VI. Legal Ethics and ESI

Sara Anne Hook, M.B.A., J.D.

A. Duties Owed to Clients, Opposing Counsel and the Courts

[N.B. All references to the Indiana Rules of Professional Conduct are taken from Indiana Rules of Court, **Rules of Professional Conduct,** *Including Amendments made through May 17, 2016*, http://www.in.gov/judiciary/rules/prof_conduct/prof_conduct.pdf, accessed 10/16/17; All references to the ABA Model Rules are taking from ABA Model Rules of Professional Conduct, http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/model_rules_of_professional_conduct_table_of_contents.html, accessed 10/16/17.]

A number of duties are owed to clients, opposing counsel and the courts. For lawyers in Indiana, one of the best places to start is the Indiana Rules of Professional Conduct. There are so many rules that apply in an electronic discovery process, whether the evidence being requested is traditional documents, digital materials or evidence generated through newer forms of technology, such as social media services, mobile messaging services and devices (fitness trackers, cell phones, Internet of Things) that are getting smaller and more powerful every day. Many sections of the Indiana Rules of Professional Conduct help lawyers to aspire to the highest standards of professionalism in how they conduct themselves and how they treat other lawyers, judges, parties, witnesses and others who may be part of the judicial process, irrespective of what kinds and formats of electronically stored information (ESI) are being requested as potentially relevant evidence and from what sources (opposing parties, third parties, etc.) For example:

Rule 3.1. Meritorious Claims and Contentions

A lawyer shall not bring or defend a proceeding, or assert or controvert an issue therein, unless there is a basis in law and fact for doing so that is not frivolous, which includes a good faith argument for an extension, modification or reversal of existing law. A lawyer for the defendant in a criminal proceeding, or the respondent in a proceeding that could result in incarceration, may nevertheless so defend the proceeding as to require that every element of the case be established.

Rule 3.2. Expediting Litigation

A lawyer shall make reasonable efforts to expedite litigation consistent with the interests of the client.

Rule 3.3. Candor Toward the Tribunal

(a) A lawyer shall not knowingly:

(1) make a false statement of fact or law to a tribunal or fail to correct a false statement of material fact or law previously made to the tribunal by the lawyer;

(2) fail to disclose to the tribunal legal authority in the controlling jurisdiction known to the lawyer to be directly adverse to the position of the client and not disclosed by opposing counsel; or

(3) offer evidence that the lawyer knows to be false. If a lawyer, the lawyer's client, or a witness called by the lawyer, has offered material evidence and the lawyer comes to know of its falsity, the lawyer shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal. A lawyer may refuse to offer evidence, other than the testimony of a defendant in a criminal matter, that the lawyer reasonably believes is false.

(b) A lawyer who represents a client in an adjudicative proceeding and who knows that a person intends to engage, is engaging or has engaged in criminal or fraudulent conduct related to the proceeding shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal.

(c) The duties stated in paragraphs (a) and (b) continue to the conclusion of the proceeding, and apply even if compliance requires disclosure of information otherwise protected by Rule 1.6.

(d) In an ex parte proceeding, a lawyer shall inform the tribunal of all material facts known to the lawyer which will enable the tribunal to make an informed decision, whether or not the facts are adverse.

Rule 3.4. Fairness to Opposing Party and Counsel

A lawyer shall not:

(a) unlawfully obstruct another party's access to evidence or unlawfully alter, destroy or conceal a document or other material having potential evidentiary value. A lawyer shall not counsel or assist another person to do any such act;

(b) falsify evidence, counsel or assist a witness to testify falsely, or offer an inducement to a witness that is prohibited by law;

(c) knowingly disobey an obligation under the rules of a tribunal except for an open refusal based on an assertion that no valid obligation exists;

(d) in pretrial procedure, make a frivolous discovery request or fail to make reasonably diligent effort to comply with a legally proper discovery request by an opposing party;

(e) in trial, allude to any matter that the lawyer does not reasonably believe is relevant or that will not be supported by admissible evidence, assert personal knowledge of facts in issue except when testifying as a witness, or state a personal opinion as to the justness of a cause, the credibility of a witness, the culpability of a civil litigant or the guilt or innocence of an accused; or

(f) request a person other than a client to refrain from voluntarily giving relevant information to another party unless:

(1) the person is a relative or an employee or other agent of a client; and

(2) the lawyer reasonably believes that the person's interests will not be adversely affected by refraining from giving such information.

Rule 4.1. Truthfulness in Statements to Others

In the course of representing a client a lawyer shall not knowingly:

(a) make a false statement of material fact or law to a third person; or

(b) fail to disclose a material fact to a third person when disclosure is necessary to avoid assisting a criminal or fraudulent act by a client, unless disclosure is prohibited by Rule 1.6.

Rule 4.2. Communication with Person Represented by Counsel

In representing a client, a lawyer shall not communicate about the subject of the representation with a person the lawyer knows to be represented by another lawyer in the matter, unless the lawyer has the consent of the other lawyer or is authorized by law or a court order.

Rule 4.3. Dealing with Unrepresented Persons

In dealing on behalf of a client with a person who is not represented by counsel, a lawyer shall not state or imply that the lawyer is disinterested. When the lawyer knows or reasonably should know that the unrepresented person misunderstands the lawyer's role in the matter, the lawyer shall make reasonable efforts to correct the misunderstanding. The lawyer shall not give legal advice to an unrepresented person, other than the advice to secure counsel, if the lawyer knows or reasonably should know that the interests of such person are or have a reasonable possibility of being in conflict with the interests of the client.

Rule 4.4. Respect for Rights of Third Persons

(a) In representing a client, a lawyer shall not use means that have no substantial purpose other than to embarrass, delay, or burden a third person, or use methods of obtaining evidence that violate the legal rights of such a person.
(b) A lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender.

