VI. Legal Ethics and ESI

Sara Anne Hook, M.B.A., J.D.
NBI, October 28, 2016
A. DUTIES OWNED TO CLIENTS, OPPOSING COUNSEL AND THE COURTS
Duties Owed to Clients, Opposing Counsel and the Courts

• 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.)
Duties Owed, cont.

• Indiana Rules of Professional Conduct
  • Rule 3.1. Meritorious Claims and Contentions
  • Rule 3.2. Expediting Litigation
  • Rule 3.3. Candor Toward the Tribunal
  • Rule 3.4. Fairness to Opposing Party and Counsel
  • Rule 4.1. Truthfulness in Statements to Others
  • Rule 4.2. Communication with Person Represented by Counsel
  • Rule 4.3. Dealing with Unrepresented Persons
  • Rule 4.4. Respect for Rights of Third Persons
Duties Owed, cont.

• 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.
Duties Owed, cont.

• 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.
Duties Owed, cont.

- 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 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.
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.
Duties Owed, cont.

- [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.
Duties Owed, cont.

- However, Comments 18 and 19 to the ABA Model Rules of Professional Conduct, Rule 1.6 provide more detailed guidance.
- It is important to note that there are rules related to the confidentiality and other duties owed to both former and prospective clients.
Duties Owed, cont.

• 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:
Duties Owed, cont.

- 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.]
Duties Owed, cont.

• 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 9/13/16.)

• 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.


- Mr. Shaw indicates that the content of this book is continually 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](http://apps.americanbar.org/dch/committee.cfm?com=ST230002), accessed 9/13/16.)

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](http://www.iltanet.org/get-involved/membership), accessed 9/13/2016.)

- 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.
B. ESI ISSUES TO ADDRESS IN THE COURTROOM
ESI Issues

• 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.
ESI Issues, cont.

- 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.
ESI Issues, cont.

- 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 9/13/16.]
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.

C. PRIVILEGE WAIVERS
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 (including social media) 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 9/13/16.]
Privilege Waivers, cont.

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

• 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.
Privilege Waivers, cont.

• 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.
Privilege Waivers, cont.

• A search of the K&L Gates database for cases from 2016 involving privilege provides the following summaries:
D. SEARCHING SOCIAL NETWORKING SITES
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.
Searching Social Networking Sites, cont.

- 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.
Searching Social Networking Sites, cont.

- Note again 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.
• 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.]

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.

There are many cases involving social media that provide guidance and many articles and seminars are available.
Searching Social Networking Sites, cont.


• 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.
Searching Social Networking Sites, cont.

• 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.
Searching Social Networking Sites, cont.

• 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, pp. 13-16.]
E. PERSONAL PRIVACY CONCERNS ARISING FROM MODERN DATABASE SEARCHES
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.
Personal Privacy Concerns Arising from Modern Database Searches, cont.

• 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 1996 (HIPAA)
  • The Children’s online Privacy Protection Act (COPPA)
  • The Family Educational Rights and Privacy Act (FERPA)
  • The Fair Credit Reporting Act (FCRA)
Personal Privacy Concerns Arising from Modern Database Searches, cont.

- 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.
Personal Privacy Concerns Arising from Modern Database Searches, cont.

- 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
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 9/13/16.]
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.”
Mining Metadata, cont.

- 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.]
Mining Metadata, cont.

• 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.]
Mining Metadata, cont.

- 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.
- See examples of metadata in this chapter of the seminar manual as well as the PowerPoint slides for Section V, supra.
Mining Metadata, cont.

• 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.
Any Questions?

• Thank you for attending today’s seminar!

• Contact:
  Sara Anne Hook, M.B.A., J.D.
  317-278-7690
  sahook@iupui.edu