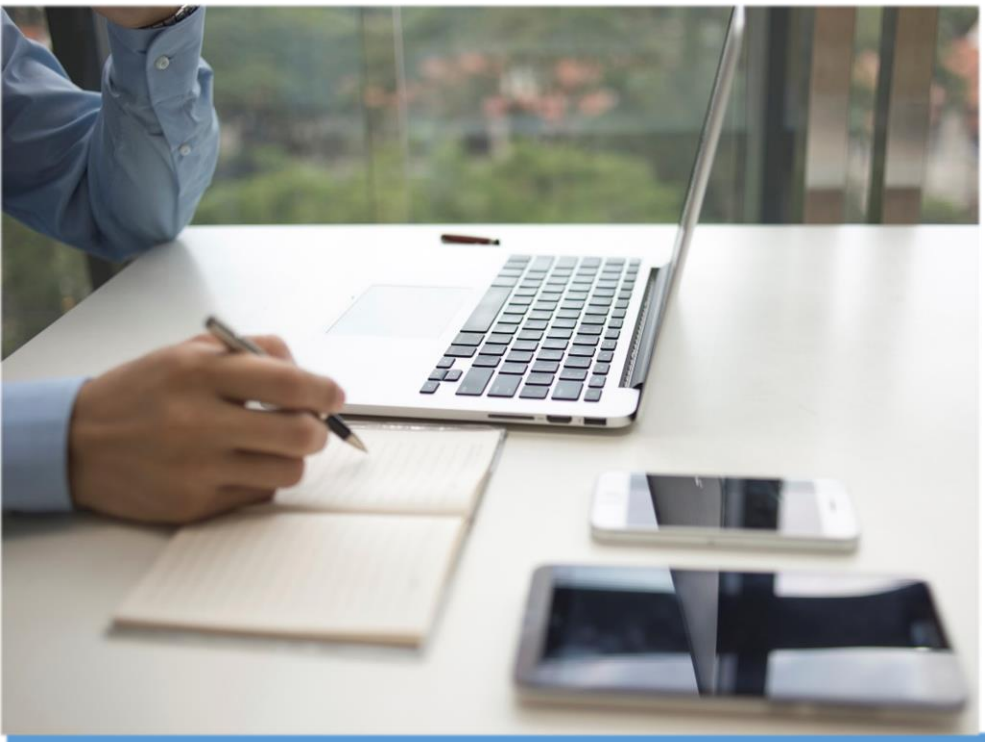


Clear Law Institute

Admissibility of Email and Internet Evidence

Presented by:
Dennis Wilenchik

Clear Law Institute | 4601 N. Fairfax Dr., Ste 1200 | Arlington | VA | 22203

www.clearlawinstitute.com

Questions?
Please call us at 703-372-0550 or email us at info@clearlawinstitute.com

All-Access Membership Program



- Earn continuing education credit (CLE, CPE, SHRM, HRCI, etc.) in all states at no additional cost
- Access courses on a computer, tablet, or smartphone
- Access more than 75 live webinars each month
- Access more than 750 on-demand courses

Register within 7 days after the webinar using promo code “7member” to receive a $200 discount off the $799 base price.

Learn more and register here:
http://clearlawinstitute.com/member

Admissibility of E-mail and Internet Evidence

Dennis I. Wilenchik, Esq.
Wilenchik & Bartness, P.C.

Clear Law Institute
Online Continuing Education

WB
WILENCHIK & BARTNESS
ATTORNEYS AT LAW

© Wilenchik & Bartness, P.C.
1

The Digital Revolution

- 2.5 quintillion bytes of data are created every day, which is expected to accelerate greatly with the growth of the Internet of Things ("IoT").
- IOT has evolved from machine-to-machine to human-to-machine, than By 2020, about **1.7 megabytes** of information will be created **every second** for **every person** on earth.
- *We perform 40,000 search queries every second (on Google alone), which makes it 3.5 billion searches per day and 1.2 trillion searches per year worldwide. http://www.internetlivestats.com/google-search-statistics/*

Marr, B. "How Much Data Do We Create Every Day? The Mind-Boggling States Everyone Should Read," Forbes (May 21, 2018).