Because of the nature of electronically stored information (ESI), including the sheer volume of it, the number of places where it might be located and the risks of waiving the attorney-client privilege, ethical duties related to competence (especially with technology) and confidentiality are paramount. Technology has brought many improvements to the practice of law, as well as in society as a whole, and is often considered by commentators to be the great equalizer in law practice because it allows solo practitioners and small firms to compete against larger firms and provides an opportunity to realize real efficiencies in the delivery of legal services. However, that same technology can pose substantial risks, particularly with respect to confidentiality. The author teaches a full- semester course on cyber-security, with special emphasis on security in law firms, as well as a full-semester course on electronic discovery, an important subset within legal technology that presents a number of concerns with client confidentiality and the waiver of attorney-client and attorney work-product privilege. In thinking about data security in law firms, one of the first principles to keep in mind is embodied in Rule 1.1 Competence, particularly Comment 6 (Indiana Rules of Professional Conduct):

Rule 1.1. Competence

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

Maintaining Competence

[6] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

Many commentators asserted that the phrase "and its practice" included the intentional, appropriate and careful use of technology. This view was manifested in the revisions to the ABA Model Rules of Professional Conduct as part of the Ethics 20/20 Project. For example, Comment 8 to ABA Model Rule 1.1, now approved as Comment 6 in the Indiana Rules of Professional Conduct, states that:

Maintaining Competence

[8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

[*See* Sharon D. Nelson & John W. Simek, *Competence in E-Discovery*. Sensei Enterprises, Inc., 2016, https://senseient.com/articles/competence-e-discovery/, accessed 10/16/17.]

Because one of the main risks of using technology is the threat to client confidentiality, it is worth reviewing the major rule and comments that relate to this. From the Indiana Rules of Professional Conduct, here is Rule 1.6(a) and Comments 16 and 17.

Rule 1.6. Confidentiality of Information

(a) A lawyer shall not reveal information relating to representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

Acting Competently to Preserve Confidentiality

[16] A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3.

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

However, Comments 18 and 19 to the ABA Model Rules of Professional Conduct, Rule 1.6 provide more detailed guidance.

Acting Competently to Preserve Confidentiality

[18] Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4].

[19] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

It is important to note that there are rules related to the confidentiality and other duties owed to both former and prospective clients.

In December 2015, the Federal Rules of Civil Procedure were revised again, with particular attention paid to proportionality and the opportunity for sanctions. However, FRCP is interesting in that it requires everyone, not just lawyers, to cooperate in the litigation process:

> **Rule 1:** Requires *parties*, as well as courts, to construe, administer, and employ the Rules in a manner "to secure the just, speedy, and inexpensive determination of every action and proceeding." The Advisory Committee on Rules of Civil Procedure ("Committee") notes that: "Effective advocacy is consistent with — and indeed depends upon — cooperative and proportional use of procedure." (Randy Wu, *Summary of December 2015 Amendments to the Federal Rules of Civil Procedure*. Orrick, December 7, 2015, https://www.orrick.com/Events-and-Publications/Pages/Summary-of-December-2015-Amendments-to-the-Federal-Rules-of-Civil-Procedure.aspx, accessed 10/16/17.)

Other revisions should encourage cooperation between lawyers, including Rules 4(m), 16, 26(d)(2) and 34(b)(2)(a), which reduce the time periods for various activities to happen. In addition, Rule 34 has been revised in ways that encourage cooperation and reduce the opportunity for dilatory tactics:

> **Rule 34:** Boilerplate objections are prohibited and objections must "state *with specificity* the grounds for objecting" and "whether any responsive materials are being withheld." The Committee notes: "An objection may state that a request is overbroad, but . . . should state the scope that is not overbroad." An objection that "states the limits that have controlled the search for responsive and relevant materials"—which might include the date range or the scope of sources or search terms used—"qualifies as a statement that the materials have been 'withheld.'" Furthermore, this Rule includes a new provision that "[t]he production must then be completed no later than the time for inspection specified in the request or another reasonable time specified in the response." This new provision appears to limit the parties' ability to engage in unconstrained rolling productions. [*Id*.]

In terms of Rule 26(b)(1)'s focus on proportionality, the Advisory Committee on Rules of Civil Procedure noted that a party "may not refuse discovery simply by making a boilerplate objection that it is not proportional." [*Id*.] As part of the revisions to Rule 37(e) on sanctions, the Committee noted that the rule recognizes that "reasonable steps" to preserve suffice; it does not call for perfection." [*Id*.]

There are many excellent sources of information on how law firms can increase the security of their data, their systems and their operations, particularly sensitive information relating to clients. One place to start is the website for Sensei Enterprises, Inc. (Sensei Enterprises, Inc., http://senseient.com/, accessed 10/16/17.) Nelson (lawyer) and Simek (engineer) have been leaders in information security, electronic discovery and data forensics for

many years. This company's website is a treasure trove of information, including articles, blogs, podcasts and YouTube videos. Lawyers are encouraged to register for the free article distribution service. Nelson and Simek, along with colleague David G. Ries, have published a number of excellent books, including *Locked Down: Practical Information Security for Lawyers*, 2nd ed. (American Bar Association, 2016, ISBN 978-1-63425-414-4). The author used the first edition of this book as one of her two textbooks in her course on cyber-security and is delighted that a new edition is available. Likewise from the ABA is *Information Security and Privacy: A Practical Guide for Global Executives, Lawyers and Technologists* by Thomas J. Shaw (American Bar Association, 2011, ISBN 978-1-61632-807-8), the other textbook used in the author's course. The content of the 1st edition has been updated by articles in the *Information Law Journal*, which is a publication of the Information Security and EDDE Committees, ABA Section of Science & Technology Law. (http://apps.americanbar.org/dch/committee.cfm?com=ST230002, accessed 10/16/17.) Recent communication with Mr. Shaw indicates that he has published two additional books that contribute to our understanding of technology in the practice of law. These books are *Emerging Technologies Law: Global Practice* (CreateSpace, 2017, ISBN 9781539769323, https://www.createspace.com/6675589) and *Information and Internet Law: Global Practice* (CreateSpace, 2016, 9781535378284, https://www.createspace.com/6434486).

