,

685 F. Supp. 2d at 465; *see also Apple I*, 681 F. Supp. 2d at 1147 (holding that the continued routine destruction of emails after a litigation hold had been issued constituted "conscious disregard"). Also citing the tort definition of negligence, Judge Scheindlin concluded that negligence included failing to obtain documents from persons other than "key persons," failing to take one of the many steps necessary to ensure preservation of relevant ESI, or failing to validate the accuracy of search terms. *Pension Comm.*, 685 F. Supp. 2d at 465.

Prejudice

In addition to a culpable state of mind, there must be prejudice resulting from the destruction of the ESI. If there is a bad-faith destruction of ESI, it is presumed that what was destroyed was relevant to the case and that the party seeking sanctions is therefore prejudiced. *Rimkus*, 688 F. Supp. 2d at 616. Some courts go one step further, allowing (but not requiring) a presumption of prejudice in instances of gross negligence. *Id.*; *Pension Comm.*, 685 F. Supp. 2d at 467. But, for negligent destruction of ESI, the party seeking sanctions must establish that his or her ability to prove the case or defend the claim has been prejudiced by the destruction of the ESI. *GenOn*, 282 F.R.D. at 353; *Pension Comm.*, 685 F. Supp. 2d at 467.

To establish prejudice, the party seeking sanctions must prove that what was destroyed was "relevant." This inquiry is narrower than determining relevance for the duty to preserve ESI. Indeed, courts do not require much to establish relevance, merely that a reasonable trier of fact could have found that the ESI would support a claim or defense. *Rimkus*, 688 F. Supp. 2d at 612. This, courts reason, is only fair because it is difficult to prove that evidence that no longer exists would have helped a claim and defense. Courts also reason that to raise the bar too high would permit "the spoliator . . . to profit from its destruction." *Id.* at 616 (citation omitted) (internal quotation marks omitted).

However, the party seeking sanctions may not rely on generalities but must provide some extrinsic evidence showing that what was destroyed was relevant. *Id.* at 617. As Judge Scheindlin explained,

> [w]hile requiring the innocent party to demonstrate the relevance of information that it can never review may seem unfair, the party seeking relief has some obligation to make a showing of relevance and eventually prejudice, lest litigation become a "gotcha" game rather than a full and fair opportunity to air the merits of a dispute.

Pension Comm., 685 F. Supp. 2d at 468.

Sanctions

Once the party seeking sanctions has satisfied his or her burden of proof, the judge decides the sanction that is appropriate. In determining this, the court has many tools in its kit. *See Apple I*, 881 F. Supp. 2d at 1136 ("A trial court's discretion regarding the form of a spoliation sanction is broad, and can range from minor sanctions, such as the awarding of attorney fees, to more serious sanctions, such as dismissal of claims or instructing the jury that it may draw an adverse inference." (footnotes omitted)). At the same time, though, the judge's discretion is not limitless; the judge must base his or her decision on several factors, including punitive (penalizing the party responsible for the spoliation) and remedial (putting the party prejudiced by the spoliation back to where he or she would have been but for the spoliation). *Id.* Some courts will apply the least sanction necessary to mitigate the harm caused by the loss of ESI. *Id.* at 1150. Others, however, focus on the degree of culpability of the party responsible for the spoliation, contending that punishment and deterrence are the ultimate objectives of any sanction. *Green*, 262 F.R.D. at 288–89.

The most severe of sanctions—dismissal of the case—is generally justified in only the most egregious cases, "such as where a party has engaged in perjury, tampering with evidence, or

intentionally destroying evidence by burning, shredding, or wiping out computer hard drives." *Pension Comm.*, 685 F. Supp. 2d at 469–70. More common among the serious sanctions are the use of adverse jury instructions, but there is no general consensus among the courts as to when that should be imposed. *GenOn*, 282 F.R.D. at 353; *Apple I*, 881 F. Supp. 2d at 1138. Courts in the Fifth, Seventh, Eighth, Tenth, Eleventh, and D.C. Circuits require "bad faith" before permitting adverse jury instructions. *Rimkus*, 688 F. Supp. 2d at 614; *GenOn*, 282 F.R.D. at 353. Other courts, however, will allow adverse jury instructions if there is gross negligence. *Rimkus*, 688 F. Supp. 2d at 614–15.

The types of adverse jury instructions used can also vary. *Apple I*, 881 F. Supp. 2d at 1150. As the magistrate judge explained in *Apple I*,

> [i]n its most harsh form, when a spoliating party has acted willfully or in bad faith, the jury can be instructed that certain facts are deemed admitted and must be accepted as true. At the next level, when a spoliating party has acted willfully or recklessly, a court may impose a mandatory presumption. At the other end of the spectrum, the least harsh instruction permits (but does not require) a jury to presume that the lost evidence is both relevant and favorable to the innocent party. If it makes this presumption, the spoliating party's rebuttal evidence must then be considered by the jury, which must then decide whether to draw an adverse inference against the spoliating party.

Id. at 1149 (footnotes omitted) (citations omitted) (internal quotation marks omitted).

As Judge Koh went on to write in reversing the magistrate judge in the *Apple I* case, the severest form of adverse jury instruction, which had been imposed by the magistrate judge, is unwarranted if the party accused of spoliation has produced significant amounts of information and the other side has been able to obtain the information through alternative methods. *Apple II*, 888 F. Supp. 2d at 994–95. Instead, the harshest of the adverse instructions is generally limited to circumstances where an entire "source of documents" has been destroyed. *Id.* at 994.

E. Sanctions and Proportionality[4]

Litigators and the courts understand that the "punishment must fit the crime." Although sought in most instances, the sanction for an ESI spoliation offense often does not merit that a party's pleading be stricken. Recent decisions review the circumstances surrounding digital or electronic spoliation claims, with courts seeking to craft a balanced sanction upon reviewing the "prejudice" to both sides, which could be the issuance of an adverse inference charge or a preclusion order. Courts may direct further discovery, including depositions, to more clearly evaluate the circumstances under which ESI spoliation occurred, or defer issuing a sanction until a later date, with the goal of then being able to determine the appropriate sanction on a proper record.

The concept of "proportionality" is widely recognized as one of the key themes in the 2015 amendments to the Federal Rules of Civil Procedure. Interestingly, while the concept of proportionality permeates the 2015 amendments, most of the scholarship on the subject analyzes proportionality only in relation to Rule 26. But the Civil Rules Advisory Committee did not use the concept of proportionality exclusively to reframe the scope of discovery in Rule 26; it also infused that concept into its amendment of Rule 37(e) in an effort to alleviate some of the burdens associated with litigants' obligations to preserve electronically stored information (ESI) and to ease the harsh penalties some courts had been imposing for failing to meet those obligations.

More specifically, in its notes discussing the 2015 amendments to Rule 37(e), the advisory committee acknowledged that, because federal circuits had adopted *significantly* different

[4] Taken from "*Keeping Things in Proportion: Preservation of ESI under Amended Rule 37(e)*, Karen Henry, ABA Section of Litigation Feb. 23, 2016.

standards regarding the imposition of sanctions for failure to preserve ESI, litigants were expending "excessive effort and money" on preservation to minimize their exposure to severe sanctions in the event a court found their preservation efforts lacking. The amendments to Rule 37(e) offer courts a standardized analytical framework to employ when evaluating the potential spoliation of ESI. Of particular relevance here, the concept of proportionality plays a primary role in that analysis.

Before amendment, Rule 37(e) provided that, "[a]bsent 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." The 2015 amendments completely overhauled the rule, which now reads:

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

The revised rule sets forth three preliminary findings a court must make *before* imposing "curative measures" for the loss of ESI. (The rule now speaks in terms of "curative measures," not "sanctions.") First, the court must find that the party who lost the ESI had a duty to preserve it in the anticipation or conduct of the litigation. Second, the court must conclude that the party who lost the ESI failed to take "reasonable steps" to preserve it. Third, the court must find that the lost ESI cannot be restored or replaced.

If all three of these preliminary findings are made, the court next must decide the appropriate "curative measure" to ameliorate the loss. To make this determination, the court should evaluate (1) whether any other party has been prejudiced by the loss of ESI, and (2) whether the party who lost the ESI intended to deprive another party of that information. Where prejudice is found, the court has broad discretion to impose measures "no greater than necessary to cure the prejudice." But if the court finds the party *intended* to deprive another party of the lost information, the court may impose more severe measures, including giving negative inference instructions or dismissing the case.

The advisory committee notes encourage litigants and courts to consider proportionality at virtually every stage of this analytical framework.

As explained above, in conducting the threshold inquiry under the revised Rule 37(e), a court must consider, among other things, whether the party that lost the ESI failed to take "reasonable steps" to preserve it. In evaluating the reasonableness of a party's preservation efforts, the advisory committee expressly instructs courts to consider "proportionality." In this context, proportionality requires courts to be sensitive to the resources of the party who lost the ESI, realizing "aggressive preservation efforts can be extremely costly, and parties (including governmental parties) may have limited staff and resources to devote to those efforts." This comment is welcome news to smaller companies with modest (or nonexistent) litigation budgets, which at times had been required to make disproportionately significant up-front investments in ESI preservation to avoid the risk of potentially crippling sanctions. Indeed, the staggering costs associated with preservation have been known to prevent smaller companies from prosecuting valid claims. But this new sensitivity to litigants' resources should allow smaller companies to

use less costly preservation methods (like custodian self-preservation), easing the costs typically associated with preservation and the attendant operational disruptions.

Proportionality also is an important consideration in the court's determination that a party's failure to take reasonable steps to preserve ESI resulted in the loss of that information. In such a scenario, the court must evaluate whether the lost information can be restored or replaced through additional discovery before the court imposes sanctions. Here again, the advisory committee notes emphasize proportionality, explaining that any "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." In other words, a party should not be required to undertake substantial measures to restore or replace information that is duplicative or only marginally relevant to the material issues in the litigation. Restoration and replacement obligations must correlate to the lost information's value to the case.

The advisory committee did not restrict proportionality considerations only to those areas where courts are evaluating whether a litigant has satisfied an affirmative obligation, like preservations and restoration obligations. Significantly, courts also must consider proportionality in imposing "curative measures" to address spoliation of ESI. Thus, although courts have broad discretion to impose curative measures where they find that a party who lost ESI acted with the intent to deprive another party of that information, the advisory committee cautions that "[t]he remedy should fit the wrong, and the severe measures authorized by [subdivision (e)(2)] 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" (emphasis added).

The proportionality considerations infused into Rule 37(e) provide an opportunity for litigants, especially those with modest litigation budgets, to rein in the costs traditionally

associated with preservation of ESI and to create a more manageable and cost-effective preservation plan. This is fully consistent with the overarching purpose of the Federal Rules of Civil Procedure—to "secure the just, speedy, and *inexpensive* determination of every action and proceeding." Fed. R. Civ. P. 1 (emphasis added).

Here are five tips to help you leverage proportionality considerations in the context of ESI preservation:

Tip No. 1: Create and document your client's preservation plan as early as practicable. Remember that Rule 37 does not require perfection in preservation; litigants are required only to take *reasonable* steps to preserve ESI. This means that counsel should work with their clients at the earliest possible opportunity to create a *written* preservation plan that can be defended if the need arises. The preservation plan should outline a reasonable approach to ensure that ESI relating to the dispute will be available in the litigation if it is requested, bearing in mind the client's resources and the sophistication of the client's business operations.

Tip No. 2: Immediately learn and understand your client's document management system. You cannot craft a reasonable document preservation plan until you understand how your client's document management system operates. Many attorneys eventually interview their client's custodian of records, but these interviews often occur later in the process than is advisable. Make a concerted effort to engage your client's custodian as early as practicable, because an early conversation may reveal areas of concern that can be addressed before they become problems.

Tip No. 3: Raise proportionality issues with opposing counsel as early as practicable. If you have engaged in early communications about preservation with your client and its custodians, you should have a clear idea about whether proportionality considerations exist. To the extent these early conversations reveal that ESI preservation obligations may negatively and disproportionately burden your client, try to raise that issue with opposing counsel *before* the initial scheduling conference, but not later than the meet and confer that precedes that conference. Be prepared to present a preservation plan that is reasonable and proportionate under the circumstances, and to explain your rationale with an appropriate degree of specificity. If the parties cannot agree on a reasonable preservation plan, raise the issue with the court during the initial scheduling conference. The 2015 amendments to Rule 16(b) now expressly permit courts to make provisions in their scheduling orders for the preservation of ESI.

Tip No. 4: Distinguish material issues from marginal issues as early as possible. Understanding the issues in dispute and being able to distinguish material and marginal issues early on is incredibly helpful in crafting a reasonable preservation plan for your client and in having a meaningful conversation with opposing counsel about why your client should not be required to invest resources to preserve ESI that is not likely to be produced in the litigation. In the summer of 2014, Professor William H.J. Hubbard from the University of Chicago Law

School published his *Preservation Costs Survey*, which provides insight into how and at what costs companies (ranging in size and industry focus) were meeting their preservation obligations. Notably, Professor Hubbard's research demonstrated that rule amendments geared toward reducing over-preservation were likely to have no adverse impact on discovery and the ultimate resolution of litigation because so little preserved data is ever used. This revelation crystalizes the need to separate the wheat from the chaff early enough in the litigation to potentially lessen (or eliminate) your client's obligation to unnecessarily preserve ESI on marginal issues.

Tip No. 5: Recognize the amount in controversy does not always determine case value. One of the key considerations in the proportionality analysis is the value of the case. In other words, the value of the case bears directly on the scope of a litigant's preservation obligations. A party should expect to have a greater preservation burden in a consumer class action lawsuit than in a small breach of contract case. But there are some instances where a case with a modest amount in controversy still could justify a somewhat disproportionate preservation burden. Typically, such cases implicate important public policy considerations, like free speech and employment practices. Where a case seeks to vindicate policies recognized as vital by courts or the legislature, the fact that the plaintiff seeks a relatively modest amount of damages (or no damages) does not necessarily mean that the corresponding preservation burdens should be minimized. When evaluating proportionality, always be mindful of whether considerations beyond monetary stakes should be weighed in the analysis.

F. Protective Orders, Production and Privilege Logs[5]

The volumes of information produced in electronic discovery may make privilege review prior to production difficult. While traditional production would contemplate privilege review by the producing party before production is made, alternative methods include: a. production of massive unreviewed data, after which the responding party reviews for responsiveness, after which the producing party reviews the identified subset for privilege; b. designation of a third party who will review for privilege and responsiveness; and/or; c. agreement on application of search terms to electronic data to determine potential responsiveness to reduce the overall volume of material. When the [privilege] review is of electronically stored information, the risk of waiver, and the time and effort required to avoid it, can increase substantially because of the volume of electronically stored information and the difficulty in ensuring that all information to be produced has in fact

[5] Taken from Nuffer, *Practical Guide to Electronic Discovery*, Southern Utah Bar Association (Dec. 2, 2011).

been reviewed. Rule 26(b)(5)(B) is added to provide a procedure for a party to assert a claim of privilege or trial-preparation material protection after information is produced in discovery in the action and, if the claim is contested, permit any party that received the information to present the matter to the court for resolution. Rule 26(b)(5)(B) does not address whether the privilege or protection that is asserted after production was waived by the production[6].