2

The Internet of Things ("IoT")

- IoT is a system of interrelated computing devices which transfer data over a network without requiring human-to-human interaction.
- By 2020, more than 26 billion connected things will be used worldwide, according to Garner, Inc., a research and advisory firm.
- The thing could be a human with a heart monitor implant or a man-made object like an automobile with built-in sensors; coffee makers; washing machines; printers.
- Devices operate in the background and transmit your personal data, which has led to an entirely new area of evidence-gathering and will require you to know how to gather that information to ensure that it is admissible in court.



3

Counsel's Duties

- To understand and be fluent in information technology.
- To "identify, locate, and maintain information that is relevant to specific, predictable, and indentifiable litigation." Victor Stanley, Inc. v. Creative Pipe, Inc., 269 F.R.D. 497 (2010). Quoting The Sedona Conference, Commentary on Legal Holds: The Trigger and the Process 3 (public cmt. ed. Aug.2007); see also, HM Elecs., Inc. v. R.F. Techs., Inc., 2015 WL 4714908 (S.D. Cal. Aug. 7, 2015).
- To understand your obligations under the applicable Rules of Civil Procedure. Qualcomm Inc. v. Broadcom Corp., 2008 WL 66932 (S.D. Cal. Jan. 7, 2008), vacated in part, 2008 WL 638108 (S.D. Cal. March 5, 2008).

4

Counsel's Duties

- With the 2015 changes to the Federal Rules of Civil Procedure, that obligation has become increasingly important.
  - Rule 1, Fed. R. Civ. P. : emphasis on cooperation and proportionality.
    - Chief Justice John Roberts stated: "The 2015 civil rules amendments are a major stride toward a better federal court system. But they will achieve the goal of Rule 1—'the just, speedy, and inexpensive determination of every action and proceeding'— only if the entire legal community, including the bench, bar, and legal academy, step up to the challenge of making real change. "

5

Counsel's Duties

- In fact, two states (Florida (2016) and North Carolina (2019) require 3 hours of Technology Training as part of their yearly CLE requirement.
- The State Bar of California Standing Committee on Professional Responsibility Opinion 2015-193 has stated:
  - "…attorney competence related to litigation generally requires, among other things, and at a minimum, a basic understanding of, and facility with, issues relating to eDiscovery, including the discovery of electronically stored information ("ESI")…"
  - "…an attorney lacking the required competence for eDiscovery issues has three options:
    - Acquire sufficient learning and skill before performance is required;
    - Associate with or consult technical consultants or competent counsel;
    - Decline the client representation- lack of competence in eDiscovery issues also may lead to an ethical violation of an attorney's duty of confidentiality…;"
    - "…attorneys who handle litigation may not ignore the requirements and obligations of electronic discovery…."

6

What is ESI?

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

7

Several Different Forms of ESI

- ESI Includes:
  - Word processing documents
  - Spreadsheets
  - Emails
  - Digital Photos
  - Videos
  - Voicemails and audio files
  - Text Messages
  - Instant Messages
  - Call Logs
  - Database Contents
  - Internet Activity (including electronic research)
  - Source Code (software which computers run in order to create and process data. More below)

8

ESI SOURCES

- Cloud storage
- Networks
- Servers
- Computer Directories
- Removable Storage Devices
- Voice activated Digital Assistants
- Peripheral Devices (i.e., scanners, printers, microphones, and other devices connected to a computer)
- Computers, Phones, Tablets, Other Smart Devices (Including BYOD – Bring Your Own Device)
- Archived Data Tapes
- Legacy Systems
- Databases
- Digital Workspaces (where employees work remotely)
- Social Media Sites

9

Important Key Terms Used in the E-Discovery World

- Why do We Have to Know these Terms?
  - Because you will know the lingo when you meet and confer about ESI, you can add the appropriate language when drafting litigation holds, protective orders, discovery, and case management orders or hiring proper third party vendors and expert witnesses.

10

Some Key ESI Terms

- Metadata: "Data about data."
- Coding: Action of labeling document as relevant or non-relevant or set of labels from that action.
- Deduplication: Replacing multiple identical copies of a document with one copy.
- Native file: Electronic documents with an associated file structure from the original application.
- OCR: Optical Character Recognition.
- ECA: Early Case Assessment, using tools or methods to investigate document collection to determine the risks and costs.
- Units of Measurement: Units of measurement for digital information. The smallest: "bit;" largest: "bronto."
- TAR: Technology Assisted Review or predictive coding.
- AI: Artificial Intelligence, demonstrated by machines, rather than humans.