Another excellent source of information on confidentiality and data security is the International Legal Technology Association (ILTA), which law firms can join for very modest annual dues based on the size of the law firm (http://www.iltanet.org/get-involved/membership, accessed 10/16/17.) ILTA publishes a quarterly journal, *Peer to Peer*, as well as White Papers, surveys, conferences, virtual events and local meetings. Many of the virtual events are free or very low cost. The author has used ILTA's webinars in her courses and there are also podcasts and recordings of various events. The American Bar Association has recently published some additional materials with respect to technology and security in the law office: *Cybersecurity for the Home and Office: The Lawyer's Guide to Taking Charge of Your Own Information Security* (John T. Bandler, 2017, ISBN 978-1-63425-907-1); *Technology Tips for Lawyers and Other Business Professionals* (Jeffrey M. Allen & Ashley Hallene, 2016, ISBN 9781634253444) and *The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals*, 2nd ed. (Jill Deborah Rhodes & Robert S. Litt, 2017, 9781634259798). In terms of professional

responsibilities in the context of electronic discovery, another source of helpful information, including case summaries, white papers, best practices and an email alert service is provided by Exterro (https://www.exterro.com/, accessed 10/16/17).

- Sharon D. Nelson, John W. Simek & Michael C. Maschke, *Risk Management: Practice Cybersecurity for Law Firms: How to Batten Down the Hatches*. ABA Journal, Oct. 2017, p. 28.
- Sharon D. Nelson & John W. Simek, *Securing Your Law Firm's Website: A Critical Cybersecurity Task*. Sensei Enterprises, Inc., 2017, https://senseient.com/articles/securing-law-firms-website-critical-cybersecurity-task/, accessed 10/16/17). A website may present risks that lawyers have not even thought about.
- Corsey Flaherty, *Developing Technological Competency as a Lawyer*. Michigan Bar Journal, June 2017, at 70.
- Joe Hoegler, *Here or There: Exchange On-Premises Versus Exchange Online*. Peer to Peer, Spring 2017, at 48.
- Brian Johnson, *Vulnerability Scanning Best Practices*. Peer to Peer, Spring 2017, at 20.
- David L. Hudson, Jr., *21st-Century Standards: Lawyers Must Secure Client Communications from Cyber Breaches*. ABA Journal, July 2017, at 24.
- Sharon D. Nelson, John W. Simek & Michael C. Maschke, *Technology/Cybersecurity Management & Policies*. Sensei Enterprises, Inc., 2017, https://senseient.com/articles/technologycybersecurity-management-policies/, accessed 10/16/17.
- Steve Flavell, *Conference Calls: The Forgotten Hole in Client Security*. Peer to Peer, Spring 2017, at 16.

B. ESI Issues to Address in the Courtroom

The philosophy behind the 2006 and 2015 amendments to the Federal Rules of Civil Procedure is that lawyers will work cooperatively to streamline the process, reduce burdens and costs and avoid behaviors and tactics that will delay or disrupt the proceedings. Indeed, such cooperation will be even more important with the reduced timelines for various activities. A particular focus of the 2015 amendments is on proportionality, with major revisions to Rule 26, and to address questions of spoliation and when and what sanctions are available as part of Rule 37. In terms of the December 2015 amendments to Rule 26:

> FRCP Rule 26(b) has been reorganized to place new emphasis on relevance and proportionality of discovery. The new rule changes the scope standard from "any relevant subject matter involved in the action" and information "reasonably calculated to lead to the discovery of admissible evidence," to information "**relevant to any party's claim or defense and proportional to the needs of the case.**"
>
> The proportionality factors have been relocated from Rule 26(b)(2)(C)(iii) to the front of the rule at FRCP Rule 26(b)(1) and include:
>
> - the importance of the issues at stake in the action;
> - the amount in controversy;
> - the parties' relative access to relevant information;
> - the parties' resources;
> - the importance of the discovery in resolving the issues; and
> - whether the burden or expense of the proposed discovery outweighs its likely benefit.
>
> These changes stress the parties' obligation to consider proportionality when propounding and responding to discovery and to focus on discovery of relevant information.
>
> Proportionality concepts in FRCP Rule 26(b) make their way into other revised rules as well. Additional depositions are permitted with leave of court in Rules 30 and 31, but the court can consider proportionality factors from 26(b). FRCP Rule 33 still limits interrogatories to 25, and additional interrogatories are permitted only to the extent consistent with the relevance and proportionality concepts in Rule 26(b)(1) and (2). [John J. Secosky, Jill Crawley Griset & Anne Bentley McCray, *E-Discovery Update: Federal Rules of Civil Procedure Amendments Go into Effect*. Legal Alert (McGuireWoods), December 1, 2015, https://www.mcguirewoods.com/Client-Resources/Alerts/2015/12/E-Discovery-Update.aspx, accessed 10/16/17.]

One of the major amendments to the FRCP in December 2015 concerned Rule 37 - an attempt to clarify what constitutes spoliation and when and what sanctions are available. First,

Rule 37(e) adopts a common law principle that a duty to preserve arises when litigation is "reasonably anticipated." Second, consequences for failing to preserve data are better defined in the new Rules. Rule 37(e)(1) provides that the court, "upon finding **prejudice** to another party from loss of the information, may order measures **no greater than necessary to cure the prejudice**."

> Under the new Rule, more serious sanctions for loss of ESI are only appropriate where the court finds that a party intended to deprive the other party's use of the ESI in litigation. Only upon a finding of intent can the court impose sanctions of an adverse inference jury instruction, dismissal of the action, or default judgment. [*Id*.]

The 2015 amendments to the FRCP, particularly Rules 26 and 37, clearly emphasize the importance of good information governance policies and procedures, not only for clients but also for law firms. In fact, assisting clients in establishing robust information governance programs may present a practice opportunity for law firms, since companies are beginning to see information as a strategic asset that needs to be managed correctly throughout its lifecycle and there is a dearth of people with this type of expertise. An article by Baron points to the interrelationship between information governance and electronic discovery with respect to the 2015 amendments. [Jason R. Baron, *IG and the New Rules: How Do the New FRCP Amendments Affect Info Gov Best Practices?* Legaltech News, Dec. 2015, pp. 60-61.]