When the [privilege] review is of electronically stored information, the risk of waiver, and the time and effort required to avoid it, can increase substantially because of the volume of electronically stored information and the difficulty in ensuring that all information to be produced has in fact been reviewed. Rule 26(b)(5)(B) is added to provide a procedure for a party to assert a claim of privilege or trial-preparation material protection after information is produced in discovery in the action and, if the claim is contested, permit any party that received the information to present the matter to the court for resolution. Rule 26(b)(5)(B) does not address whether the privilege or protection that is asserted after production was waived by the production.

FRE 502(d) (Attorney-Client Privilege and Work Product; Limitations on Waiver) is intended to reduce the risk of forfeiting the attorney-client privilege or work product protection so that parties need not scrutinize production of documents to the same extent as they do now. The rule provides as follows:

> **Controlling Effect of a Court Order.** A federal court may order that the privilege or protection is not waived by disclosure connected with the litigation pending before the court — in which event the disclosure is also not a waiver in any other federal or state proceeding.

The purpose of 502(d), which pertains to "disclosure of a communication or information covered by the attorney-client privilege or work-product protection," is simple. An order entered

[6] Comment to 2006 Amendments to Fed. R. Civ. P. 26(b)(5)(B).

pursuant to the rule provides litigants an extra layer of protection in the event of inadvertent production. Importantly, the production of a privileged or protected document does not constitute a waiver on behalf of the producing party both in the current litigation and "in any other federal or state proceeding." In stark contrast to FRE 502(b), which requires a demonstration that the producing party took reasonable steps to prevent disclosure and rectify the error, an order under 502(d) provides absolute protection so long as the disclosure was "connected with the litigation pending before the court."

As explained by the Committee on Rules of Practice and Procedure of the Judicial Conference of the United States, the impetus for FRE 502 was a recognition that "the current law on waiver of privilege and work product is responsible in large part for the rising costs of discovery, especially discovery of electronic information." The rule's drafters expected that the rule would permit litigants to minimize efforts to conduct privilege review, and thereby reduce the cost of responding to discovery demands, when litigants no longer faced the risk of waiver of privilege in concurrent or future litigation.

Under the new rule, the inadvertent disclosure of privileged or protected information would not create a waiver if reasonable steps were taken to prevent the disclosure, and retrieval of the information is promptly demanded. Also, the disclosure of privileged or protected information would not waive the privilege or protection accorded other information concerning the same subject matter, unless fairness so requires. Furthermore, a confidentiality order entered by the court would bind all nonparties in any federal or state court. The [proposal includes] a possible provision governing selective waiver, which would prevent a general waiver of the privilege or protection for information disclosed to a law enforcement or regulatory agency in the course of an investigation.

The court considers the following five factors in its determination of whether an inadvertent disclosure of documents effects a waiver of the attorney-client privilege: 1) the reasonableness of the precautions taken to prevent inadvertent disclosure; 2) the time taken to rectify the error; 3) the scope of discovery; 4) the extent of disclosure; and 5) the overriding issue of fairness. *Wallace v. Beech Aircraft Corp*. 179 F.R.D. 313, 314 (D.Kan.,1998) Ken M. Zeidner, Note: *Inadvertent Disclosure and the Attorney-Client Privilege: Looking to the Work-Product Doctrine for Guidance*, 22 Cardozo L. Rev. 1315 (2001).

Protective Orders

The court should enter a protective order at the start of the case to avoid delays in the production of documents. The protective order should include a "snap back" provision that allows parties to "snap back" or "claw back" any document inadvertently produced that is privileged. This type of provision will increase the speed with which parties can produce documents, because parties do not have to be petrified that if a privileged document is overlooked during the production of terabytes of data, the production will be a waiver of privilege. Until a non-waiver order is entered, the parties should agree (or the court should order) that information that contains privileged matter or attorney work product shall be immediately returned to the producing party (i) if such information appears on its face that it may have been inadvertently produced or (ii) if the producing party provides notice within 15 days of discovery by the producing party of the inadvertent production.

Production Logs[7]

[7] Source, *Recommendations for Electronically Stored Information (ESI) Discovery Production in Federal Criminal Cases*, DOJ and Administrative Office of the U.S. Courts Joint Working Group on Electronic Technology in the Criminal Justice System (JETWG) (Feb. 2012).

General recommendations for the production of ESI discovery are: a). The parties should discuss what formats of production are possible and appropriate, and what formats can be generated. Any format selected for producing discovery should, if possible, conform to industry standards for the format. b). ESI received from third parties should be produced in the format(s) it was received or in a reasonably usable format(s). ESI from the government's or defendant's business records should be produced in the format(s) in which it was maintained or in a reasonably usable format(s). c). Discoverable ESI generated by the government or defense during the course of their investigations (e.g., investigative reports, witness interviews, demonstrative exhibits, etc.) may be handled differently than in (a) and (b) above because the parties' legal discovery obligations and practices vary according to the nature of the material, the applicable law, evolving legal standards, the parties' policies, and the parties' evolving technological capabilities. When producing ESI discovery, a party should not be required to take on substantial additional processing or format conversion costs and burdens beyond what the party has already done or would do for its own case preparation or discovery production. For example, the producing party need not convert ESI from one format to another or undertake additional processing of ESI beyond what is required to satisfy its legal disclosure obligations. If the receiving party desires ESI in a condition different from what the producing party intends to produce, the parties should discuss what is reasonable in terms of expense and mechanics, who will bear the burden of any additional cost or work, and how to protect the producing party's work product or privileged information. Nonetheless, with the understanding that in certain instances the results of processing ESI may constitute work product not subject to discovery, these recommendations operate on the general principle that where a producing party elects to engage in processing of ESI, the results of that

processing should, unless they constitute work product, be produced in discovery along with the underlying ESI so as to save the receiving party the expense of replicating the work.

The parties should discuss transmission methods and media that promote efficiency, security, and reduce costs. In conjunction with ESI transmission, the producing party should provide a general description and maintain a record of what was transmitted. Any media should be clearly labeled.

Privilege Logs

A privilege log is designed to provide a party with "sufficient information to evaluate a claim of privilege or work-product protection, and to allow a court to rule on a claim of privilege without having to review the allegedly protected document itself."[8] The privilege log is sometimes referred to as a "Vaughn Index," based on the decision in *Vaughn v. Rosen*, 484 F.2d 820 (D.C. Cir. 1973). The privilege log doctrine was incorporated into F.R. Civ. P. 26(b)(5)(A) in 1993.[9]

Propose to the opposing party, and absent agreement, see if the court will order, that the privilege log need not include: 1) Communications exclusively between a party and its trial counsel. 2) Work product created by trial counsel, or by an agent of trial counsel other than a party after commencement of the action 3) Internal communications within a law firm, a legal assistance organization, a governmental law office or a legal department of a corporation or other organization 4) With respect to privileged or attorney work product information generated after the filing of the complaint, parties are not required to include any such information in privilege logs. 5) Activities undertaken in compliance with the duty to preserve information.

G. Defensible Legal Holds[10]

[8] Source: Paul Grimm and Charles Fax, *Discovery Problems and Their Solutions* 89 (ABA 2d ed. 2009).
[9] Source: Michael D. Berman, et al., eds., *Managing E-Discovery and ESI* 343-344 (ABA 2011).
[10] Taken from "*Implementing a Litigation Hold*" Nicholas Panarella, Practical Law Practice Note (2018).

When faced with litigation or a regulatory investigation in the US, companies must implement and maintain litigation holds (also called document holds or legal holds) designed to identify and preserve relevant evidence. Companies that fail to take reasonable steps to preserve relevant electronically stored information (ESI) risk severe legal repercussions, including monetary sanctions, adverse jury instructions, default judgment, and dismissal.

A litigation hold is an instruction within a business organization directing employees to preserve (and refrain from destroying or modifying) certain records and information (both paper and electronic) that may be relevant to the subject matter of a pending or anticipated lawsuit or investigation. The ultimate purpose of a litigation hold is to ensure that the company complies with its duty to preserve relevant information, including ESI and its accompanying metadata, in response to litigation or to a regulator's investigation.

US courts consistently rule that the duty to preserve begins when a company reasonably anticipates litigation or an investigation, which may happen before a complaint is filed against the company. At that time, the company must issue a **hold** and suspend any routine document destruction under its document retention policies to prevent the loss of information that may be relevant to the subject matter of the proceeding.

Determining when a company should reasonably anticipate litigation or an investigation is a fact-specific inquiry and not always an easy task. Case law does not perfectly clarify the question of when a company must issue a litigation hold and the breadth of the hold. However, courts generally find that a company should reasonably anticipate litigation when it is on notice of a credible threat that it will become involved in litigation or subject to an investigation, such as when it is involved in a pre-litigation dispute (having sent or received a cease and desist letter, for example).

Other possible triggering events include:

• Management discussions about a complaint that may lead to litigation (see *Doe v. Norwalk Community College*, 248 F.R.D. 372, 377 (D. Conn. 2007)).

• A whistleblower's complaint to management.

• The filing of an accident report (see *McCabe v. Wal-Mart Stores, Inc.*, 2016 WL 706191, at *2 (D. Nev. Feb. 22, 2016) (filing of an incident report triggered the defendant's duty to preserve relevant evidence)).

• Any other particular event that, in the company's experience, typically results in litigation or a government investigation (see *Burton v. Walgreen Co.*, 2015 WL 4228854, at *3 (D. Nev. July 10, 2015) (plaintiff's return of incorrectly filled medication to the defendant triggered duty to preserve); *Waters v. Kohl's Dep't Stores, Inc.*, 2015 WL 1519657, at *3 (N.D. Cal. Apr. 2, 2015) (duty to preserve triggered at the time of the plaintiff's serious fall); *Apple Inc. v. Samsung Elec. Co., Ltd.*, 888 F. Supp. 2d 976, 991 (N.D. Cal. 2012) (duty to preserve triggered after the plaintiff presented the defendant with its patent infringement positions)).

Likewise, when a company decides to initiate a lawsuit, it is almost always under a duty to preserve (*Apple*, 888 F. Supp. 2d at 997 (recognizing that it is more reasonable for a plaintiff to foresee litigation than it is for a defendant)). When a credible threat of litigation arises, the company should issue a written litigation hold notice quickly.

A company should assemble a team to oversee the litigation hold and document preservation processes. Because of the legal and technological issues involved in implementing a litigation hold and the possible effects of a hold on the company's business, the team should include:

• Key employees from the business units affected by the litigation or investigation.
• Employees from the company's information technology (IT) and records departments.
• In-house counsel.
• Outside counsel.

This team should coordinate to determine:
• What potentially relevant information (electronic and otherwise) is available.
• Who maintains or has access to the information.
• The form in which the information is available.
• How to cost-efficiently preserve the information.

Small companies without in-house counsel may want to appoint a high-level executive (the chief information officer or chief financial officer, for example) to be in charge of implementing and monitoring a litigation hold, as well as liaising with outside counsel.

The company's litigation hold plan should define the scope of the company's efforts to identify and preserve relevant information.At a minimum, the plan should:

• Identify the key players and custodians of relevant records associated with the litigation or investigation's subject matter,including potential witnesses, support staff, and former employees.
• Identify other current and former employees who may have records relevant to the dispute.
• Identify the relevant time period to which the preservation obligation applies.
• Identify the types of records and materials, including ESI and paper documents, that the company must preserve.
• Outline the company's data storage architecture and identify where the relevant information may reside, for example:
• on network servers, digital copiers, and backup tapes;
• in employees' offices and email folders; and
• on employees' handheld devices.
• Determine whether the company has possession, custody, or control of potentially relevant information and data, after understanding the company's data storage procedures.
• Determine whether to notify any individual or entity outside of the company, including:
• the parent company;
• subsidiaries;
• contractors;
• cloud providers;
• off-site records storage facilities; and
• former employees.

Counsel also should meet with IT personnel before and after issuing the litigation hold to better understand:

• The locations of various categories of information.
• The accessibility of the different types of information.
• Who in the company has had access to which type of information.

The company must issue the litigation hold notice to all individuals who may have relevant material. The company may easily identify some individuals based on the subject matter of the investigation or lawsuit. However, counsel always should consult with the heads of any business units affected by the lawsuit or investigation to identify all key players and other individuals who

may possess relevant materials. Counsel should determine the types of information that the key players likely possess and where they keep it.

Counsel also should provide the litigation hold notice to IT personnel (internal and outsourced) so that they can:

• Suspend any of the company systems' auto-delete features that could lead to the destruction of relevant documents (including ESI).
• Preserve the files, emails, and any records in the custody of any departing employees (including temporary staff and interns) until the litigation hold team reviews them and determines whether the company must retain them.

H. Citing Online Content Properly[11]

Citing websites and media sources using Harvard referencing.

Websites:

In text

Cite the name of the author/ organization responsible for the site and the date created or last revised):

(International Narcotics Control Board 1999)

List of references

International Narcotics Control Board 1999, United Nations, accessed 1 October 1999, <http://www.incb.org>

Include the following information:

- author (the person or organization responsible for the site)
- year (date created or last updated)
- name of sponsor of site (if available)
- accessed day month year (the date you viewed the site)
- URL or Internet address (between pointed brackets). If possible, ensure that the URL is included without a line-break.

Specific pages or documents within a website

11 Taken from "*How Do I Cite Online Sources*" UNSW, https://student.unsw.edu.au/how-do-i-cite-electronic-sources (07/31/2018)

In text

Information should include author/authoring body name(s) and the date created or last revised:

(Li 2004) or: (World Health Organization 2013)

List of references

One author:

Li, L 2014, *Chinese scroll painting H533*, Australian Museum, accessed 20 February 2016, <https://australianmuseum.net.au/chinese-scroll-painting-h533>.

Organization as author:

World Health Organization 2013, *Financial crisis and global health*, The United Nations, accessed 1 August 2013, <http://www.who.int/topics/financial_crisis/en/>.

Include the following:

- author (the person or organization responsible for the site)
- year (date created or last updated)
- page title (in italics)
- name of sponsor of site (if available)
- accessed day month year (the day you viewed the site)
- URL or Internet address (pointed brackets).

Webpages with no author or date

No author

In text

If the author's name is unknown, cite the website/page title and date:

(*Land for sale on moon 2007)*

List of references

Land for sale on moon 2007, accessed 19 June 2007, <http://www.moonlandregistry.com>.

No date

In the text

If there is not date on the page, use the abbreviation n.d. (no date):

(ArtsNSW n.d.)

(Kim n.d)

List of references

ArtsNSW n.d., *New South Wales Premier's Literary Awards*, NSW Department of the Arts, Sport and Recreation, accessed 19 June 2007, <http://www.arts.nsw.gov.au/awards/LiteraryAwards/litawards.htm>.

Kim, M n.d., *Chinese New Year pictures and propaganda posters*, Museum of Applied Arts and Sciences, accessed 12 April 2016, <https://collection.maas.museum/set/6274>.