See also, M. Grossman, G. Cormack, *Grossman-Cormack Glossary of Technology-Assisted Review*, 7 Federal Courts Law Review 1 (2013).

11

What is Discoverable?

- "Any designated documents or electronically stored information—including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations—stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form." Fed.R.Civ.P. 34(a)(1).

12

The Sedona Principles

- The 2006 Amendments to the Federal Rules of Civil Procedure were based upon these 14 principles developed by the Sedona Conference, a nonprofit group of judges, attorneys, experts and academics, founded in 1997 to study law and policy in the areas of antitrust, complex litigation and intellectual property. https://thesedonaconference.org/
- The 14 Sedona Principles are being updated to keep up with the expanding types and volumes of ESI and how to handle all aspects of e-discovery.

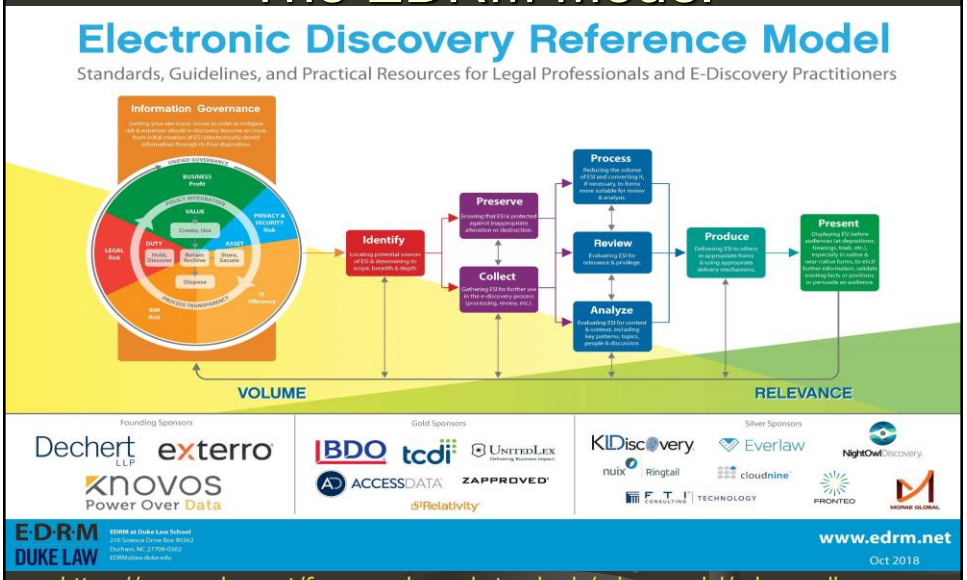
13

The EDRM Model and the Life Cycle of E-Discovery

- Understanding the life cycle of ESI is now an important part of the practice of law and assists counsel and clients in navigating risks, mitigating the high costs of discovery and ensuring admissibility in court.
- EDRM: The Electronic Discovery Reference Model at the Duke Law Center for Judicial Studies, creates resources for improving e-discovery and information governance.