C. Privilege Waivers

The waiver of privilege may be one of the riskiest aspects of an electronic discovery process, especially given the volume of potentially relevant ESI that needs to be reviewed and the shortened timeframes for when various activities need to happen, particularly under the 2015 amendments. As indicated by Secosky, Griset and McCray,

> The recent amendments to Rule 16 will reduce delays at the beginning of litigation by limiting the time to issue the scheduling order to the earlier of either 90 days (not 120 days) after service or 60 days (not 90 days) after any defendant has appeared. Also, the scheduling order may include Federal Rule of Evidence 502 agreements, which further the Courts' encouragement of non-waiver and claw-back agreements to facilitate discovery. [John J. Secosky, Jill Crawley Griset & Anne Bentley McCray, *E-Discovery Update: Federal Rules of Civil Procedure Amendments Go into Effect*. Legal Alert (McGuireWoods), December 1, 2015, https://www.mcguirewoods.com/Client-Resources/Alerts/2015/12/E-Discovery-Update.aspx, accessed 10/16/17.]

What the parties will rely on as relevant electronic evidence, Matthews notes the number of issues that parties are expected to meet and confer on under Rule 26(f).

- Electronic documents, such as email, documents, etc.
- How that data will be stored and preserved by each party
- Whether the data is considered reasonably accessible
- What will be considered privileged or work-product
- What formats will be expected for production of the data (with or without metadata, final drafts or all drafts, native file format or another format that the parties agree on) [David R. Matthews, *Electronically Stored Information: The Complete Guide to Management, Understanding, Acquisition, Storage, Search, and Retrieval*, 2nd ed. CRC Press, 2016, p. 5.]

Although often viewed with skepticism, lawyers should consider the wisdom of negotiating claw-back agreements rather than relying on federal or local rules to prevent a waiver of attorney-client privilege, attorney work-product or other confidentiality doctrine. While the parties can negotiate a "claw-back" agreement, the risk is that the court will still determine that the attorney-client privilege or attorney work-product has been waived if the e-discovery process was sloppy, especially the review step. There are also protections against waiver in the Federal Rules of Evidence (FRE). Note that FRE 502 specifically addresses the attorney-client privilege and gives protection from inadvertent disclosure, similar to FRCP Rule 26(b)(5). Rule 502(b) allows you to request the return of inadvertently produced privileged or work-product evidence if you took reasonable steps to prevent the error, noticed it quickly and responded promptly.

However, it especially points to the need to have a solid e-discovery process, especially at the crucial review step – the last line of defense before the ESI is produced to the opposing party.

A search of the K&L Gates database for cases from 2016-2017 involving privilege provides the following summaries:

- *Ballentine v. Las Vegas Metro Police Dept.*, NO. 2:14-cv-01584-APG-GWF, 2016 WL 3636917 (D. Nev. July 5, 2016).

  Among other things, court denied motion for protective order upon finding that Plaintiffs were "entitled to obtain basic information sufficient to determine whether searches were reasonably conducted and the results properly verified" even without "evidence that specific documents were destroyed or withheld" and reasoned that "the fact that [Defendant's] attorney(s) conducted or supervised the searches does not protect such non-privileged information from disclosure."

- *Whitesell Corp. v. Electrolux Home Prods., Inc.*, NO. CV 103-50, 2016 WL 1317673 (S.D. Ga. Mar. 31, 2016).

  Where promised emails were not produced but Defendant ultimately produced all documents relevant to the alleged spoliation, including "preservation communications to document custodians, a list of custodians who were searched, the search terms used to conduct the search, and project documents and materials relating to such searches," and also submitted a representative for an extensive Rule 30(b)(6) deposition, the court found Plaintiff's request to compel production of "every privileged document described as concerning data collection—was overly broad, unduly burdensome and had not been shown to relate to the issue at the forefront of this entire exercise—the missing Leon emails" despite acknowledging that "otherwise privileged documents may be discoverable upon a preliminary showing of spoliation."

- *Harleysville Ins. Co. v. Holding Funeral Home, Inc.*, No. 1:15cv00057 (W.D. Va. Feb. 9, 2017).

  In this case, the court found that the placement of privileged information on a file share site and dissemination of the hyperlink to access that information without additional protections (e.g, password protection) constituted a failure to take reasonable steps to protect the information and that the attorney-client privilege and work-product protections were waived. Notably, however, because defense counsel accessed the information but failed to notify Plaintiff's counsel of the possible production of privileged materials, they were ordered to pay Plaintiff's fees and costs in bringing the motion to disqualify them, which was denied.

- *Irth Sols. LLC v. Windstream Commc'ns LLC*, No. 2:16-CV-219, 2017 WL 3276021 (S.D. Ohio Aug. 2, 2017).

  In this case, despite the existence of a clawback agreement (not an order) indicating that "[i]nadvertent production of privileged documents does not operate as a waiver of that

privilege," the court found that privilege was waived by the inadvertent but "completely reckless" production of privileged materials … twice. In so concluding, the court rejected the notion that a clawback agreement always protects against waiver, regardless of its terms, and instead indicated its support for courts that have precluded protection from a clawback agreement when the disclosure was "completely reckless" and for a framework that allows a court to rely on Fed. R. Evid. 502(b) when a clawback agreement fails to provide sufficiently concrete terms.

- *CP Salmon Corp. v. Pritzker*, ---F. Supp. 3d.---,No. 3:16-cv-00031-TMB, 2017 WL 744022 (D. Alaska Feb. 24, 2017).

  Applying Fed. R. Evid. 502, court found Defendants' inadvertent inclusion of privileged information in the Administrative Record did not waive privilege where declarations of persons with "sufficient personal knowledge" established the inadvertence of the inclusion where, in light of the multiple levels of review of the documents and the relevant circumstances including the "sheer number of pages and compressed timeframe," the court found Defendant had undertaken reasonable steps to prevent disclosure, and where Defendants took action to rectify the error within three weeks of the disclosure

Likewise, the Kroll Ontrack database of cases yielded interesting results for 2016-2017:

- *Gardner v. Continental Cas. Co.*, 2016 WL 155002 (D. Conn. Jan. 1, 2016).