Database items

UNSW library offers students access to the full text of journals articles, newspapers, and other publications through searchable databases. They are usually accessed through the Library Resource Database, or through MyCourse materials. Journals in full text databases are usually available via subscription by the library. For this reason, cite the database name and the date of access. Full text databases include ProQuest, EAI, and Wiley Interscience.

Library-subscribed resources usually have URLs that will not work independently, so URLs are not generally included when citing database resources.

To cite a journal article from full text database

In text

Cite as you would a journal article:

(Nicholls 2006, p. 171)

(Holmes 2004)

Articles retrieved from databases are usually in pdf form and have page numbers.

List of references

Nicholls, D 2006, "Does the meaning mean a thing?": Johnny Young's hit songs of the 60s-70s', *Australian Cultural History*, No 2, pp. 163-183, accessed 11 May 2007 from Informit Full Text Database, ISSN; 0728-8433.

Holmes, S 2004, "But this Time You Choose!': Approaching the 'Interactive' audience in reality TV', *International Journal of Cultural Studies*, No. 7, pp. 213-231, accessed 3 March 2007 from Sage Journals Online.

Cite the article as you would the same article in a print publication, listing:

- author(s) name and initials
- title of the article (between single quotation marks)
- title of journal (in italics)
- any publication information (volume, number etc.)
- page range
- accessed day month year (the date you accessed the article)
- from name of database
- item number (if given)

To cite a thesis accessed through a database

In text

Cite author, date, page number:

(Lee 2005 p. 78)

List of references

Lee, C 2005, 'Beyond the Pink: (Post) Youth Iconography in Cinema', PhD thesis, Murdoch University, accessed 15 June 2007 from Australian Digital Thesis Program Database.

Include the following:

- author name and initial
- year
- thesis title (between single quotation marks, no italics)
- type of thesis (eg. MA, PhD)
- institution
- date accessed
- from database name

Newspapers and magazines (print)

In-text

If there is no author, list the name of the newspaper, the date, year and page number:

(*Sydney Morning Herald* 7 March, 1994, p.8)

If there is an author, cite as you would for a journal article:

(Donaghy 1994, p. 3)

List of references

An unattributed newspaper article:

'UNSW gains top ranking from quality team', *Sydney Morning Herald*, 30 February, 1994, p.21.

A newspaper article with a named author:

Donaghy, B 1994, 'National meeting set to review tertiary admissions', *Campus News*, 3-9 March, p. 3.

News and magazines (online)

To cite a news article from an electronic database

In text

If the article has a named author:

(Pianin 2001)

List of references

Pianin, E 2001, 'As coal's fortunes climb, mountains tremble in W.Va; energy policy is transforming lives', *The Washington Post*, 25 February, p. A03, accessed March 2001 from Electric Library Australasia.

Include the following information:

- author (if available)
- year of publication
- article title (between single quotation marks)
- newspaper title (in italics)
- date of article (day, month, page number—if given—and any additional information available)
- accessed day month year (the date you accessed the items)
- from name of database
- item number (if given)

To cite a news article without a named author

In text

No named author:

(*New York Daily Times 1830)*

The article can also be discussed in the body of the paragraph:

An account of the popularity of the baby tapir in *The Independent* (2013) stated that ...

List of references

If there is no named author, list the article title first.

'Amending the Constitution', *New York Daily Times*, 16 October 1851, p. 2, accessed 15 July 2007 from ProQuest Historical Newspapers database.

'Baby tapir wins hearts at zoo', *The Independent*, 9 August 2013, Accessed 25 January 2014, <http://www.independent.ie/world-news/and-finally/baby-tapir-wins-hearts-at-zoo-30495570.html>.

To cite an online news article

In text

Cite the author name and year:

(Coorey 2007)

List of references

Coorey, P 2007, 'Costello hints at green safety net', *Sydney Morning Herald*, 10 May, accessed 14 May 2012, <http://www.smh.com.au/news/business/costello-hints-at-green-safety-net/2007/05/09/1178390393875.html>.

While a URL for the article should be included, if it is very long (more than two lines) or unfixed (from a search engine), only include the publication URL:

Holmes, L 2017, 'The woman making a living out of pretending to be Kylie Minogue', *The Daily Telegraph*, 23 April, accessed 22 May 2017, <http://www.dailytelegraph.com.au>.

Media releases

To cite a media release

In text

In the text, cite the author (the person responsible for the release) and date:

Prime Minister Howard (2007) announced plans for further welfare reform...

List of references

Include the following information:

- author name or authoring organisation name
- date
- title of release (in italics)
- format
- accessed day month year
- URL (between pointed brackets)

Office of the Prime Minister 2007, *Welfare Payments Reform*, media release, accessed 25 July 2007, <http://www.pm.gov.au/media/Release/2007/Media_Release24432.cfm>.

Films, television and online videos

To cite a film, video, and television or radio program

In text

Include the full title and date of production:

(*My Brilliant Career*, 1979)

(*Four Corners* 9 July 2001)

List of references

Include the following details in the list of references:

- title (if part of an ongoing series, list the episode title first, then the series name)
- year of recording
- format
- publisher/distributor
- place of recording
- date of recording (if applicable)

My Brilliant Career, 1979, motion picture, New South Wales Film Corporation, distributed by Australian Video, Australia.

Going backwards: Four Corners 2001, television program, Australian Broadcasting Corporation, Sydney, 9 July.

To cite an online video

In text

In the Overlander's (2007) short film...

The Cabinet of Dr. Caligari (1919) is a German expressionist classic from the silent era...

List of references

The Overlander 2007, *Overlander.tv: Aboriginal tent embassy*, Canberra, online video, accessed 31 July 2007, <http://www.youtube.com/watch?v=abMlHjO2nh4>.

The Cabinet of Dr. Caligari, 1919, online video, accessed 20 June 2011, <http://www.youtube.com/watch?v=ecowq77Y3C0>.

Audio CD or CD ROM

In text

Cite the CD title and year:

(*Australia through time* 1994)

List of references

The bibliographic details are the same as those required for films, videos, DVDs, television and radio programs:

- title (in italics)
- year of recording
- format
- publisher
- place of recording

Australia through time 1994, CD-ROM, Random ROM in assoc. with the ABC, Sydney.

To cite a Weblog (blog)

In text

Include author name and year of posting:

(Bartlett 2006)

(Bahnisch 2007)

List of references

Include:

- the name (or alias) of the author

- year of post
- the title of the posting (if applicable) between single quotation marks
- the title of the site (in italics)
- format
- the date of posting (day month)
- accessed day month year (the date you viewed the site)
- the URL of the blog post (between pointed brackets)

A blog

Bartlett, A 2007, *The Bartlett diaries*, weblog, accessed 22 May 2007, <http://www.andrewbartlett.com/blog/>.

A blog post

If you are citing a group blog, cite the author of the post:

Bahnisch, M 2007, 'The commentariat vs. the people?', *Larvatus Prodeo*, weblog post, 11 May, accessed 22 May 2007, <http://larvatusprodeo.net/2007/05/11/the-commentariat-vs-the-people/>.

To cite a Wiki

In text

As wikis usually feature user-generated content, there is usually no named author. Cite the title of the wiki and the date of last revision:

(*An Essay Evolves* 2007)

List of references

Include the following information:

- article name (between single quotation marks)
- title of wiki (in italics)
- format
- date of last revision
- accessed day month year (the date you viewed the site)
- the URL of wiki article page (between pointed brackets)

'Freud and science', *An essay evolves*, wiki article, March 8 2007, accessed 20 May 2007, <http://evolvingessay.pbwiki.com/Freud+and+Science >.

Personal communication

To quote from a privately obtained interview, letter or other personal communication

In-text

Include in the abbreviation 'pers. comm.' in your text reference:

(B Daly 1994, pers. comm., 7 Aug.)

Note that the initial(s) precede the surname.

List of references

- Details of a personal communication do not usually need to be included in the List of References as it cannot be traced by the reader. Check with your tutor or lecturer for their preferences.
- Before using personal communications, ensure you have the permission of the person with whom you communicated.

To cite an email

In text

Include the abbreviation 'pers. comm.' in your in-text reference:

(J Smith 2006, pers. comm. 23 July)

Note that the initial precedes the surname.

If the form of communication is relevant, mention it in the text:

Email confirmation was received (J Smith 2006, pers. comm. 23 July).

List of references

References to emails are treated as a form of personal communication and are not usually included in reference lists as they cannot be traced by the reader. However, if your tutor or lecturer requests an entry in the List of References, cite emails as below:

Smith, J 2006, email 23 July, <j.smith@mailbox.com.au>.

To cite electronic mail lists, usenet groups and forum boards

In text

Include the author name and date of posting:

(Wiggers 2006)

List of references

Wiggers, D <darryl@nestcom.net> 2006 ‘Media and imperialism’, list server, 4 June, H-Net Humanities & Social Sciences OnLine, accessed 12 September 2006, <http://www.h-net.org/~film/ >

Include the following details:

- author
- author's details (eg. email address)
- date of posting
- title of posting (from the 'subject' line in the message)
- format (listserver)
- name of list owner
- accessed day month year (the date of viewing)
- URL or Internet address (between pointed brackets)

Podcasts

In text

(*Lingua Franca* 2007)

referring to the speaker:

Jill Kitson (Lingua Franca 2007) reported that ...

List of references

List a podcast as you would a radio program. Include the following:

- name of the podcast (in italics)
- year
- format (podcast)
- publisher
- date of podcast (day, month)
- accessed day month year
- the URL (between pointed brackets)

Lingua Franca 2007, podcast radio programme, ABC Radio National, 28 April, accessed 25 May 2007, <http://abc.net.au/rn/podcast/feeds/lin.xml>.

Twitter

To cite a tweet

Include the author name and date of posting:

(Gillard 2016)

Use the author's real name. Only use the Twitter handle as the author if the author's real name in unknown.

Enclose the tweet itself in 'single quotes'. Type the words **Twitter post**, and the day and month of the post, after the text of the tweet.

Gillard, J 2016, 'No girl's opportunities should be defined by her gender. All children deserve the same access to health, education & the future', Twitter post, 7 March, accessed 15 April 2016,<https://twitter.com/JuliaGillard/status/706921359314526208>.

- the name (or alias) of the author
- year of post
- the tweet itself, between single quotation marks
- format (twitter post)
- the date of posting (day month)
- accessed day month year (the date you viewed the site)
- the URL of the tweet (between pointed brackets)

Facebook post

In text

Include the author name and date of posting:

(The Learning Centre UNSW 2015)

(Obama 2015)

The author name can also be included in the running text:

A 2015 post on Obama's Facebook page stated that ...

Reference list

- Author name and initial
- year
- place the first few words of the post (up to about 15 words) in 'single quotes', using [...] if necessary to indicate that some words have been left out.
- format (Facebook post)
- date of post (day, month)
- accessed day month year
- the URL (between pointed brackets)

The Learning Centre UNSW 2015, 'November is AcWriMo (Academic Writing Month) at UNSW! [...]', Facebook post, 8 October, accessed 27 February 2016, <https://www.facebook.com/TLC.UNSW/>.

Obama, B 2015, 'It's not about politics. It's about whether we as a nation live up to our founding ideal of liberty and justice for all [...]', Facebook post, 1 November, accessed 11 April 2016, <https://www.facebook.com/barackobama/>

Citing Images and Tables Found Online

To cite an online image you are discussing in your writing

In the text

Mention the image in the text and cite the author and date:

The cartoon by Frith (1968) describes ...

If the image has no named author, cite the full name and date of the image:

The map shows the Parish of Maroota during the 1840s (Map of the Parish of Maroota, County of Cumberland, District of Windsor 1840-1849) <http://www.oph.gov.au/frith/theherald-01.html>.

List of references

Frith J 1968, From the rich man's table, political cartoon by John Frith, Old Parliament House, Canberra, accessed 11 May 2007. Include the following information:

- author (if available)
- year produced (if available)
- title of image (or a description)
- Format and any details (if applicable)
- name and place of the sponsor of the source
- accessed day month year (the date you viewed/ downloaded the image)
- URL or Internet address (between pointed brackets)

If there is no named author, put the image title first, followed by the date (if available):

Khafre pyramid from Khufu's quarry 2007, digital photograph, Ancient Egypt Research Associates, accessed 2 August 2007, <http://www.aeraweb.org/khufu_quarry.asp>.

Map of the Parish of Maroota, County of Cumberland, District of Windsor 1840-1849, digital image of cartographic material, National Library of Australia, accessed 13 April 2007, <http://nla.gov.au/nla.map-f829> .

To cite online images/ diagrams used as figures

Figures include diagrams, graphs, sketches, photographs and maps. If you are writing a report or an assignment where you include any visuals as figures, you must include a reference.

If you include figures in your work, they should be numbered and labelled with captions. Captions should be very simple and descriptive and be followed by an in-text citation. Figure captions should be directly under the image.

In the text of the assignment

Cite the author and year:

Figure 1: Questions the Literature Review can Answer (The Learning Centre 2007)

In the list of references

Provide full citation information:

The Learning Centre 2007, Some of the questions a review of the literature can answer, digital image, The University of New South Wales, accessed 2 August 2007, http://www.lc.unsw.edu.au/onlib/litrev.html.

To cite online data in a table caption

If you reproduce or adapt table data found online you must include a citation. All tables should be numbered and table captions should be above the table.

In the text of the assignment

Table 2: Agricultural water use, by state 2004-05 (Australian Bureau of Statistics 2006)

State	**Total ML**
NSW (including Canberra)	3 976 108
Vic.	2 570 219
Qld	2 864 889
SA	1 004 828
WA	429 372
Tas	255 448
NT	45 638
Total ML	**11 146 502**

List of references

Include the name of the web page where the table data is found.

Australian Bureau of Statistics 2006, *Water Use on Australian Farms*, 2004-05, Cat. no. 4618.0, Australian Bureau of Statistics, Canberra, accessed 4 July 2007 <http://www.abs.gov.au>.

What is the 'accessed' date?

The date on which you viewed or downloaded the source. As online materials can change or disappear at any time, you must cite the date on which you accessed the information.

I. Privileged ESI That Is Discoverable (Exceptions)

Generally, litigation hold notices are privileged, protected by the attorney-client privilege or work product doctrine. See, e.g. *Gibson v. Ford Motor Co*., 510 F. Supp. 2d 1116, 1123 (N.D. Ga. 2007). However, the privileged nature of litigation hold letters may be lost if a party spoliates evidence (destroys evidence) or fails to observe appropriate litigation hold procedures.

Litigation hold letters are not discoverable in litigation if they include information protected by the attorney-client privilege. See, e.g, *Muro v. Target Corp*., 250 FRD 350, 360 (N.D. Ill. 2007) (finding a litigation hold notice privileged because it was a communication "of legal advice from corporate counsel to corporate employees regarding document preservation…."). Although information in litigation hold letters may be protected, courts often permit discovery of the date of issue, the recipients, and steps taken to preserve evidence. *Cannata v. Wyndham Worldwide Corporation*, Case No. 2:10-cv-00068-PMP-VCF (D. Nev. Aug 16, 2012).