14

The EDRM Model



https://www.edrm.net/frameworks-and-standards/edrm-model/edrm-wall-poster/

15

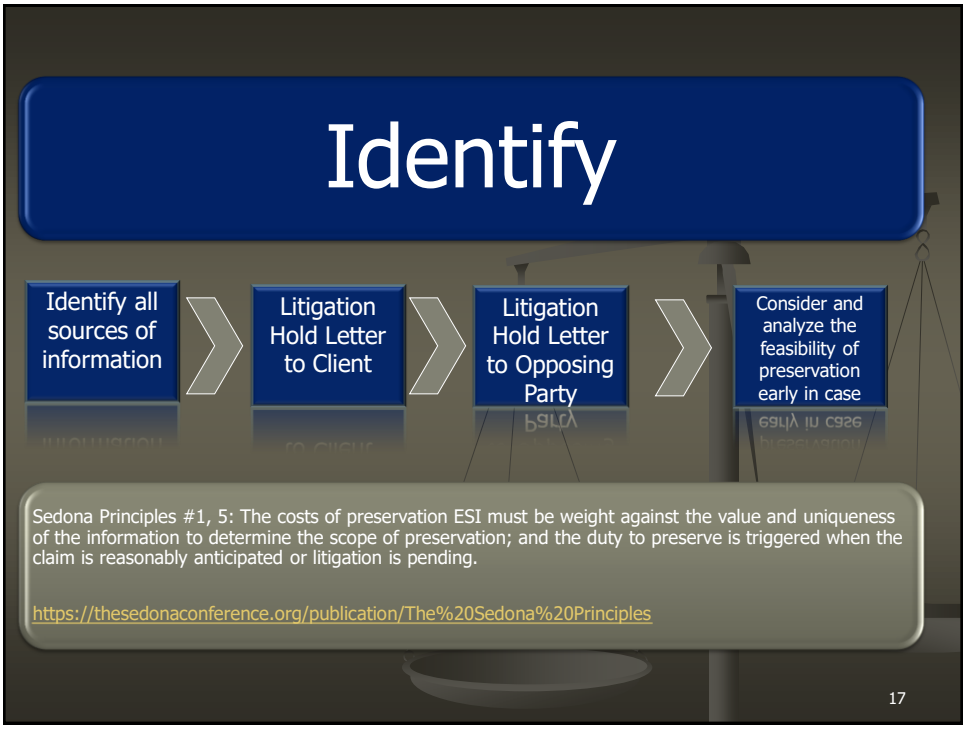
Information Governance

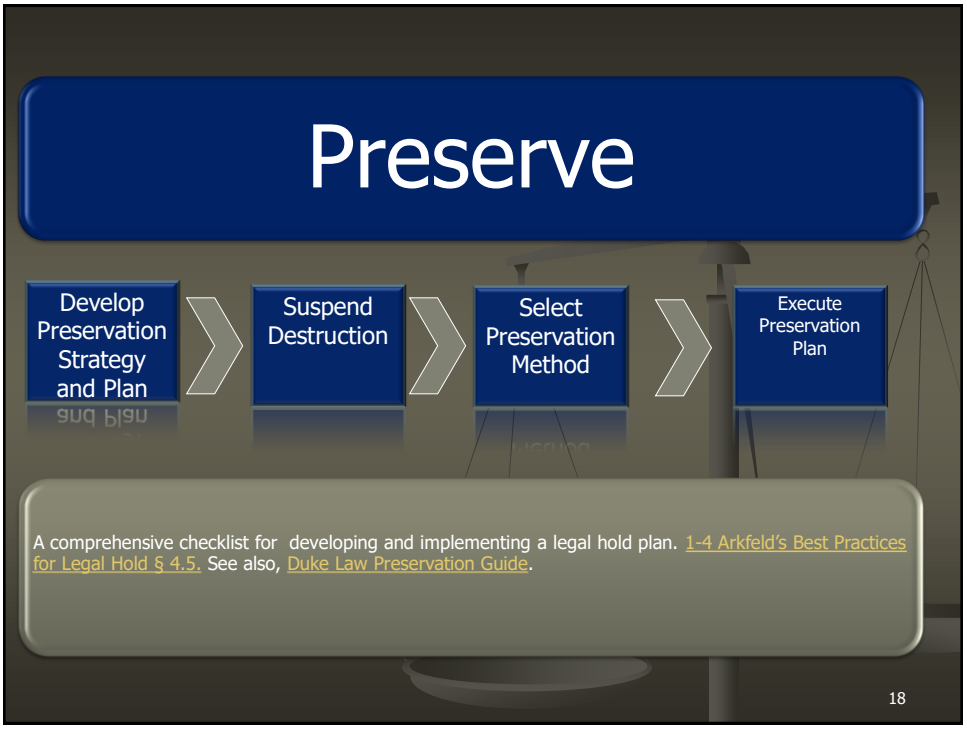
Business Users → Legal, risk and regulatory departments → IT Organizations