  In this insurance case, the plaintiffs sought to compel production of 38,000 documents, all of which were found using the agreed-upon search terms. The defendant only produced 2,214 pages after a relevance and privilege review, and 274 of the produced documents were just "copies of the complaints, with exhibits, filed in the lawsuit." The plaintiffs argued that the defendant "cherry-picked" documents for production. Further, the plaintiffs argued that the purpose of the agreed-upon search terms was "to avoid prolonged and detailed debate over what ESI documents [were] 'responsive' . . ." The plaintiffs supported their position regarding the scant production by pointing out that the defendant's third-party claims adjustor submitted a "far more comprehensive and informative" production, while the defendant argued that it had already provided "extensive discovery" and that it had spent "significant resources" reviewing the documents from the agreed-upon search terms. The court held that the plaintiffs' position was "untenable," and concluded that the defendant was not obligated to produce all 38,000 documents "after a review eliminates some on the basis of privilege." The court did, however, recognize the plaintiffs' "legitimate concern" regarding the limited production, and ordered opposing counsel to confer and discuss approaches for addressing the search hits - "sampling and iterative refinement" or "quick peek protocol" - and also ordered an in camera review of several documents to determine if redactions were appropriate.

- *Thorne Research v. Atlantic Pro-Nutrients*, 2016 WL 1122863 (D. Utah Mar. 22, 2016).

  In this patent infringement suit, the defendant filed a motion to compel, seeking a copy of a database that the plaintiffs' inventor used to enter the patented formula at issue. The defendant claimed that it required the metadata from the database to determine the truth

behind the plaintiffs' claim that their inventor had developed the formula first. The defendant believed that the plaintiffs had tampered with the database to falsify an early formation date. The plaintiffs argued that the Microsoft Access database did not maintain metadata like a word processing or spreadsheet program, that production of the entire database would give the defendant access to other proprietary information and that there was no evidence of metadata tampering. The court found that the parties offered conflicting affidavits regarding the existence of metadata associated with the database and stated that the defendant could access the database to conduct a forensic analysis to determine if metadata exists under a protective order containing "an attorneys' eyes only" designation.

- *Wit v. United Behavioral Health*, 2016 U.S. Dist. LEXIS 7242 (N.D. Cal. Jan. 21, 2016).

  The defendant, claiming attorney-client privilege, objected to producing redacted information in discovery. The court, construing relevance broadly due to the 1978 Supreme Court opinion in Oppenheimer, held that some of the redacted information was indeed discoverable, despite the privilege. The court was aware of the fact that the Oppenheimer decision was interpreting relevance at a time that "subject matter" jurisdiction was still in the rule (it was deleted in the 2015 Amendments). Despite the new amendments and their emphasis on proportional discovery, some courts will still interpret relevance broadly. While use of Oppenheimer has been criticized, it is consistent with Supreme Court and other Circuit case law and probably is not causing courts to inappropriately broad discovery. "Traditionally, the relevance requirement of Rule 26(b)(1) has been construed broadly."

- *Rowan v. Sunflower*, 2016 U.S. Dist. LEXIS 72254 (D. Kan. June 2, 2016).

  In this personal injury case, the plaintiff motioned the court to compel discovery from one of the defendants. Before this motion, the defendant had already produced 75,000 pages of responsive documents and ESI. The defendant argued that it could not produce the desired discovery because it was subject to attorney-client privilege. Using the newly amended FRCP 26(b)(1) and its emphasis on proportionality, the court denied the plaintiff's motion. The court elaborated that even though the parties themselves did not bring up proportionality in their arguments, "[u]nder the amended rule, however, the Court has an obligation to limit the frequency or extent of discovery," if the discovery requests are not proportional.

- *Shawe v. Elting*, 2017 Del. LEXIS 61 (Del. Feb. 13, 2017).

  In this business dispute, the plaintiff appealed the Court of Chancery's decision ordering the plaintiff to pay the defendant's legal fees totaling over $7 million. The parties were business partners and former romantic partners, and were engaged in highly contentious litigation. The Chancery Court found that the plaintiff committed several bad acts including, among other things, breaking in to the defendant's office and having a third party image her hard drive; concealing his activities with a write blocker; accessing 19,000 of the defendant's emails, 12,000 of them privileged communications with defendant's counsel; deleting nearly 19,000 files from his computer after placing his own legal hold due to impending litigation; hiring a third party to break into the defendant's

office to take photos and remove documents; attempting to destroy 44,000 documents from his laptop after the court ordered expedited discovery; failing to preserve his mobile phone and its contents; and giving false testimony. The court held that there was no abuse of discretion, that the plaintiff acted in bad faith with his "egregious conduct and multiple falsehoods," and that court was "well within its discretion to impose sanctions." Additionally, the court found that the sanctions were not in excess, as they were to compensate the defendant's actual litigation expenses.

- *Liguria Foods, Inc. v. Griffith Labs., Inc.*, 2017 WL 976626 (N.D. Iowa Mar. 13, 2017).

  In this breach of contract case over spoiled sausage, each party accused the other of abusive discovery practices. The court, expressing its frustration over lawyers' widespread "addiction to boilerplate discovery objections . . . that plague the litigation industry", issued an order to show cause why both parties should not be sanctioned for "flaunting" the rules of discovery and continuing the use of boilerplate language. The court pointed to FRCP 1 that courts have an obligation to ensure "the just, speedy, and inexpensive determination of every action and proceeding", and explained that using broad language in discovery objections only hinders, rather than expedites discovery, by "obstruct[ing] the discovery process, violat[ing] numerous rules of civil procedure and ethics, and impos[ing] costs on litigants that frustrate the timely and just resolution of cases." The court cited to various judicial authorities that have articulated similar concerns, and are increasingly encouraging courts to impose sanctions to get the legal community's attention and "punish this nonsense." Counsel for both parties acknowledge their failure to respond with specificity, but that they did not do so to delay proceedings or harass the other party. Instead, the parties explained that they used boilerplate language primarily to preserve their clients' rights. Additionally, the parties explained that such language was part of the present litigation culture that they anticipated that the other party would also use the same language, and that changing their wording to comply with the 2015 amendments would weaken their case. The court emphasized the proportionality requirements of FRCP 26, the need to respond to requests for privileged documents with "more than bald responses", and the need to respond with specificity when making objections to FRCP 33 and FRCP 34 requests. The court also expressed policy concerns that discovery is the most costly part of litigation in large part due to delays caused by overly broad objections, causing parties to settle disputes out of concern over cost rather go forward in the pursuit of justice. In spite of the judiciary's push to impose sanctions, the court did not do so in this case. The court found that the parties have acted cordially and professionally throughout the proceeding, and required minimal intervention by the court considering the case's complexity. However, the court issued stern words of caution: "NO MORE WARNINGS. IN THE FUTURE, USING "BOILERPLATE" OBJECTIONS TO DISCOVERY IN ANY CASE BEFORE ME PLACES COUNSEL AND THEIR CLIENTS AT RISK FOR SUBSTANTIAL SANCTIONS."