J. Clawback Agreements

Attorneys should enter into clawback agreements prior to the commencement of e-discovery. Claw-back agreements are formal agreements that prevent the attorney-client privilege from being waived by an inadvertent disclosure of privileged information. Rather the receiving party must return the privileged material to the responding party.

Quick peek agreements allow attorneys to look at each party's entire data before production. Attorneys then designate items that are responsive to the discovery request and items that are privileged. Attorneys should ensure that such agreements address electronic documents in general and metadata specifically.

K. Making Email Evidence Usable in the Courtroom[12]

One of the first places to look for assistance in understanding the law governing the use of electronic records as evidence in court is *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007), in which Magistrate Judge Grimm issued a 101-page order setting forth the issues and which rules and cases were applicable. The opinion is a primer on how to use electronic evidence in court.

FRE 901 establishes the requirements for authentication or identification as a condition precedent to the admissibility of non-testimonial evidence. FRE 901(b) gives examples of how authentication can be accomplished. Generally, the proponent of the internet printout must provide testimony by live witness or affidavit that the printout is what it purports to be. See *In re Carrsow-Franklin*, 456 B.R. 753, 756-57 (Bankr.D.S.C. 2011) (noting that blogs are not self-authenticating and rejecting blog evidence due to failure to present authentication testimony) and cases cited there. The *Lorraine* case gives an excellent discussion of how Rule FRE 901 works with FRE 104 and the necessity for the court to decide authentication as a preliminary question. However, if the evidence is not relevant to begin with, it cannot be authenticated because it cannot meet the requirements under FRE 104 and 401.

The social media evidence has to be relevant to issues in the case. See FRE 401. The courts routinely decide relevance of such evidence. See, e.g., *Bass*, supra; *Ledbetter*, supra; *Engman v.*

[12] Taken from "Social Media Evidence-How To Find It and How To Use It" ABA Section of Litigation, 2013 ABA Annual Meeting, Aug. 8-12, 2013).

City of Ontario, 2011 WL 2463178*10-11 (C.D.Cal. June 20, 2011) (excluding information on plaintiff's MySpace page); *B.M. v. D.M.*, 2011 WL 1420917, at *5 (N.Y. Sup. Ct. Apr. 7, 2011) (admissions in blog were relevant and admissible). If a party fails to produce relevant evidence in discovery, the consequences can be severe. In *Lester v. Alliance Concrete Co.*, a Virginia state court reduced a jury award by over $4 million dollars and ordered the plaintiff and his counsel to pay the defendants over $700,000 in fees and expenses because of deliberate deletion of Facebook photos responsive to discovery requests.

Hearsay objections may arise when using electronic evidence. See *Miles v. Raycom Media, Inc.*, 2010 WL 4791764 *3 n.1 (S.D.Miss. Nov. 18, 2010) (unsworn statements made on Facebook page by nonparties were inadmissible under FRE 801). You may have multiple layers of hearsay involved and have to rely upon several hearsay exceptions. Judge Grimm provides an extensive discussion in Lorraine of hearsay in the context of electronically stored information. The procedural posture may affect how the court treats the information. In granting defendant's motion for summary judgment in *Witt v. Franklin County Board of Education*, 2013 WL 832152 (N.D.Ala. Feb. 28, 2013), the court considered three Facebook messages from nonparties offered by plaintiff because plaintiff could have reduced them to admissible form at trial by calling the witnesses. You may also often be faced with objections concerning unfair prejudice under FRE 403 and 404. See, e.g., *Quagliarello v. Dewees*, 2011 WL 3438090 *2-4 (E.D.Pa. Aug.4, 2011) (allowing some but not all photos from plaintiff's MySpace page because relevance to emotional distress claim outweighs unfair prejudice); *State v. Townsend*, 208 N.C. App. 571, 706 S.E.2d 841 (2010) (court denied request to allow testimony about Facebook and MySpace postings because probative value substantially outweighed by danger of unfair prejudice). Not all courts will use the same approach. Some commentators suggest that statements on Facebook and other social media are not

considered statements of one's actual knowledge or belief but more in the nature of loose talk that do not merit admission as evidence. Those arguments seem to go to the weight to be given not the admissibility.

II. What To Look for, Where to Find It and What to Do with It

A. Types of Data, Production Specifications and Formats-In Detail[13]

Counsel should identify in a production protocol the format in which the parties intend to produce hard copy documents and ESI. Production format describes the manner in which the producing party actually gives responsive documents and ESI to the requesting party.

Parties and subpoenaed entities often produce hard copy documents by either:

• Making the original hard copy documents available for inspection (review) and copying.
• Producing photocopies of responsive documents.
• Scanning documents and producing the resulting electronic files (such as PDFs), which also may include searchable text generated by an optical character recognition (OCR) tool.

Counsel should specify in the protocol how the parties should produce hard copy documents that:

• Originated as hard copies (like handwritten logs or notes).
• Are printouts of ESI (like printed emails).

When producing documents, counsel may prefer to treat hard copies as surrogates for the corresponding ESI for ease of production (that is, to relieve them of the obligation to locate, collect, and process the electronic version of the document).

However, the receiving party may object to hard copy surrogates because the hard copies lack the original electronic files, metadata, and the parties generally cannot electronically filter, sort, or search them.

Common ESI production formats include:

• Native productions.

[13] Taken from "*Document Production Protocols in Federal Civil Litigation*," Practical Law Litigation Practice Note.

• Image productions

The production format impacts other production specifications, such as:

• The need for a load file.
•How the producing party discloses the beginning and end of each document

Native format refers to electronic files produced in their original or maintained form (for example, producing a responsive Microsoft Word document as a .doc or .docx file, rather than converting it and producing it as a PDF).

Certain types of ESI are significantly more useful in their native format, so counsel may opt to produce those file types natively, even if they produce other ESI as images. For example, native versions of:

• Spreadsheets (such as Microsoft Excel files) enable the requesting party to view cell formulae, color coding, relationships among content, and the organization of columns, rows, and worksheets.
• Presentation files (such as Microsoft PowerPoint files) enable the requesting party to view animations, layered content, and video elements that may not be fully visible when the presentation is converted to a static image.

Even when counsel generally agree to produce ESI in native format, they may need to make special arrangements for ESI that:

• They must **redact**. Parties cannot permanently and securely redact native files without altering the native file. Counsel often make exceptions to a native production agreement and allow parties to produce redacted ESI as images.
• Other parties cannot view without access to specialized software. Some ESI can only be accurately displayed with software that the requesting party cannot access.

Counsel often agree to produce this ESI in an alternative format. For example, rather than producing native ESI from a proprietary database, counsel may:

• negotiate the manner in which the producing party queries the database for relevant information; and
• agree that the producing party can produce a PDF of the query result.

When natively producing ESI, some counsel only provide the responsive native files. On receipt, the requesting party can either:

• Open and review each file using the software program used to create it (or another compatible software program).
• Process the ESI to extract metadata and text and then upload it to a document review platform for review.

However, counsel natively producing ESI typically process the ESI before production. They may produce with the native files:

• A load file to provide select metadata and other information
• Extracted text files to enable the requesting party to simultaneously search the content of all produced ESI.

Image Productions

Counsel producing ESI as images convert the responsive ESI to static, digital images (such as PDF or TIFF) and produce only the resulting images (for example, converting a responsive Microsoft Word document to PDF and producing only the PDF). The requesting party may prefer to receive a particular type of image, depending on how it intends to review the produced ESI.

For example, if a requesting party:

• Plans to upload the images to a document review platform, the available platform may only accurately display certain image types.
• Does not have access to a document review platform, it may prefer to receive ESI as PDFs so that it can view the ESI in a simple PDF viewer.

When producing images, counsel may convert each responsive file to a static, digital image and produce only the image. On receipt of this production, the requesting party can either:

• Open and review each file using a software program that displays image files. Depending on the producing party's conversion process, the requesting party may or may not be able to search the text of the image file.
• Process the ESI to extract any text or metadata that was preserved by the producing party's conversion process and then upload the images and extracted metadata and text to a document review platform for review.

However, because counsel typically process ESI before they convert it to static images, counsel may produce with the images:

• A load file containing select metadata and other information
• Extracted text files to enable the requesting party to simultaneously search the content of all produced ESI.

The parties may agree to produce some file types as images and other file types as native files. Although many common types of ESI, like emails and word processing files, generally are usable as static images, the production of other file types as images may significantly limit the requesting party's review of those documents. For example, converting a Microsoft Excel file to an image typically breaks the content of the spreadsheet into several pages that the requesting party cannot practically view in the proper orientation.

Load Files and Extracted Text Files

Load files provide information about produced ESI, such as:

• Metadata.
• Content generated during document review and production, such as:
• Bates numbers;
• confidentiality and privilege designations; and
• the relevant issue or discovery request.

The parties should identify in the protocol whether to provide load and extracted text files. Parties generally provide load and extracted text files only when the requesting party intends to upload the ESI production to a document review platform. If the requesting party uploads to a document review platform a production that includes load and extracted text files, the platform generally:

• Links the information in the load and extracted text files with the corresponding image or native file.
• Permits counsel to leverage the load file and extracted text content as they search, sort, and filter the universe of ESI hosted in the platform.

The types of load and extracted text files counsel need vary by document review platform. Counsel should identify in the protocol compatible file types to ensure that other producing parties provide workable load and text files. If the requesting party does not intend to use a document

review platform to host and review the production, load and text files generally have little to no value.

Unitization

Regardless of production format, counsel generally should ensure that:

• Their hard copy and ESI productions maintain original document breaks.
• The original document breaks are apparent to the requesting party.

How counsel communicate where each produced document begins and ends depends on the production format. For example,counsel producing:

• PDFs can produce each ESI file as a single PDF, so that all pages of a multi-page document are contained in a single PDF.
• ESI as images with a load file often:
• provide single-page images (in other words, a separate image file for each distinct page in the production); and
• construct the load file in a way that enables the requesting party's document review platform to accurately and automatically reconstruct each multi-page document.

If counsel plan to identify document breaks in a manner that is only useful if the production is loaded into a document review platform (such as in a load file), they should confirm that the requesting party has access to a sufficient platform.

B, Obtaining Evidence: Smartphones, PCs and Tablets, Third Parties, Flash Drives and External Hard Drives, Cloud Storage

The principal methods to obtain this type of evidence are using production requests and subpoenas of third party items.

Most employers have policies that information on company-supplied smartphones, PCs, tablets, flash and external drives and information stored in the cloud belongs to the company. With departing employees, it is essential that the employer enforce its policy to have all company-related information returned by the employee or contractor.

As for privately owned equipment, there are potential privacy interests that may prevent obtaining this type of evidence, at least without a subpoena. Medically related information may be protected under HIPAA, while financial information may be subject to consumer privacy laws.

Use of a forensic examiner may be necessary if there is suspicion of recent downloading and/or deletion of data. It may be necessary to obtain or break through password-protected data and information.

C. Using Apps on Your Clients Smartphone to Collect Evidence[14]

Smartphones contain a wealth of personal and sensitive information like passwords, security or access codes, account numbers, electronic communications, and much more. But they are more than mere containers of data. Between the operating system, installed applications, and service providers, there's a wealth of information that can provide dramatic insight into conversations, activities, habits, preferences, and movements of the phone's user.

There are essentially three places where smartphone related data can be found: on the phone itself, with mobile app providers (e.g. Facebook, Snapchat, or Yelp), and with the service provider (e.g. AT&T or Verizon). Data from all three sources can be very useful in civil lawsuits, criminal cases, or internal investigations, depending on the needs of the case.

Let's look at data stored locally on the phone and captured by mobile application providers. Many mobile apps require access and store data you're not aware of, enabled by permissions sometimes given without a second thought. Common examples are photo editing apps accessing camera and media files and navigation apps accessing your GPS (Global Positioning System). Some apps seek permissions to access user data not needed for app functionality, like gaming apps accessing text messages or contacts. Many apps transmit and

[14] Taken from Supreet Singh, "The Smartphone: A Treasure Trove of Evidence"

receive data between phone and remote servers, meaning a copy of user content may be collected and stored on those remote servers in the name of a better user experience.

The third player, service providers, collect and store information like historical call records, including locations of cell towers a phone connected to. This can be powerful evidence in relatively simple cases or highly complex crimes. Let's use a middle of-the-road example: serial bank robbery. If a bank crew robbed different banks at different locations, and they carried phones turned on during the thefts, then cell tower logs from in and around each bank's location could be analyzed to narrow down persons of interest, as it would appear unlikely for people other than the robbers to be at all the same locations on the dates and times of the thefts. Smartphone data can be a key source of evidence in litigation or investigations. Preserving and retrieving it in a manner that is admissible and defensible in court is vital. Many smartphones can be wiped remotely, so they usually should be turned off when seized, and stored in a secured location with no cellular, WiFi, or Bluetooth connectivity. Smartphones may present challenges to many forensic investigators due to their frequently changing systems. Capturing all associated data can be difficult – interpreting it even more so. We have had great success with custom tools developed to speed up the extraction, analysis, and mapping of usage data.

Counsel should be aware there's more to smartphones than meets the eye. At a minimum, the first step in litigation or investigations should be to preserve data from any smart device, and seek expert forensic assistance. It could make an invaluable impact in your next case.

A. Predictive Coding Dos and Don'ts[15]

[15] Taken from Blog, Predictive Coding Do's and Don'ts, Insight Case Management, http://www.iscmny.com/blog/predictive-coding-dos-donts/; and Christopher Spizzirri, Predictive Coding: What's New and What You Need to Know, Law Practice Today, ABA Law Practice Management Section (Aug. 2012).

Technology-assisted review, or TAR as it has come to be known, is a broad term that (mostly) means what it says: using a technology to assist review. Here, the technology typically refers to some form of language-based analytics. The two primary flavors are "concept clustering" (grouping documents based on content) and "concept search" (or 'find more like this'). These technologies aren't new. In fact, the 'find more like this' feature has been available in legal research software for some time now. What's new is using these analytics in a formal workflow to improve review efficiency. In the past, users were given access to these analytics and, maybe, given ad hoc advice from their vendor on using them, but vendors hadn't offered a predefined plan for using the analytics. Now, many vendors (and more every day, it seems) are offering a defined workflow for using analytics to improve the efficiency and effectiveness of document review. So, "technology-assisted review" ultimately is a workflow or process designed to make good use of pre-existing technologies. So what is the secret sauce that transforms a workflow into technology-assisted review? There is no one special recipe for making a TAR workflow. As far as I can tell, each vendor has developed a unique workflow for improving review with analytics.

What's predictive coding and how is it different from technology-assisted review? Predictive coding is a form of technology-assisted review offers computer-generated document relevance rankings. Those relevance rankings ARE the predictive coding. The computer is predicting the likelihood that you will code a document one way or another. If the relevance ranking is high, the computer is predicting that you are likely to agree the document is relevant. Other TAR methods don't rank relevance, so they aren't "predictive coding."