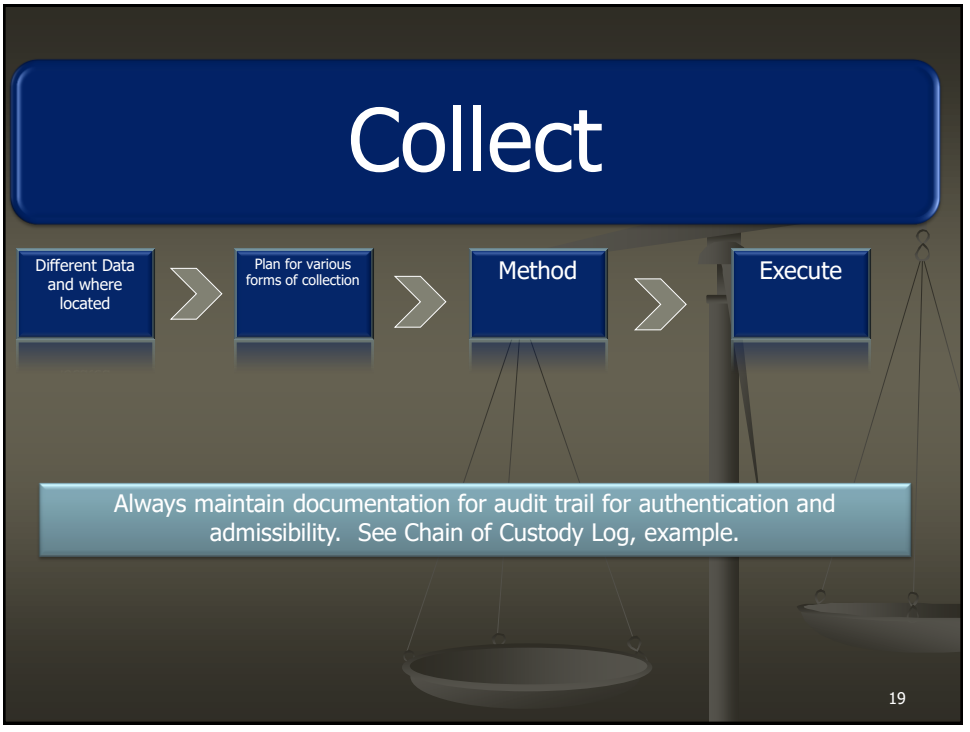
Outside legal counsel can play a key role in validating best practices for how a company—including the law firm—governs its information. Working with the groups that manage the information (set forth above) can get a company's ESI house in order prior to litigation.

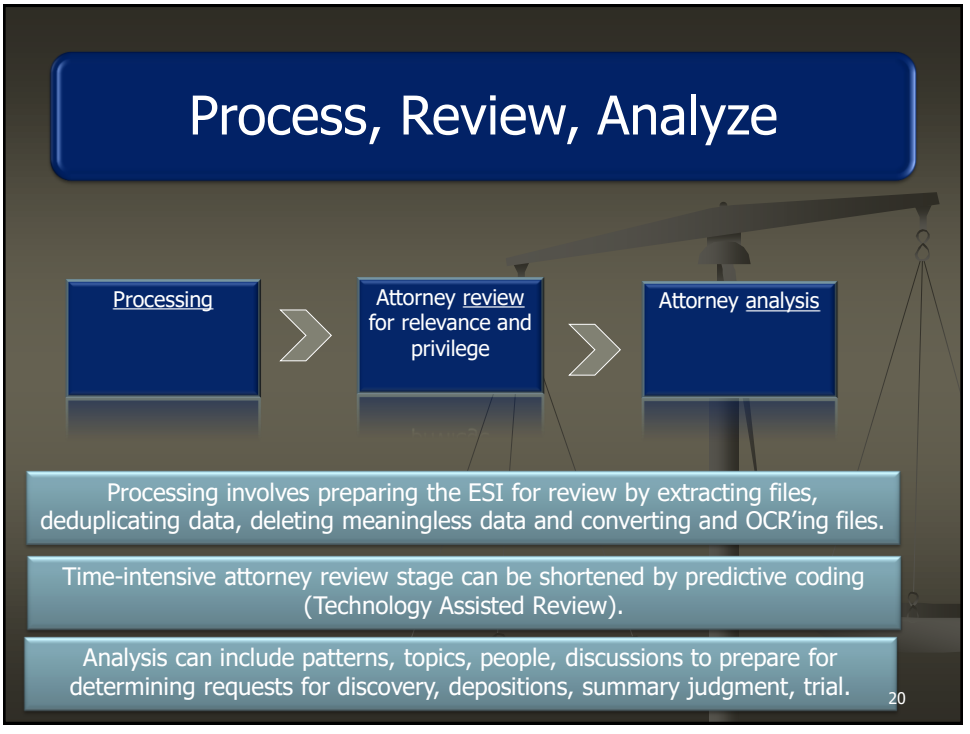
What are the company's document retention/destruction policies, what is the information cycle, does the business have a legal hold tracking system, a data loss prevention system, is the information in the cloud or on a server, social media policies, BYOD policies and their permissible use, identifying the records managers, technology providers and other personnel to ensure that they, too, are following and implementing the policies. *See* Fed.R.Civ.P. 1 and ABA Model Rule 1.1: requiring the attorney to keep abreast of how the benefits and risks associated with relevant technology affect the law and its practice.