- See also: Vincent A. Citro, *Time to Evolve the Attorney-Client Privilege to Protect Communications Stored Electronically*. 64 The Federal Lawyer 40 (June 2017).

D. Searching Social Networking Sites

The client's use of social media poses risks to confidentiality. One recommendation is to have a thorough conversation with the client about how he/she would like to be communicated with. This information should be included in the representation letter. This is an opportunity to alert the client to the risks of communicating through a public fax, an employer-provided email system, an email system where family members have access to each other's messages or share the same login and password or talking loudly in public on a cell phone, all of which can waive the attorney-client privilege. Social media is especially tempting for clients – it is so easy to post information about an opposing party (soon-to-be ex-spouse) or reveal information that would be adverse to a client's case (mountain climbing when claiming to be injured and unable to work). Social media provides a particularly rich repository of evidence in bankruptcy. [*See* Sara Anne Hook & Katherine Taht, *Social Media and Electronic Discovery: A Potential Source of Evidence in Bankruptcy Proceedings.* NABTalk: The Journal of the National Association of Bankruptcy Trustees, Winter 2011, pp. 24-29.] Lawyers do use social media extensively to find information about opposing parties, judges, witnesses, etc., so clients should be made aware of this. On the other hand, the client should be admonished not to alter, change or remove information from his/her social media site once litigation is reasonably anticipated, because doing so could bring a claim of spoliation.

Note that one of the major revisions to the Federal Rules of Civil Procedure was to Rule 37(e), which attempts to clarify when sanctions are available for spoliation. Many clients – and even their lawyers – would be shocked to learn about all of the ways that potentially relevant evidence is being generated by daily activities and use of devices, often without being aware of it. The Internet of Things, such as wearable devices and Smarthouse technology, is going to provide a rich repository of information about people's whereabouts and habits. For example, a recent article in *The Indiana Lawyer* indicates that data from fitness trackers is already being requested in civil and criminal cases. [*See* Marilyn Odehdahl, *Fitness Trackers Add to Flood of Digital Evidence in Court*. The Indiana Lawyer, Aug. 10, 2016 and Vishakha Kumari & Sara Anne Hook, *The Privacy, Security and Discoverability of Data on Wearable Health Devices: Fitness or Folly?* HCI International 2017, Vancouver, Canada, July 12, 2017.] Lawyers need to be careful about the risks of revealing confidential, privileged or work-product information

through their own social media activities as well as through the law firm's website or blog. These tools are tempting for law firm marketing and promotion of individual achievements, but need to be used with care, with policies and procedures in place and regular review and updating. This is particularly important with blogs, as a recent survey indicates that more law firms plan to use this feature as a way to generate more clients. [Victor Li, A Blog Clog? *Survey: Law Firms Plan More Posting for More Business*. ABA Journal, April 2016, p. 32.] Gubbins provides some excellent articles on improving a law firm's website and online presence. [Roberta M. Gubbins, *Time for Review of Your Online Presence*. Michigan Bar Journal, June 2016, at 16, Roberta M. Gubbins, *Is One Online Presence Enough?* Michigan Bar Journal, May 2016, at 16. and Roberta M. Gubbins, *How to Write a Winning Lawyer Profile*. Michigan Bar Journal, Sept. 2017, at 14.] Parness covers five lessons that we can learn about the ethical issues for lawyers when using social media (Hillel I. Parness, *Toward a Social Networking Law (2017 Edition)*. 10 Landslide 44 (Sept./Oct. 2017).

- Lesson No. 1: Why Can't We Be Friends?
- Lesson No. 2: It's OK to Look, Isn't It?
- Lesson No. 3: Was It Something I Said?
- Lesson No. 4: Don't Use "Password" as Your Password
- Lesson No. 5: Boyfriends Often Become Ex-Boyfriends

Social media is perhaps one of the most fruitful kind of evidence to pursue, because of its spontaneity, its informality, its near permanence, and how easy it is to gather. Moreover, most courts have said that what is posted on social media is nearly always discoverable and admissible. However, newer forms of social media and mobile messaging systems are being designed to specifically avoid later discoverability. [*See* Cori Faklaris & Sara Anne Hook, Oh, Snap! *The State of Electronic Discovery Amid the Rise of Snapchat, WhatsApp, Kik, and Other Mobile Messaging Apps*. 63 The Federal Lawyer 64 (May 2016).] There are many cases involving social media that provide guidance and many articles and seminars are available. For example, the International Legal Technology Association is offered a webinar in July titled Social Media and Mobile Device Data Collection and Defensibility. [John Evans & Gordon J. Calhoun, *Social Media and Mobile Device Data Collection and Defensibility*. International Legal Technology Association, July 26, 2016, http://connect.iltanet.org/viewdocument/07-26-16-webinar-rec?_ga=1.57906536.313945060.1473775475&ssopc=1, accessed 10/16/17.]

Although nearly always discoverable, there are ongoing issues with authenticity and integrity. Chapter 1 of *Electronically Stored Information: The Complete Guide to Management, Understanding, Acquisition, Storage, Search, and Retrieval*, 2nd ed., highlights these issues. [David R. Matthews, *Electronically Stored Information: The Complete Guide to Management, Understanding, Acquisition, Storage, Search, and Retrieval*, 2nd ed. CRC Press, 2016.] The author devotes several pages to the problems with ESI as discoverable evidence, stating that we have to think about how it is different from any other type of data or information. He gives the example of a contract on page 50 to show how evidence would be handled in a paper-based world, including that proving the integrity of that type of evidence would be relatively easy. The author then invites us to think about how electronic evidence is different.