In a typical TAR workflow, the first thing to do is gather a “seed set” of documents from among all the documents needing review. The seed set will ideally be reviewed by the lawyer who knows the most about the case. It wouldn’t be uncommon for the most senior partner on a matter to delegate this task to a junior partner or senior associate. Either way, the set needs to be reviewed by someone with strong knowledge of the case

Back to the seed set. After gathering and reviewing the seed set, the machine begins to learn what we are looking for by analyzing the relationships between the words in documents we have marked responsive. It then looks for similar documents.

In e-discovery, predictive coding is primarily used to quickly and accurately locate relevant document in order to expedite the review process.

How predictive coding works

The software is a keyword search designed to look at broad patterns of language to establish what is relevant, while creating a profile of both relevant and irrelevant documents.

This can assist in faster decision making, saving time and money, and is more reliable in finding documents which a human reviewer might have missed.

Do’s and Don’ts

- Use more than one technique/algorithm
- Start with familiar data in order to view its success and functionality, then expand into unfamiliar data
- Don’t use the default model accuracy metric
- Don’t leave it all up to the software – clear definition of what is needed

Keyword search – How do Private investigators work

When it comes to private investigations, we can use either a manual search of keywords that change from case to case, an automated system that allows the investigator to define keywords to narrow the search.

For example, TA9 IntSight is a data analysis platform that is designed to integrate with a variety of data sources and channels all the data collected to one source. One of the options is to predefine keywords relevant to our search.

B. Metadata Explained

Metadata is information embedded in an electronic file about that file, including author and date of creation. It is increasingly common for attorneys to request that information in discovery. Complying with this request presents a variety of problems.

1. Defining Different Types and Formats

Metadata is often hidden, invisible, and normally inaccessible by the computer's user. Examples of metadata include comments, edit dates and history, authorship, dates sent and received, et cetera. Metadata is simply "data about data."

2. Metadata Landmines to Avoid

Does this mean that metadata is to be treated the same as ordinary data in the attorney-client privilege context? In other words, what happens to metadata if it is inadvertently sent to opposing counsel in a discovery request? Does this mean the attorney-client privilege is waived? The ABA Standing Committee on Ethics and Professional Responsibility has held that attorneys may mine for metadata embedded in responses to discovery requests. Instead of limiting its holding to inadvertent disclosures, the committee only limited its holding's scope to metadata that was not obtained in a "fraudulent, deceitful, or otherwise improper" manner. As a result, an attorney who inadvertently receives metadata embedded in privileged electronic documents can argue that the privilege has been waived. Contrary to the ABA's decision, some state bars have required attorneys to return privileged metadata transmitted inadvertently. These states base their rules primarily on the 2006 amendments to Federal Rules of Civil Procedure. Rule 26(b)(5)(B) provides

that [i]f information produced in discovery is subject to a claim of privilege or of protection as trial-preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; [and] must not use or disclose the information until the claim is resolved. In the District of Columbia—one of the jurisdictions that does not follow the ABA's decision—attorneys may not mine for metadata if the attorney has actual knowledge that the data was sent inadvertently. New York goes one step further, not requiring actual knowledge—just inadvertent submission—to prohibit an attorney's use of privileged metadata. Attorneys should check their respective bar rules to ensure that they are in compliance with all ethical requirements regarding mining and use of metadata.

3. "Scrubbing" Metadata to Remove It From Documents[16]

Most of us are oblivious to the metadata contained in the files we're preparing and it can be useful stuff, but, because it's not obviously visible to authors and reviewers, it has the potential to embarrass or, at its worst, do serious damage.

Metadata can consist of anything from comments, tracked changes, revision marks, and document properties, to personal information, such as an author's name, a company's details, timestamps, headers, footers, watermarks and more. Getting rid of metadata when a file is circulated or shared can often be for your own good.

Here are the top five reasons why:

1. Mum's the Word

Microsoft Word is essentially the mother of all word processing applications, so she'll look after us, right? Surprisingly, misuse of Word's "track changes" feature is one of the most common

[16] Taken from "Five Reasons Removing Metadata Is A Must," https://www.workshare.com/blog/top-5-reasons-why-removing-metadata-is-a-must

causes of hidden metadata escaping the family. Most users don't realize you must accept changes and then turn the tool off *before* attaching the document to an email in order to avoid that moment of despair when you realize you've just sent something out that you definitely shouldn't have.

2. The BIG reveal

The Rules of Professional Conduct say a lawyer shouldn't reveal information relating to the representation of a client unless the client consents to it themselves. Therefore, accidentally sending a client's details in the metadata contained within an email attachment is a contravention of the rules.

Beyond this, the introduction of the General Data Protection Regulation (GDPR) in May 2018, will raise the stakes higher, with potential fines for those who (even inadvertently) share personal data pertaining to EU citizens without their permission.

3. Rabbit in the Headlines

The media *love* a good data blunder, so it's preferable not to give them one to talk about. Metadata can be a powerful weapon in the wrong hands, and email is the smoking gun. There are numerous instances of metadata "shaming" large firms and government bodies alike. Only last year, a large pharma retailer left track changes in a document that was emailed to a national newspaper with embarrassing consequences.

4. Skinny files with that?

If you're still not concerned about sending out personal data to others, the fact that metadata adds extra "weight" to your files might convince you. Metadata, especially that of image formats, like JPEG, is often held in a separate file, which results in the unnecessary use of valuable bandwidth.

5. You won’t feel a thing

Data protection is definitely something to keep in the front of your mind when sharing files if you want to cover your back. In an age where technology is part of daily life, it’s easy to get complacent about sharing data, but sifting through every detail is time-consuming and prone to human error, so automatically removing metadata is obviously the best way forward.

4. Producing Responsive Non-Privileged ESI with Appropriate Metadata and OCR

Counsel should document in their production protocol whether they intend to produce metadata and, if so:

• Which metadata fields they intend to produce for each type of ESI. For example, counsel often produce different metadata fields for email than they produce for general office documents (such as Microsoft Word files or PDFs) or digital photographs.
• How they intend to present the metadata. For example, counsel may produce:
• metadata in a load file; or
• ESI as native files that contain the metadata within the file.

When considering which metadata fields to produce, counsel should generally plan to preserve and produce metadata fields that they reasonably expect are relevant to the case unless opposing parties agree that they do not need to do so. For example,in cases involving the alleged manipulation of critical documents, the metadata field reflecting the date on which ESI was last accessed or last modified is likely relevant for at least a subset of ESI. However, in other cases, that metadata field may not be important.

Commonly produced metadata fields include:

• Created date and time (may be parsed into separate metadata fields).

• Last modified date and time (may be parsed into separate metadata fields).

• Last accessed date and time (may be parsed into separate metadata fields).

• Custodian.

• Author.

• File name.

• File extension.

• File path.

• Family or group identifier.

• Email from (including name and email address).

• Email to (including name and email address).

• Email CC (including name and email address).

• Email BCC (including name and email address).

• Email subject.

• Email sent date and time (may be parsed into separate metadata fields).

• Email received date and time.

• Email time zone.

Counsel can only produce metadata if they previously implemented preservation, collection, and processing protocols that preserved the relevant metadata. Failing to do so may result in the permanent corruption or loss of the metadata that they later want (or need) to produce.

F. Working With and Subpoenaing Social Media Companies[17]

The retention policies of various wireless carriers mean the window of time within which to obtain the actual content of text messages is narrow. There is a narrow window within which to obtain the actual content of text messages which may ultimately be important to your case.

[17] Taken from Michael Lowry, "*Subpoenaing Text Messages"* (Sept. 24, 2012) and William Vogeler, "Social Media Companies Must Comply with Subpoenas for User Communications" https://blogs.findlaw.com/california_case_law//06/social-media-companies-must-comply-with-subpoenas-for-user-communications.html (June 15, 2018). See also, "Social Media Evidence-How To Find It and How To Use It" ABA Section of Litigation, 2013 ABA Annual Meeting, Aug. 8-12, 2013).

In a significant social media case, the California Supreme Court said Facebook and other social media companies must comply with subpoenas for information that users make public.

Facebook v. Superior Court of the City and County of San Francisco is actually based on a criminal case, but it reaches beyond criminal law or procedure. In the underlying matter, Derrick D. Hunter and Lee Sullivan subpoenaed social media communications of a homicide victim and a witness.

The state Supreme Court said the defendants are entitled to social media posts and messages that the users made public. The judges remanded the case to the trial court to sort out which communications were public at the time.

A review of many reported cases indicates that the likeliest sources of relevant information are Facebook, Twitter, and MySpace. While LinkedIn has become immensely popular, it is work-oriented and postings are less likely to reveal the bad acts and true character of the posters. Facebook. Your public postings on Facebook go to anyone in the world unless you have placed access restrictions on your Facebook page. Note also that Facebook updates access controls and often defaults new features to "public view" which necessitates frequent checking of preferred settings and options to maintain desired levels of privacy. Twitter. Twitter posts differ from Facebook posts. Twitter users post "tweets" of up to 140 characters, can monitor, follow, and repost others' tweets, and can permit or forbid access to their own tweets. Twitter is more like a private electronic bulletin board which is only seen by persons who sign up to be on the board. If you follow someone on Twitter, Twitter will send them an email notifying them that you are following them using your Twitter account name. Despite this difference, tweets on Twitter are usually discoverable. MySpace. After dominating from about 2005 to 2008, MySpace appears to have lost the battle for No.1 to Facebook in the personal message arena. However, it has had more

success in discovering and promoting new music artists. MySpace is in the process of reinventing itself by focusing on interaction about entertainment, including music, movies, celebrities, and TV.

Privacy Protection

A. Federal Statutory Privacy Protection.

A number of federal statutory schemes govern the possession and use of individuals' private data. Included:

1. The Federal Trade Commission Act (FTC Act), 15 U.S. C. § 25, generally prohibits unfair and deceptive acts and practices affecting commerce. The FTC has brought a number of cases under the FTC Act in instances where companies have failed to comply with 3 their own privacy policies. These types of actions have generally arisen in two circumstances: (1) where the company promised a specific level of data security to its customers, only to have its data compromised because it did not in fact deliver the promised level of security, and; (2) where the company promised not to sell or otherwise disclose customer information to third parties, only to do so when a sale of the information turned out to be financially attractive to the company;

2. The Financial Services Modernization Act, also known as the GrammLeach Bliley Act (GLBA), 15U.S.C. §§ 6801-6809, requires financial institutions to issue privacy notices to their customers giving them the opportunity to opt-out of sharing personally identifiable financial information with outside companies;

3. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), includes provisions designed to encourage electronic transactions and also creates an opt-in framework for the use and disclosure of protected health information. There are hefty criminal and civil penalties available to punish violators;

4. The Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501-08 and 16 C.F.R. Part 312, applies to online business collecting information from children under the age of 13;

5. The Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g and 34 C.F.R. § 99, and the Protection of Pupil Rights Amendment (PPRA),"), 20 U.S.C. § 1232h and 34 C.F.R. § 98, govern student records. Institutions that receive federal funds must comply with FERPA or lose their federal funding. Specifically, the statute and its regulations cover public and private institutions that "provide education services or instruction" and receive any kind of federal funding. See 34 C.F.R. § 99.3.

6. The Fair Credit Reporting Act (FCRA), 15 U.S.C. §§ 1681 et seq., applies to data collected by consumer reporting agencies;

7. The primary statute affecting discovery of social media is the Stored Communications Act (SCA), 18 USC §§ 2707-2711, which is part of the Electronic Communications Privacy Act enacted in 1986. This is a pre-Internet statute. See Section D below for more about the SCA.

The 50 individual states have their own privacy laws and standards. Many states have laws governing privacy for social security numbers; some have laws governing website privacy policies. Some states, like California, have constitutional provisions as well as numerous privacy statutes (see, e.g., California Constitution, Sec. 1, California Invasion of Privacy Act and Song-Beverly Credit Card Act). California also has a new Privacy Enforcement and Protection Unit.

International data privacy laws may be more restrictive than those in the United States though there are decisions in other countries, including the United Kingdom and France, that allow employers to discipline employees for making social media comments that are detrimental to the employer and its image. The Baker Hostetler law firm has an accessible International Compendium

of Data Privacy Laws on its website. It is organized by country and runs about 200 pages long. If you have an issue regarding social media evidence posted by someone outside the United States, then you ought to examine the laws that apply in that country as well as the laws in the country in which you are trying to obtain the information. In addition to the laws enacted by individual countries, there are international organizations' laws that might apply. For example, EU Directive 9546 was created to regulate movement of personal data across the borders of the EU countries and to establish security guidelines for storing, transmitting, and processing personal information. It has 33 articles in 8 chapters and took effect in October 1998. Other European Commission (EC) enactments also affect privacy such as the e-Privacy Directive applicable to the communications sector and Framework Decision 2008/977/JHA applicable to police and criminal matters. The EC is also expected to unify data protection in the EU with a single law called the General Data Protection Regulation. A proposal was published on January 25, 2012, and is planned for adoption in 2014, to take effect in 2016 (to allow for the transition).

In addition to the specific federal statutes described above, common law causes of action provide private remedies where sensitive information is improperly disclosed. Three common law privacy causes of action that can be brought in the wake of improper disclosure of private information include the torts of intrusion upon seclusion; public disclosure of private facts; and misappropriation of personality. Generally they entail the following:

1. intrusion upon seclusion is a tort where a given intentional intrusion (in circumstances where there is a reasonable expectation of privacy) would be highly offensive to a reasonable person, but does not include conduct that is simply offensive, insensitive or intrusive in the normal sense;

2. public disclosure of private facts is a tort which occurs when private personal information (such as health information, etc.) is "published" in a manner that would be highly offensive to a reasonable person. This tort results in liability for the owner of the database in which the information is stored and for the publisher. California recently expanded this tort in *Ignat v. Yum! Brands, Inc*., 214 Cal.App.4th 808, 154 Cal.Rptr.3d 275 (2013) (did not involve social media evidence); and

3. misappropriation is a tort where someone else's name or personality is used for gain without consent. In *Roberts v. Careflite,* 2012 WL 4662962 (Tex. Ct. App. 2012), Roberts, a paramedic, had commented on Facebook that she had wanted to slap a patient who needed restraining. The post was communicated to a company compliance officer who gave Roberts a calm warning. Rather than take heed, Roberts again let her anger show in another post and was soon thereafter fired. She challenged the firing by asserting two invasion of privacy torts – public disclosure of private facts and intrusion upon her seclusion. She lost on summary judgment. In *R.S. v. Minnewaska Area Sch. Dist*. No. 2149, 894 F.Supp.2d 1128 (D.Minn. 2012), the court allowed a claim for invasion of privacy claim to go forward but dismissed a claim for intentional infliction of emotional distress. In *Lawlor v. North American Corp*., 983 N.E.2d 414 (Ill. 2012), the Illinois Supreme Court affirmed a lower court holding that defendant was vicariously liable for "invasion upon seclusion" when its hired investigators obtained her phone records by pretending to be her, i.e., "pretexting."