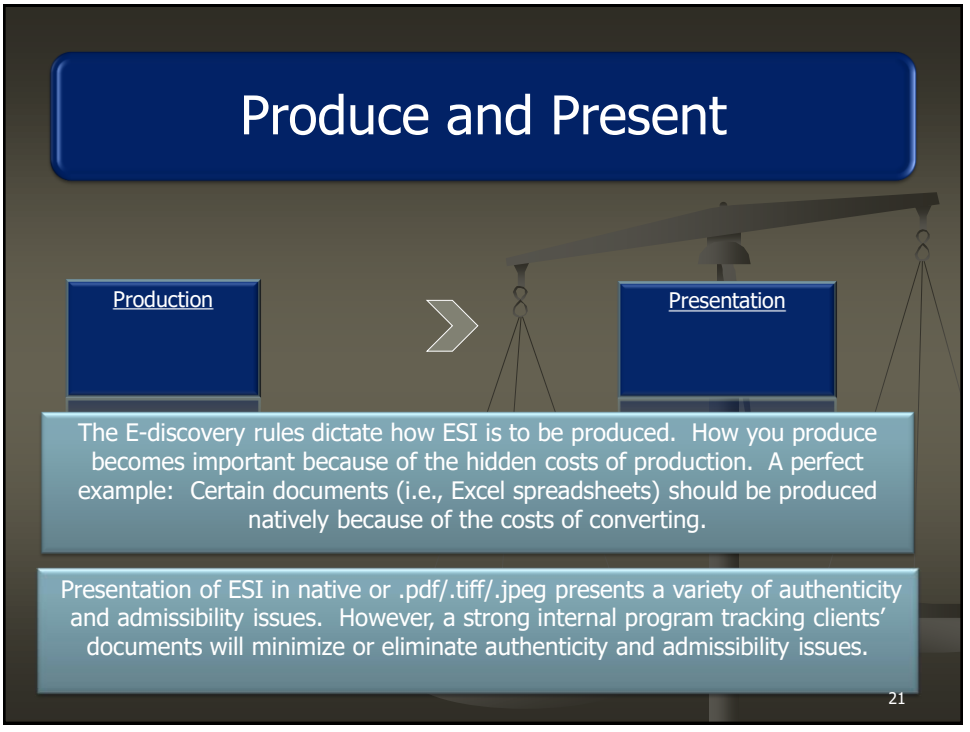
16

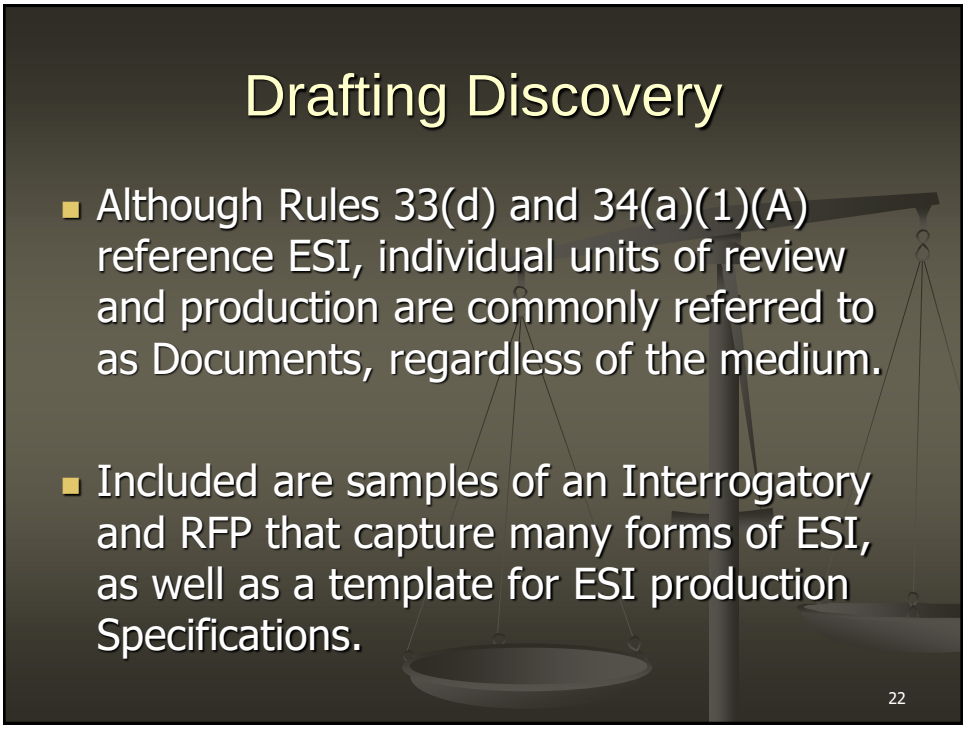

Identify
Identify all sources of information
Litigation Hold Letter to Client
Litigation Hold Letter to Opposing Party
Consider and analyze the feasibility of preservation early in case
Sedona Principles #1, 5: The costs of preservation ESI must be weight against the value and uniqueness of the information to determine the scope of preservation; and the duty to preserve is triggered when the claim is reasonably anticipated or litigation is pending.
https://thesedonaconference.org/publication/The%20Sedona%20Principles
17


Preserve
Develop Preservation Strategy and Plan
Suspend Destruction
Select Preservation Method
Execute Preservation Plan
A comprehensive checklist for developing and implementing a legal hold plan. 1-4 Arkfeld's Best Practices for Legal Hold § 4.5. See also, Duke Law Preservation Guide.
18


Collect
Different Data and where located
Plan for various forms of collection
Method
Execute
Always maintain documentation for audit trail for authentication and admissibility. See Chain of Custody Log, example.
19


Process, Review, Analyze
Processing
Attorney review for relevance and privilege
Attorney analysis
Processing involves preparing the ESI for review by extracting files, deduplicating data, deleting meaningless data and converting and OCR'ing files.
Time-intensive attorney review stage can be shortened by predictive coding (Technology Assisted Review).
Analysis can include patterns, topics, people, discussions to prepare for determining requests for discovery, depositions, summary judgment, trial.
20


Produce and Present
Production
Presentation
The E-discovery rules dictate how ESI is to be produced. How you produce becomes important because of the hidden costs of production. A perfect example: Certain documents (i.e., Excel spreadsheets) should be produced natively because of the costs of converting.