The first big difference between ESI and paper-based evidence is the sheer volume of it. We can assume that, given the exponential growth in electronic data worldwide, the quantity of electronic evidence will continue to grow, which is one of the most important problems we have to deal with when working with ESI. In fact, a recent survey indicates that the volume of data that needs to be handled continues to be the largest obstacle in e-discovery.

Another big difference is the data itself, which is dynamic by its very nature. It can be changed in ways that are not even apparent, simply by accessing it, viewing it or moving it. The non-apparent information that can become part of electronic data is metadata. This dynamism creates problems with the integrity of electronic data, because it is easy to manipulate it to reflect a different reality. It can be difficult to confirm that such manipulation has occurred. Note the increasing pressure to have digital evidence deemed "hearsay" or at least to change the rules of evidence to require a higher level of reliability be demonstrated. As indicated on page 52, this issue is being treated very differently in different jurisdictions. On pages 52-55, the author provides some examples based on real-life scenarios to demonstrate the challenges with electronic evidence. As he states on page 55, "[t]hough we have moved to a world where nearly all documentation is electronic, the issues of relevance, integrity, and availability remain as important as ever." He goes on to caution that a high level of expertise and training are required to understand, analyze, and clearly explain whether electronic documentation is relevant to a case, is what it purports to be, has not been tampered with, and can be counted on to prove or

disprove an assertion. [*See* Angela Foster, *Admissibility of Social Media Evidence in Federal Court: Is It What It Purports to Be?* The Computer & Internet Lawyer, June 2016, at 13.]

E. Personal Privacy Concerns Arising from Modern Database Searches

A long line of cases supports the discoverability and admissibility of potentially relevant evidence from social media sites as well as evidence created in all types of formats and by a wide variety of software tools and devices. The stance of most courts is that this evidence is going to be allowed in spite of concerns about personal privacy. The reality is that our globally-connected, technology-enabled world means that there is a multiplicity of information available about us which is easily accessed, much of it without our even knowing about it. A long line of cases regarding social media has made this very clear, even though a party may have challenged the availability of this evidence on a number of grounds. The materials from a seminar at the 2013 ABA Annual Meeting provides a comprehensive list of privacy protections that may or may not protect private information. [Gary L. Beaver, Steven Brower, Amy Longo, Cecil A. Lynn, III, & Mark Romance, *Social Media Evidence – How to Find It and How to Use It*, ABA Annual Meeting, Aug. 8-12, 2013:

- Federal Trade Commission Act (FTC Act)
- Financial Services Modernization Act (also known as the Gramm-Leach Bliley Act)
- Health Insurance Portability and Accountability Act of 2996 (HIPAA)
- The Children's online Privacy Protection Act (COPPA)
- The Family Educational Rights and Privacy Act (FERPA)
- The Fair Credit Reporting Act (FCRA)
- The Stored Communications Act (SCA), which is part of the Electronic Communications Privacy Act. Note that although this statute was enacted before the Internet, the SCA remains the primary statute affecting social media. A long line of cases indicates that this may still be an unsettled topic. However, commentators suggest that the parties be approached with requests for social media materials rather than the vendors as a way to avoid claims that the material is protected under SCA. [*See Id.* at 5-7, which offers a summary of the SCA and relevant cases.]
- State data privacy laws, such as disposal of customer records and security of personal information, with Massachusetts considered to have the most robust legislation for personal privacy
- International data privacy laws – note the weakening of the safe harbor provisions offered under the EU directives and the potential impact from Brexit
- Common law protections, such as intrusion upon seclusion, public disclosure of private facts and misappropriation
- Constitutional protections under the First, Fourth, Fifth and Ninth amendments
- The National Labor Relations Act (which is even being extended beyond unionized employers)

Terms of service also need to be considered when planning to request information from social media services, Internet service providers and other vendors of technologically-based communications:

> 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). [*Id*. at 8.]

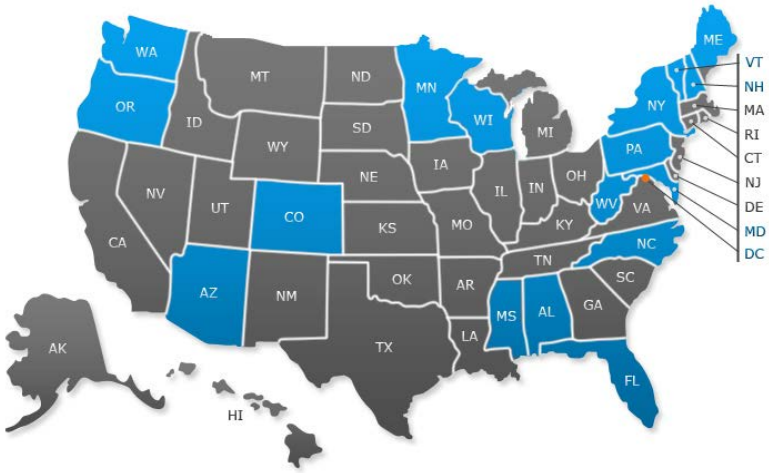
F. Ethical Duties When Mining Metadata

The ABA has provided an excellent website with all of the ethics opinions on mining for metadata as well as two of its own Formal Opinions that relate to metadata, Formal Opinion 06-442 and 05-437. [Metadata Ethics Opinions Around the U.S., American Bar Association, http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/metadatachart.html, accessed 10/16/17.] The ABA provides the following definition of metadata:

> Metadata is loosely defined as "data about data." More specifically, the term refers to the embedded stratum of data in electronics file that may include such information as who authored a document, when it was created, what software was used, any comments embedded within the content, and even a record of changes made to the document.
>
> While metadata is often harmless, it can potentially include sensitive, confidential, or privileged information. As such, it presents a serious concern for attorneys charged with maintaining confidentiality -- both their own and their clients. Professional responsibility committees at several bar associations around the country have weighed in on attorneys' ethical responsibilities regarding metadata, but the opinions vary significantly. [*Id.*]

Simply put, metadata is "data about data."

The ABA's website features a map to make it easy to access each state's ethics opinion as well as a table indicating the jurisdiction/source of the opinion, the sender's duty when transmitting the metadata, whether the recipient may review or "mine" the metadata and whether the recipient must notify the send if metadata is found.