4. Social Media and the Stored Communications Act Congress passed the SCA because "the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address." See *Quon v. Arch Wireless Operating Co., Inc*., 529 F.3d 892, 900 (9th Cir. 2008). The SCA governs the circumstances under which electronic data service and storage providers may

disclose customers' data. It provides that whoever (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section. 18 U.S.C. § 2701.

5. The SCA precludes certain "providers" of communication services from divulging private communications to certain entities and individuals. The SCA defines an electronic communications service provider ("ECS") as "any service that provides the user thereof the ability to send or receive wire or electronic communication." 18 USC §2510[15]. An ECS provider is only prohibited from divulging "the contents of a communication while in electronic storage by that service." "Electronic storage" is defined as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" or alternatively "any storage of such communication by an [ECS] for purposes of backup protection of such communication."

6 The SCA defines a remote computing service provider ("RCS") as "the provision to the public of computer storage or processing services by means of an electronic communications system." RCS providers are prohibited from "knowingly divulg[ing] to any person or entity the contents of any communication which is carried or maintained on that service." Standing under SCA to prevent production. Ordinarily a party has no standing to move to quash a subpoena issued to a nonparty unless the objecting party claims some personal right or privilege with regard to the information sought. Under the SCA, the party has a personal right with regard to stored emails and other electronically stored information. See *Crispin v. Christian Audigier*, 717 F.Supp.2d 965, 974 (C.D. Cal. 2010) (discovery sought from Facebook, MySpace, and others); *Chasten v. Franklin*,

2010 WL 4065606, at *1 (N.D. Cal. 2010) (Yahoo! email account*); J.T. Shannon Lumber Co. v. Gilco Lumber, Inc.*, 2008 WL 3833216, at *1 (N.D.Miss. Aug. 14, 2008) (emails).

Application of the SCA by the courts.

The majority of courts hold that internet service providers and social media websites are ECS providers bound by the SCA to not produce postings and emails of their subscribers/ registrants in response to a civil subpoena. Instead, the party seeking discovery must use Rule 34 requests to the opposing party to obtain the postings. To obtain social media postings a non-party witness one the best practice is to serve a subpoena on the non-party, not the social media ISP.

Constitutional Protections. You should prepare yourself for arguments for privacy protection under the First, Fourth, Fifth, and Ninth Amendments, which will be made to try to block your discovery efforts.

Social Media Website Terms of Service.

Always check the Terms of Service for the social media website as they may have an impact on your approach to obtaining the information or even the target of your discovery demands. For example, Twitter's Terms of Service clearly state that a Twitter user provides Twitter a license to distribute to anyone at any time whatever the user tweets. In People v. Harris, a criminal prosecution of an Occupy Wall Street protestor, the prosecutor served a subpoena on Twitter. The court denied defendant's motion to quash (36 Misc.3d 613, 945 N.Y.S.2d 505 (2012)) because he lacked standing. Twitter then moved to quash; the court again denied (36 Misc.3d 868, 949 N.Y.S.2d 590 (2012)) and held that the defendant had no proprietary interest or expectation of privacy in his tweets and that by submitting tweets he had granted Twitter an unlimited license to use and distribute the tweets. Similar results have occurred in civil cases regarding the Terms of Service for other social media. See, e.g., Tompkins v. Detroit Metro. Airport, 2012 WL 179320,

at *2 (E.D.Mich. Jan. 18, 2012); EEOC v. Simply Storage Mgmt., LLC, 270 F.R.D. 430, 434 (S.D. Ind. 2010); Beye v. Horizon Blue Cross Blue Shield of New Jersey, 2:06-cv-05337 (D. N.J. 2007); see also Patterson v. Turner Constr. Co., 931 N.Y.S.2d 311, 312 (N.Y.App.Div. 2011); Romano v. Educational & Institutional Coop Servs., Inc., 907 N.Y.S.2d 650 (N.Y.App.Div. Sept. 21, 2010). Generally, attorneys may access and review public portions of a party's or nonparty's social networking sites without ethical implications. However, trying to get past privacy protections or misrepresenting any facts to access social media information will land you in hot water.

Methods/Techniques to Obtain Social Media Discovery

At the beginning of a case, be sure to notify the opposing party or counsel to preserve the party's social media information. Also tell your own client to preserve all social media accounts. All parties are obligated to preserve evidence that they reasonably should know is relevant to the lawsuit. Zubulake v. Warburg, 220 F.R.D. 212 (S.D. N.Y. 2003). If a party closes a social media account, the information may be lost forever. If that deleted information was potentially relevant, the consequences for the deleting party are not good. In Gatto v. United Air Lines, Ltd., 2013 WL 1285285 (D. N.J. March 25, 2013), the plaintiff deleted his Facebook account after the defendant sought it. The court punished the plaintiff with an adverse instruction to the jury. The usual methods of discovery can be used – informal requests, written interrogatories and document production requests to parties, and subpoenas to non-parties. You will find sample written interrogatories and document production requests at Appendix A. A special problem occurs with regard to information posted on the internet by persons who do not identify themselves (usually on purpose).

Discovery requests/subpoenas for social media evidence should be drawn narrowly. 16 Tie your discovery requests to information already in hand that shows that the request is seeking

evidence that likely exists and, therefore, not a fishing expedition. Courts normally hold that the posted social media information is discoverable because any privilege or privacy protection was waived by sharing the content. However, most courts will require some showing of relevance and not allow discovery of all or a broad scope of material. Usually, the discovering party must show information that at least suggests the existence of relevant information at the social media account before the court will order production or access to the information.

ISPs are not responsible for defamatory or derogatory postings under the Communications Decency Act. 47 U.S.C. § 230(c)(1) (2008). You have to go after the poster of the comments

Subpoena Information:

Subpoenas for T-Mobile:
Custodian of Records
T-Mobile Subpoena Compliance
4 Sylvan Way
Parsippany NJ 07054
(f) 973.292.8697
973.292.8911
Subpoenas for Verizon:
Custodian of Records
Verizon Cellco Partnership, d/b/a Verizon Wireless
Subpoena Compliance
180 Washington Valley Road
Bedminster, NJ 07921
Fax (888) 667-0028
Voice (800) 451-5242

Subpoenas for AT&T records (including what used to be Cingular):
Custodian of Records
AT&T Subpoena Compliance
P.O. Box 24679
West Palm Beach, FL 33416
Fax (888) 938-4715
Voice (800) 635-6840

Subpoenas for Sprint records (and what used to be Nextel):
Custodian of Records
Sprint Corporate Security
6480 Sprint Parkway

Overland Park, KS 66251
Fax (816) 600-3111
Voice (800) 877-7330

Subpoenas for Cricket records:
Custodian of Records
Attention: Subpoena Compliance
Cricket Communications/Leap Wireless
5887 Copley Drive, San Diego, CA 92111
San Diego, California 92121
Fax: (858) 882-9237
Or scan and email to: compliance@cricketcommunications.com
Voice (858) 882-9301

Subpoenas for Cellular South:

Mr. Robert A. Geoghegan, Esq.
Director of Subpoena Compliance & Coordinator of Corporate Security
Telapex, Inc.
1018 Highland Colony Parkway, Suite 500
Ridgeland, MS 39157
Phone: 691-355-1522
Fax: 601-487-7517

G. Facebook's Archive Feature

Facebook has silently added the ability for users to archive their Stories, just like Instagram did late last year. Facebook still isn't giving up on Stories on its platform, even though its Instagram equivalent is much more popular. And now, a feature it announced back in May is finally here – being rolled out to more users. The feature in question is Facebook Stories archiving. Any brands who like to use Facebook Stories should know this is a pretty useful feature.

Why is it useful? Well, for one, Stories are ephemeral content by design, which means they will disappear unless you save them somehow. Therefore, if saved, Stories can be re-used and re-posted. Do you want to use something after 24 hours? Here's the way to do it. If you don't, it will simply disappear after 24 hours. This may encourage more brands to work with Stories, as content will go further if one can re-use it.

The archive icon now appears at the top of your Facebook Stories bar, but you can turn it off if you want all your content to be ephemeral. Using the archive, you can sift through the Stories you'd like to use again or keep for reference. The only missing right now is a highlights section used to showcase Stories posts. Instagram already has the feature.

H. Using Friending/Following to Obtain Info[18]

The American Bar Association's Model Rules of Professional Conduct ("Model Rules") provide a framework in which to analyze the potential ethical issues that arise in this situation. Lawyers should take a conservative approach to accessing social media sites through informal discovery, limiting their searches to passive review of publicly accessible pages and requesting further access only when dealing with pages maintained by unrepresented persons.

A lawyer wishing to obtain evidence contained on an otherwise private social media site may ethically seek such information by utilizing formal discovery mechanisms. Several courts have allowed formal discovery of information contained on social networking sites and find the practice is entirely ethical so long as the lawyer ensures that his or her discovery request is made in good faith and comports with the appropriate laws. The Federal Rules of Civil Procedure, the equivalent state rules, and other laws applicable to electronically stored information govern the discoverabilityof social media. However, added layers of complexity accompany any formal request for discovery of information contained on social media sites, given the notions of privacy associated with the sites and the existence of multiple entities with access to and control of the information contained thereon.

[18] Taken from Allison Clemency, Comment "Friending, Following and Digging Up Evidentiary Dirt: The Ethical Implications of Investigating Information on Social Media Websites, 43 Ariz.St.L.J. (Fall 2011) and Jeffrey Boyd & John Browning, "Ethics of Social Media Use." 32nd Annual Advanced Civil Appellate Practice, State Bar of Texas (Sept. 6-7, 2018).

Because of the Stored Communications Act, parties may not be able to obtain information directly from the service providers, e.g., Facebook, MySpace, Twitter, without also obtaining the account owner's consent. Ultimately, formal discovery is an ethical channel for obtaining access to social media profiles, but the procedural and technical structure in which to conduct formal discovery of social media is still in a somewhat fledgling state.

Many practitioners and courts still favor informal discovery because of its efficiency, ability to canvas a broad range of information, and cost effectiveness.

Although courts have not yet addressed the ethics of informal discovery of social media sites, several city and state ethics committees have recently considered hypothetical scenarios and analyzed the ethical problems associated with informal discovery of information on social media sites. The opinions generally reason that informal discovery of social media sites presents two primary ethical problems: (1) use of deceptive investigatory tactics, a practice commonly referred to as “pretexting,” and (2) engagement in prohibited communications.

Changes to Model Rule of Professional Conduct 1.1 have ushered in new expectations of digital competence as attorneys are now held to a higher standard of being conversant in the benefits and rights of technology. Ethics opinions across the country are addressing issues like the limits of advising clients about what to “take down” from their Facebook pages, contact with witnesses via social media, and even researching the online profiles of prospective jurors.

While there generally is no ethical prohibition against viewing the publicly available portion of an individual’s social networking profile, may an attorney (or someone working for that attorney) try to “friend” someone in order to gain access to the privacy-restricted portions of that profile? Ethics opinions from the Philadelphia Bar Association (March 2009), the New York City Bar (September 2010), the New York State Bar (September 2010), the Oregon Bar (February

2013) the New Hampshire Bar (June 2013), and others have made it clear that the rules of professional conduct against engaging in deceptive conduct or misrepresentations to third parties extend to cyberspace as well.[2] Not surprisingly, lawyers have found themselves in ethical hot water for engaging in such "false friending."

In addition to using social networking sites for gathering information, the ethical duty to preserve information is another concern in the age of Facebook and Twitter. While no lawyer wants to discover embarrassing photos or comments on a client's Facebook page that might undermine the case, Rule 3.4 prohibits an attorney from unlawfully altering or destroying evidence or assisting others in doing so.

Another area in which lawyers' use of social media can raise ethical questions is jury selection. Should lawyers probe the online selves of prospective jurors? The Missouri Supreme Court actually has imposed an affirmative duty on lawyers to conduct certain Internet background searches of potential jurors (specifically that juror's litigation history), if the lawyer plans to argue juror bias related to his/her litigation history.[6] Multiple ethics opinions, including an ABA Formal Opinion, have addressed the issue of "Facebooking the jury." In the first of these, the New York County Lawyer's Association Committee on Professional Ethics held in 2011 that "passive monitoring of jurors, such as viewing a publicly available blog or Facebook page" is permissible so long as lawyers have no direct or indirect contact with jurors during trial. Subsequent opinions from the New York City Bar Association (2012) and the Oregon Bar (2013) agreed with this, while sounding a cautionary note to lawyers that even accessing a prospective juror's Twitter profile or LinkedIn profile could cause the juror to learn of the lawyer's viewing or attempted viewing. Such contact, according to both ethics committees, "might constitute a prohibited communication even if inadvertent or unintended." In other words, as with other aspect in which lawyers might use

social media, ignorance or lack of familiarity will not be an excuse in committing an ethical violation.[7]

In April 2014, the ABA weighed in on this issue with Formal Opinion 466. Like the earlier state ethics opinions, it too concluded that a lawyer is ethically permitted to review a juror's social networking presence, provided that no contact is made with the juror. However, the ABA opinion diverges from its state counterparts in its consideration of whether auto alerts by sites such as LinkedIn or Twitter to the juror/user that her profile is being viewed would constitute impermissible contacts. Formal Opinion 466 doesn't see this as a problem, stating that "The fact that a juror or potential juror may become aware that a lawyer is reviewing his Internet presence when a network setting notifies the juror of such does not constitute a communication from the lawyer in violation of Rule 3.5(b)."

Lawyers need to be mindful that they face heightened public and ethical scrutiny when they express opinions online or on social media platforms, particularly in light of today's more polarized climate. Lawyers also need to remember not only the speed with which our wired world reacts and the ubiquitous nature of social media, but also the fact that the same ethical rules that apply to every other form of communication similarly apply to social networking platforms. If you wouldn't put it in a letter or publish it in a newspaper, don't post it on Facebook or tweet about it.

I. What Can Be Done if the Account Has Been Closed?

If you delete your account, there's a good chance that not everything disappears as quickly as you might want.

"We store data for as long as it is necessary to provide products and services to you and others," Facebook's data policy states.

According to Facebook's website, it could take 90 days to delete all of the things a user has posted, including pictures, status updates and other data stored in its backup system. However, once an account is deleted, this information will no longer be available for other users to view. Information others have shared about you will not be deleted, however, as it is not part of your account.

On Instagram, you can't really delete your account at all. However, you can deactivate it. According to Instagram's terms of service, if you choose to deactivate your account your photos, comments, likes, friendships and other data won't be available through your account. However that material and data may still exist and appear within the service. So for example, your profile and images could no longer be viewed from your page, but if someone reposted a picture that you originally published, it would still exist on the platform.

Your posts can end up anywhere

With all the social media faux pas these days, it might seem obvious that everything you do online can end up just about anywhere, regardless of how private you intended it to be.

While privacy settings on sites like Instagram, Facebook or Twitter may limit the reach of your original post, there's no way to really rein in how others on the social site may use your publicly shared content.

For example, if you post a picture to your profile and have privacy settings set to only share with your friends, there's still the chance that a friend could always take that post and share it elsewhere. So while Facebook is using its license to your content to distribute as you intended doesn't mean everyone else will respect that.

"Even though you are aware you are granting certain rights to Facebook, Twitter or Pinterest or Vine or whoever, you may not necessarily [be] granting those rights downstream to

the other users of the site," Frazer said. "You still need to be vigilant to see how other people are using your content. Just because I granted a license to Facebook, doesn't mean that I granted it to some kid I knew in high school to take my photo and put it on a thousand T-shirts," he added.

"Think about the consequences of your posting because it really could end up anywhere."

Obtaining Deleted Data[19]

Look in the Recycle Bin

Just double-click on the Recycle Bin or trashcan and you can see everything that's inside. Did you find what you thought you had deleted? Simply drag it back onto your desktop, and you are good to go. If it's not in your trashcan, then there are a number of other things you can try to recover a deleted file. Hopefully you have been doing backups. If so, you can recover an earlier version of your file through the recovery service in backup. It might be a day old, but it’s better to lose a day than lose everything.

How to Recover Deleted Files Using File History

If you are not doing backups, hopefully you have turned on File History Backup. If you're running Windows* 10, select the Start button, select Settings > Update & security > Backup > Add a drive, and then choose an external drive or network location for your backups.

To Restore That Important Missing File or Folder:

Type Restore files in the search box on the taskbar, and then select Restore your files with File History.

Look for the file you need, then use the arrows to see all its versions.

[19] Taken from Cadie Thompson, “What you really sign up for when you social media”

When you find the version you want, select Restore to save it in its original location. To save it in a different place, press and hold (or right-click) Restore, select Restore to, and then choose a new location.

No Backups?

If you don't have any backups and your file is not in the trash, you might want to try one of the many file recovery programs out there, either a free one or a commercial app like Piriform Recuva*, or Stellar Data Recovery*.

Another option is Disk Drill*, a recovery tool originally designed for Mac* and now available for Windows. It offers help with partition loss, hard drive reformatting, failed boot-ups, accidental deletions, and more.

Another possibility to consider: Have you emailed the file to anyone? Have you saved a copy on a cloud-based service like DropBox*, iCloud*, or SkyDrive*? If so, you might be able to grab a copy from there. Again, even if you lose the most recent changes, it is better than nothing.

However you approach it, there are lots of options to explore after you realize you have accidentally deleted a photo, document, spreadsheet, report, or other file. And get those backups going too, so next time you need to find a deleted file, you have more options.

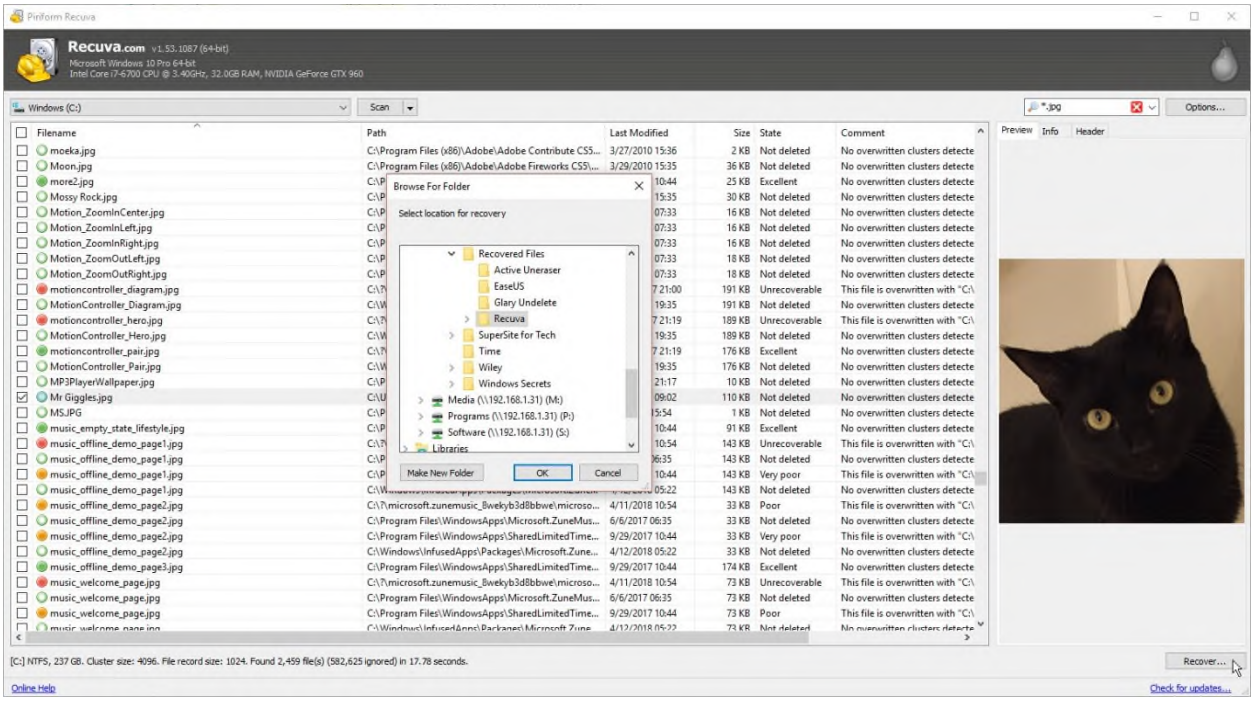
If the deleted file is one you've synced or stored in the cloud, you can typically undelete it as long as your cloud provider offers some type of recycle bin or trash folder. Popular services such as OneDrive, iCloud, Google Drive, Box and Dropbox all give you ways to resuscitate deleted files, but even here you need to act quickly. These services typically grant you up to 30 days to recover a file. After the clock has run out, those deleted files are purged and removed from their file servers.

If you want to revive a deleted file, an old adage applies: the sooner the better. When you delete a file in Windows, that file first bounces to the Recycle Bin. You can bypass the bin by turning it off through its Properties window or holding down the Shift key when you delete a file. Even if you use the Recycle Bin, at some point it will get too full and start kicking out older files. In other cases, you may decide to empty your bin to free up disk space. And that's when the adventure begins.

When you permanently delete a file in Windows, it's not physically removed from the disk. Rather, the file's locations are marked as available by the file-allocation table. As such, the file still lives -- unless and until you start storing new files that end up overwriting the deleted one. A file is stored in separate clusters of space on your hard drive. Some of a file's clusters may become overwritten with new data while other clusters remain intact. In those cases, you may be able to recover parts of a file but not necessarily the whole thing.

Of course, going forward, you should always back up important documents and other files on a regular basis. In that case, you can retain deleted files on your backup source for as long as you want. But as far as repairing the damage that's been done, these three apps do a good job recovering a deleted file from your PC.

Recuva



Recuva handles all types of deleted files, from documents to photos to videos to emails, and it can grab them from your hard drive, a removable drive or a USB stick. The program kicks off with a wizard that asks for the type and location of the file you want to restore. You can narrow the search this way or opt to look for all files in all locations. Recuva scans your drive to display a list of deleted files. You'll see each file's name, location, size, its chances for recovery and a comment with more details. After you select the file you want to restore, Recuva asks where to put it. Tip: If you hope to restore additional files from the same drive, save the recovered file in a different location to avoid overwriting any more clusters.

To cut to the chase, switch to advanced mode instead of using the wizard. There, you can select a location, pick a file type and enter a specific name or wildcard combination to limit the search. If your file doesn't pop up, try a deep scan that digs for deleted files by analyzing each

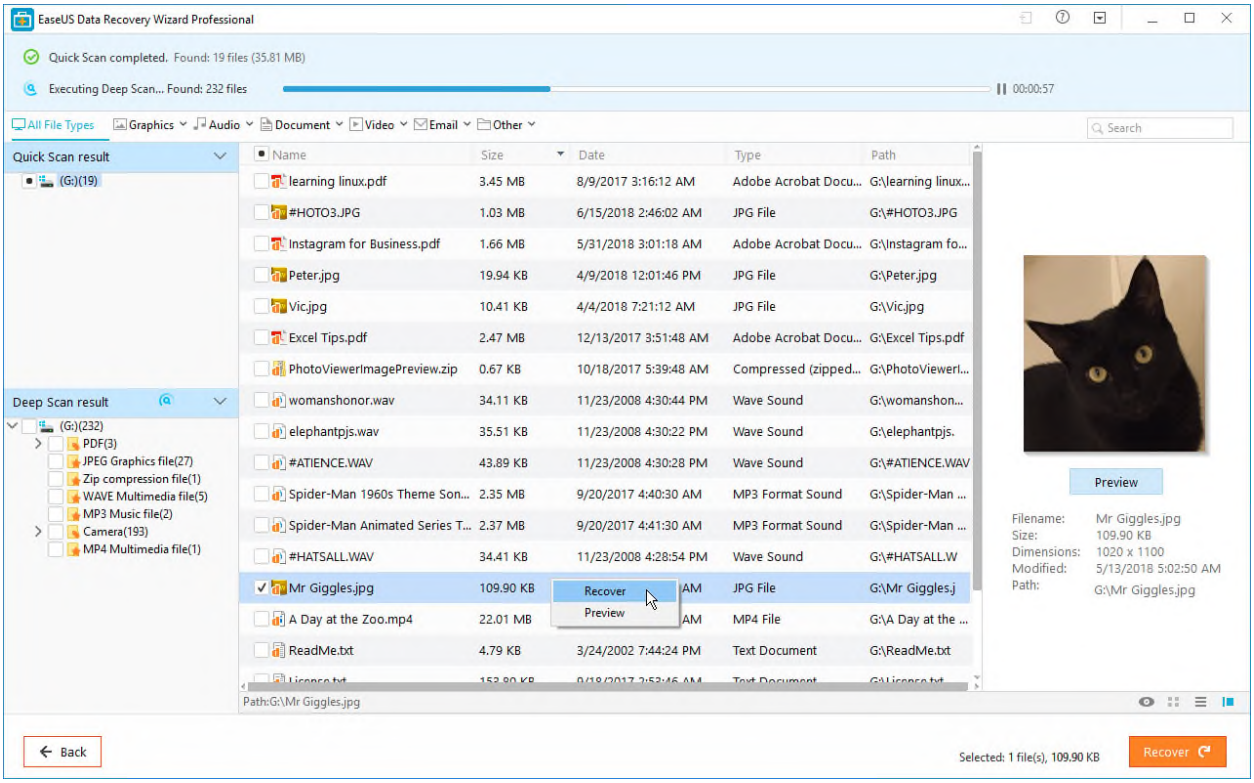
sector on the disk. But be prepared to wait: The deep scan took more than two hours to complete on my 2TB hard drive with 240GB of data.

I used Recuva to bring back deleted files from a hard drive, USB stick and SD card. I was able to successfully restore all files that were rated as "excellent" for recovery state. Files that were categorized as "poor" or "very poor" were either not recoverable at all or only partially recoverable, while those ranked as "unrecoverable" sadly never stood a chance. So we're clear, a rating of excellent describes a freshly deleted file with no clusters overwritten. Poor or very poor refers to a file with few of its clusters intact. And unrecoverable points to an older deleted file with all of its clusters overwritten.

The basic version of Recuva is free; a $19.95 Pro edition works with virtual hard drives, provides automatic updates and delivers free premium support. There's also a portable version you can run off a USB drive to avoid installing the software on your hard drive.

All told, Recuva works smoothly and efficiently. The wizard is simple to use, but be warned that it dumps so many deleted files into your lap that you might have a hard time locating the one you want. Instead, consider jumping straight to advanced mode, where you can exercise more control over what you see.

EaseUS Data Recovery



EaseUS Data Recovery, available for Windows and macOS, offers a variety of features and is available as both a free and paid product. You can restore files from internal and external hard drives, USB sticks, RAID configurations, SD cards, MP3 players, cameras, camcorders and more. EaseUS Data Recovery Wizard Free starts off by showing all of your hard drive partitions. Select a partition to scan for deleted files or choose a specific folder. Run a scan to begin the search; the program then displays a list of locations on your drive where it uncovered deleted files, arranged by folder or file type. Select a specific folder to see the files inside. You can narrow the list by opting to view only specific file types, such as graphics, audio, video, documents and emails. You can also search for files by name and wildcard symbols, such as an asterisk.

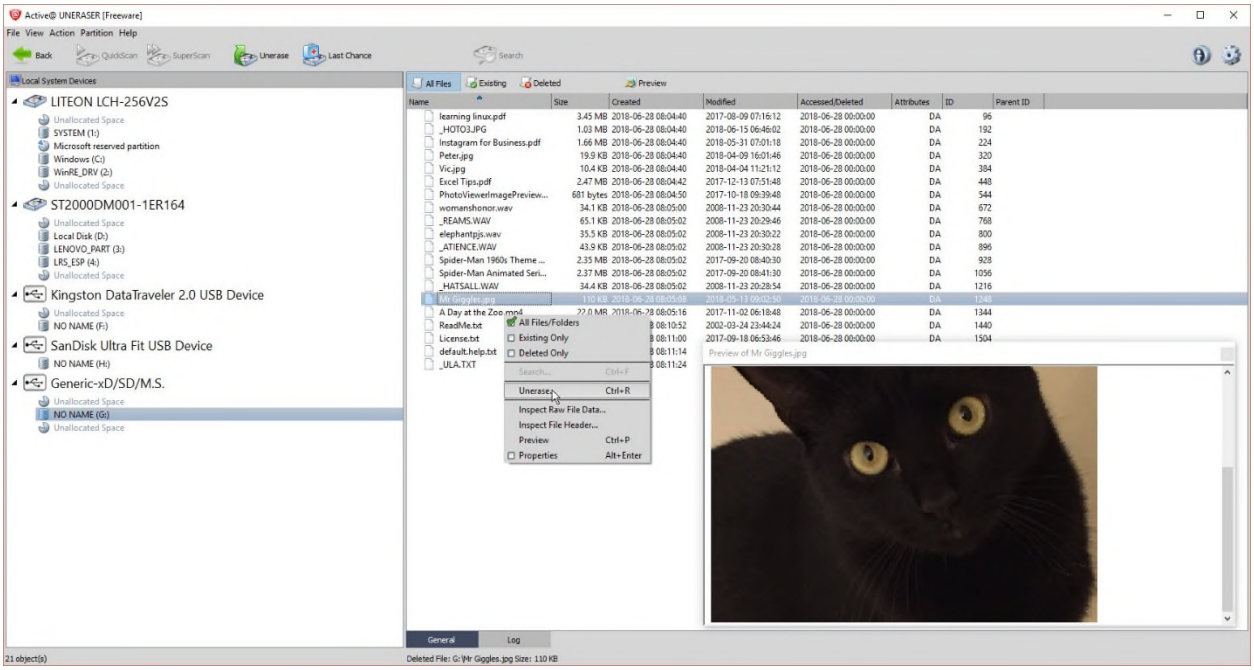
By default, the software shows you key details for each file, including the name, size, date, type and path. The program doesn't indicate the recovery state of deleted files, but you can preview a deleted file to see if it's intact.