In terms of the sender's duty when transmitting metadata, the ABA's response is that there is:

> No explicit duty regarding metadata is imposed, but a number of methods for eliminating metadata (including "scrubbing," negotiating a confidentiality agreement, or sending the file in a different format) are suggested for attorneys who are "concerned about the possibility of sending, producing, or providing to opposing counsel a document that contains or might contain metadata." [06-442]
>
> Presumably, a lawyer's general duties with regard to the confidentiality of client information under Rule 1.6 apply to metadata. [*Id*.]

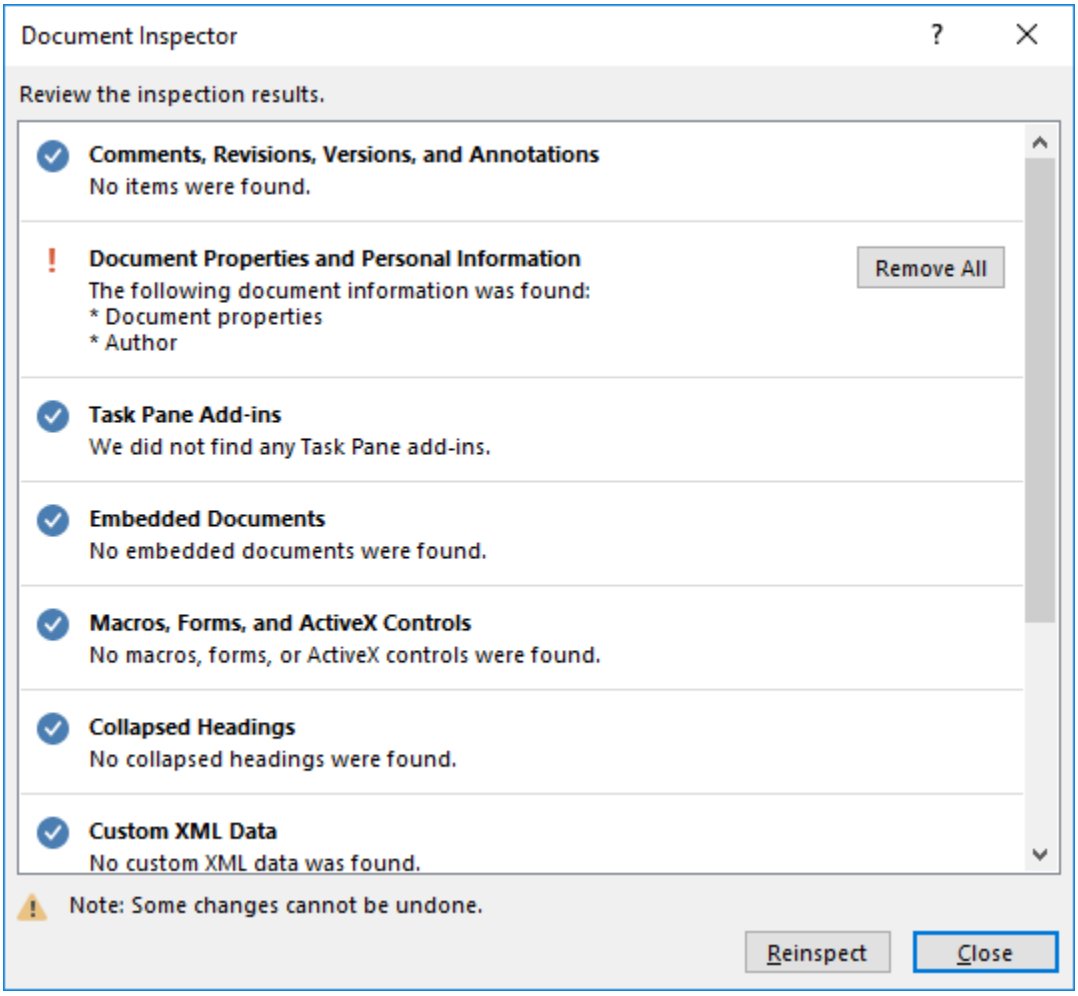
As to the question of whether the recipient may review or "mine" the metadata, the ABA opinions indicate that this is permissible, with the following commentary:

> Some authorities have found metadata mining "ethically impermissible," the Committee states that it "does not share such a view, but instead reads the recent addition of Rule 4.4(b) identifying the sole requirement of providing notice to the sender of the receipt of inadvertently sent information, as evidence of the intention to set no other specific The ABA's opinions indicate that the recipient must notify the sender if metadata is found, if the lawyer knows or reasonably should have known that transmission was inadvertent.
>
> ABA Formal Opinion 05-437 cites the Rule 4.4(b) provision that a "lawyer who receives a document relating to the representation of the lawyer's client and knows or reasonably should know that the document was inadvertently sent shall promptly notify the sender." [05-437]
>
> The Opinion goes on to state that Rule 4.4(b) "obligates the receiving lawyer to notify the sender of the inadvertent transmission promptly" but "does not require the receiving lawyer either to refrain from examining the materials or to abide by the instructions of the sending lawyer." [05-437] [*Id.*]

It is important to note that metadata is generated automatically by common software programs, often without the user even being aware of it. Such potentially relevant information as the document's author, date of creation, date of revisions, time spent on the document, etc. are easily determined without fancy digital forensics capabilities. For example, by using the Info selection in Word, I can already see the following information about this chapter in the seminar manual, even though I am starting from the bottom up with section F.

I can easily obtain additional information by selecting Show All Properties, found at the bottom right of the screen.

Then the Inspect Document tool may provide even more information that might be potentially relevant.



Using features such as Track Changes may also reveal information that should be kept confidential. The lawyer and all members of the legal team will want to take care that metadata has been removed from all documents and files before transmitting them using one of the recognized methods for doing this (software tools, redacting, etc.). Although many people believe that converting the document to PDF format will be enough to remove metadata, others caution that this is not necessarily always effective. Of course, if the material is being – or it is reasonably foreseeable that it will be – requested as part of an electronic discovery process, the lawyer and client are under a duty to preserve that material in its native format with the metadata intact.