While you're hunting for your deleted file, EaseUS conducts a deep scan to seek out files that may not have been uncovered in the first scan. That process isn't exactly speedy: On my drive, the deep scan took more than five hours to finish. The good news is that you can view the initial results of the deep scan while it's running. After the scan, check the file or files you wish to restore, and the software will ask for a recovery location. Remember to choose a drive other than the source if you want to undelete additional files from the same spot. After the program has revived your chosen files, it opens the recovery folder so you can check out the results.

With EaseUS Data Recovery, I was able to restore all recently deleted files and mostly recover older deleted files as well as those on hidden or lost partitions. The Deep Scan was especially effective at restoring files that I thought I'd lost forever.

The free version of EaseUS Data Recovery poses one major obstacle: You can recover only up to 500MB of files at a time. By sharing a link to the application on Facebook, Twitter or Google+, though, you can increase that limit to 2GB. If you need to restore a larger file, however, you'll have to pony up for one of the paid editions. Priced at $69.95, Data Recovery Wizard Pro can undelete any size file. For $99.90, Data Recovery Wizard Pro+WinPE offers a bootable media option in case your hard drive ever goes belly up. And if you recover files and hard drives for a living, paying $299 per year (or $499 for a lifetime subscription) scores you the Data Recovery Wizard Technician version. All three paid editions grant you free lifetime upgrades and free technical support.

Active Uneraser



Active Uneraser has several tricks up its sleeve. You can start with the free version, which is plenty powerful in its own right. You can recover files from your hard drive, external drives, USB sticks and SD cards. You can undelete damaged partitions. The software also supports RAID configurations. Active Uneraser kicks off by displaying your hard drive partitions, even ones that have been deleted. Select a specific partition and the program provides plenty of details, such as the total capacity, used space, free space, file system and condition.

After you scan a partition, Active Undelete displays all the files contained within. You can switch the view among all files, existing files and deleted files. The files are arranged by folder to allow for quick and easy searching. You can always search for a deleted file by name and/or wildcards. If the initial QuickScan comes up empty, try the QuickScan Plus feature to detect more lost or damaged files or folders. Next in line, a SuperScan digs deeper but takes longer to find

deleted files. If those methods don't do the trick, turn to the Last Chance option, which tries to uncover files based on their signatures, which are used to identify their format.

You can preview certain types of deleted files, but the software limits your view to files 10MB or smaller. To bring back a file, select it and run the Unerase command. Active Undelete asks for a location to restore the file and then opens File Explorer or Windows Explorer to display the recovery folder.

I was able to restore all recently deleted files from a hard drive, USB stick and SD card. SuperScan took four hours to run while Last Chance ran for six hours; both were able to find and revive older files as well.

The free version comes with one small restriction: You can recover just one file at a time. To get past this limitation and access other features, upgrade to one of the two paid versions. For $39.99, the Professional edition adds a bootable Windows Recovery environment in case your PC can't boot up. For $49.99, the Ultimate edition kicks in a Linux recovery CD and the ability to repair or restore damaged RAID configurations.

The best recovery program

Recuva, EaseUS Data Recovery and Active Uneraser all work smoothly and effectively to recover your deleted files. If you're seeking a free tool, try Recuva. It works well and isn't saddled with the limitations imposed by the free flavors of the other two programs. If you don't mind spending a few bucks, check out the Professional edition of Active Uneraser, as it's reasonably priced, offers three different levels of scans, and kicks in the bootable recovery environment.

K. Processing, Review and Production Pitfalls[20]

Electronically Stored Information (ESI) must first go through the multi step eDiscovery process, whereby electronic data is sought after, obtained, secured, and/or searched with the intent of presenting it as evidence in civil or criminal litigation. The three phases of eDiscovery are: (1) relevant data is identified, preserved, and protected while using proper protocol; (2) with the use of specially designed software with advanced analytics technologies, data is analyzed and up to 50% or more of irrelevant data has the potential to be eliminated; and (3) the processing and review of smaller subsets of relevant data, and the production of a supporting chain of evidence to be presented during litigation.

The ESI Processing and Review phase is instrumental in creating a strategy for court and producing a defensible chain of evidence to support the litigation. Our advanced analytics technologies allows your team gain control of large, complex sets of data quickly and accurately. In order to authenticate ESI, electronic data must go through proper protocols, which are repeatable and defensible procedures. Courts and opposing counsel are increasingly paying closer attention to how ESI is processed during eDiscovery to ensure proper protocols are followed. "A party who produces documents for inspection shall produce them as they are kept in the usual course of business …" (Rule 34[b][i]). The committee notes expand on this: "The responding party must produce ESI either in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable."

Top 10 Mistakes to Avoid When Creating Productions:

1.Being unaware of the rules (FRCP/state/local)

[20] Taken from Gene Albert, *Top 10 Mistakes to Avoid When Creating Productions* | eDiscovery Webinar Series | Lexbe LC (October 30, 2014).

2. Neglecting to match review requests with your review approach

3. Not knowing the common file deliverables in productions

4. Missing the opportunity to use ‘Meet & Confer’ (Rule 26) to your advantage

5. Failing to Request specific file types & metadata as needed

6. No custodian tracking causing reduplication nightmares

7. Not Addressing placeholders, databases, and unusual file types

8. Negotiating incomplete discovery orders in complicated cases

9. Stepping into redaction traps

10. Decreasing privilege review accuracy by failing to apply Near dup checks

1.Being unaware of the rules (FRCP/state/local)

FRCP 34(b)

○ If No Agreement - Requires that ESI (electronic stored information) be provided in a form in which it is ordinarily maintained or a form that is reasonably usable. (E.g., native format)

○ If Specific Request, No Objection - If the requesting party specifies a different form, and the receiving party does not object, the receiving party may be bound to the requested form of production.

○ If Specific Request, With Objection - If the requesting party specifies a different form, the producing party can object and propose its own form.

Other Rules

○ Local Rules - Specific federal courts may have local rules specifying forms of production.

○ State Laws - Many states have similar rules.

2. Neglecting to match review requests with your review approach

Possible Review Application Options ○ Litigation Review Application - Designed to organize, search, code & produce large data sets. Some work best or only with some data types (e.g., TIFF with load files); some with several or many types (natives, PDFs, TIFFs). Some can load and work with native files and some require pre-processing and conversion. Applications can be workstation, firm server or internet-based.

○ Review email/files on a local computer- Some review small email data sets directly in Outlook. Other natives files may simply be reviewed on a local computer.

○ Review in PDF - Some convert everything to PDF and review on computer without a Litigation Review Application.

○ Consistent Request - Match your production request/form of production to your intended review application.

3. Not knowing the common file deliverables in productions

Native File Type

What is it? Saved as designated by the original application used to create it (e.g. a DOC or DOCX file created by Microsoft Word) Advantages ● Most accurate approximation of what custodian saw and used ● Minimal size expansion ● All metadata available Disadvantages ● Need application for all file types ● Can increase attorney review time if no paginated equivalents Notes ● Processing still needed ● Often must produce in addition to other formats ● Increased privilege issues

Near Natives

What is it? Saved as designated by the original application used to create it (e.g. a DOC or DOCX file created by Microsoft Word) Advantages Allows structured databases and specialty applications to be converted to reviewable types (e.g., Excel) Disadvantages ● Usually needs to

be converted by specialists with case subject matter expertise ● Relatively expensive Notes ● Usually 'as needed' only ● Rare/special file types may be review ed in original application without conversion

Rendered HTML

What is it? Native files converted or rendered to HTML equivalents for review Advantages ● Size expansion less than images (TIFFs) ● Retains native searchability ● Fast processing for review start Disadvantages ● May only be a rough document approximation ● Cannot be Bates/control stamped per page ● With scanned ESI can be a lot of OCR errors Notes ● Not a production format usually ● Usually must still produce as Native, PDF and/or TIFF

PDF

What is it? Natives converted to PDF from native or scanned and OCRed Advantages ● Familiar & easy to use ● Does not require review platform ● Page-level Bates stamping; Retains color ● Size expansion less than images (TIFFs) Disadvantages ● Some review platforms may not support well ● A complex format which can present corruption issues downstream in review Notes ● Different types of PDFs: -Text-Based (converted from native) -Image-only (scanned or rasterized) -Text-under-image (OCR added as text layer) -Acrobat Portfolio (must be extracted in most platforms)

TIFF & Text

What is it? Natives converted to TIFF-images, usually single-paged; or scanned Advantages ● Traditional review format (predates PDF) ● Required for some platforms ● Robust bitmapped file type (image-viewer used) Disadvantages ● Cumbersome--requires separate text files and load file to use ● Requires review platform to pull together ● Substantial file expansion from native (3-5X) ● May lose color, hidden and other data Notes ● Usually in the form of one image

and one text file per page (older text in load file) ● Document breaks and associated metadata are stored in one or more separate 'load files', which can corrupt

Blended Productions

What is it? Delivery in multiple formats as needed: Native, PDF & TIFF/text, with multiple load file formats Advantages ● Lessens format discussions/delays ● Flexible for multiple platforms ● PDFs available for easy transfer; Natives for backup and review; TIFFs for review systems that require it (if needed) ● Versions linked for easy comparison Disadvantages ● If TIFFs produced, larger hosting space required Notes ● Multiple version of load files provided for system flexibility

Load File

What is it? Structured text or database type file that references document files and associates metadata and other information, for use in Litigation Review Database Systems May Be Included ● Document and email metadata ● Document breaks (for single page TIFFs) ● Email family associations ● Map to multiple versions of files (e.g., TIFF, Text, PDF, Native) Formats in Use ● DAT (Concordance, Ringtail, Relativity) ● DII (Summation) ● LFP (iPro) ● Excel XLSX (Lexbe) Notes ● Production may include multiple load files formats ● Can be used in TIFF, PDF and Native productions ● Some systems can load multiple formats

4. Missing the opportunity to use ‘Meet & Confer’ (Rule 26) to your advantage

○ FRCP 26 ‘Meet & Confer’ Timing - Parties must meet & confer 21 days before the scheduling conference - Scheduling conference must occur within 120 days of filing (FRCP 16) ○ FRCP 26 ‘Meet & Confer’ Requirements - Discuss ESI preservation - Develop a proposed discovery plan - Submitting to the court a written report outlining the plan - Assumes ‘collaboration’ and ‘good faith’ ○ How helpful? - Can help resolve many matters, or - Can be a total waste of time

○ Before the Conference - Identify Custodians relevant to your production and your opponents - Map amount of ESI in GBs you expect to produce - Be ready to discuss any ESI that is not ‘reasonably accessible’ - Have proposed keyword searches if you plan to use them - Know what form of production you prefer and load file requirements ○ At the Conference - Have a technical representative from the client or eDiscovery vendor available if needed to discuss particularities of ESI and Production issues - Determine what Document Review Platform/Approach your opponent will use and what Form of Production they will request

○ After the Conference - Memorialize agreements in an agreed order - Document disagreements

○ Tips - Know what you are agreeing to. Scope and cost of ESI production commitments - Most cases in this area involve interpreting what the parties agreed to - Watch time commitments as ESI technical issues can delay - Native production is common but can increase time for privilege review - Metadata production format should be understood - Address databases and other unstructured or unusual data that may need to be converted to Near Native for production

5. Failing to Request specific file types & metadata as needed

File Types Requested ○ TIFFs or PDFs - Some Review Applications require a paginated version to load (TIFF/PDF) - This allows for review application independence and page level Bates stamping ○ Loadfiles - These usually should include - Many Review Applications require; good idea even if not required - File metadata (e.g., email date, time, sender, subject) - Page breaks for single paged TIFFs; email attachment associations ○ Natives - Increasingly common to request in addition to TIFF or PDF - Some Review Applications allow Natives to be input directly and convert to another format (PDF, TIFF, HTML or PNG) for review, redaction and production.

6. No custodian tracking causing deduplication nightmares

○ Custodian Tracking - Attributing specific files/ESI to custodians is increasingly requested - Custodians must be associated with incoming Natives or loadfiles - Custodian association also may be needed for chain of custody/admissibility ○ Deduplication - Emails and other files may be deduplicated as part of a review process - Exact copies of emails/other files may be deleted/filtered from review set - Deduplication is usually done only within each custodian (vertical deduplication) to retain custodian associations of duplicates - Deduplication between custodians (horizontal deduplication) may also be done, but is more complicated as custodian associations of deduped files must be retained. Also adding and removing custodians can be very complicated in a horizontal deduplication.

7. Not Addressing placeholders, databases, and unusual file types

○ Unconverted Files & Placeholders - When a production is being done in paginated form (TIFF or PDF), some files will not convert as corrupted, password protected, of unusual type, etc. - These files will be produced with a placeholder file, noting the unconverted file and allowing Bates-stamping of the placeholder. - Native versions of unconverted files can be examined as needed. ○ Databases and Other Structured/Unstructured Data; Files - Databases and similar data usually is not produced natively - Instead reports are specified and run to meet production requirements. - Intermediate versions of database reports may also be saved into Excel files and produced natively as Excel ○ Unusual Filetypes; Applications - Unusual/rare file types may be produced natively - Alternatively they may be separately examined by an expert.

8. Negotiating incomplete discovery orders in complicated cases

○ Comprehensive Discovery Orders - In large, complex, or multi-party litigation, a comprehensive discovery order may be appropriate. - Special masters may handle disputes ○ Possible Items to Cover - General Format of Production; How Email is Handled; Metadata -

Database handling - Documents in hard copy; scanning specifications - Handling of Dups - Bates numbering protocols - Search term disclosure, and procedure to handle disagreements - Procedures for Predictive Coding, if utilized - Privilege logs - Costs of Production and any cost shifting - Example complex order in Deepwater Horizon litigation: http://www.laed.uscourts.gov/OilSpill/Orders/PTO16.pdf.

9. Stepping into redactions traps

○ Redaction Issues - Privileged and sensitive information may be redacted prior to production - If Native docs are produced, the original natives should be withheld as they can't be directly redacted - Redaction is done on TIFF, other imaged, or PDF converted versions - For TIFFs, text must be re-OCRed - PDFs must have text layer re-OCRed - Natives including redacted data should be withheld - Container files (e.g., MSG, ZIP) including redacted data should be withheld

10. Decreasing privilege review accuracy by failing to apply Near dup checks

○ Near Dup Identification - A Near Duplicate identification groups documents that are similar but not exact duplicates - Near dup grouping is very helpful but processing intensive ○ Near Dup Uses - Group similar documents together (e.g., versions of same doc, email threads) to allow mass tagging to speed review - Check near dups of privileged documents to reduce potential of inadvertent release of privileged information - Quickly find similar versions of key documents during review

VI. Real World Examples, Handy How-Tos and Sample Screen Shots[21]

A. Preservation, Spoilation and Authentication Obstacles

B. Facebook, Twitter, LinkedIn and Tumblr

C. Emails (Work-Related and Personal)

[21] See Attached power point slides

D. Video Surveillance (Private and Public)

E. Computerized Versions of Contracts and Other Documents

F. Text Messages and Voicemail

G. Chats and Instant Messages

H. YouTube

I. Instagram, Pinterest and Snapchat