Presentation of ESI in native or .pdf/.tiff/.jpeg presents a variety of authenticity and admissibility issues. However, a strong internal program tracking clients' documents will minimize or eliminate authenticity and admissibility issues.
21


Drafting Discovery
Although Rules 33(d) and 34(a)(1)(A) reference ESI, individual units of review and production are commonly referred to as Documents, regardless of the medium.
Included are samples of an Interrogatory and RFP that capture many forms of ESI, as well as a template for ESI production Specifications.
22

Rule 45 Subpoenas and ESI

- Nonparty subpoenas raise important issues related to ESI.
  - Provides opportunities for "testing or sampling" ESI.
  - Subpoena should specify form of ESI Production; otherwise, they can be produced in a form ordinarily maintained or in a reasonably usable form or forms.
  - The "one bite" rule in 45(d)(1)(C) protects a nonparty from having to produce the same ESI in more than one form.
  - Rule 45(d)(1)(D) contains a two-tiered limitation on ESI production if the sources are "not reasonably accessible because of undue burden or cost," and subject to a showing of "good cause."
  - The "claw back provision" is available for inadvertent disclosure. Rule 45(d)(2)(B), Fed.R.Civ.P.

23

Responses to Discovery: Don't Use Boilerplate

- Boilerplate Responses violate the specificity requirements of Rule 34, Fed.R.Civ.P. *Fisher v. Forrest, No. 1:2014cv01304, opinion dated February 28, 2017 (S.D.N.Y., 2017);*
- The 2015 amendments deleted "likely to lead to the discovery of relevant, admissible evidence." This language and "overly broad and unduly burdensome" should be removed from every form.

24

Rule 502: Attorney-Client Privilege and Work Product

- Rule 502(d): "**Controlling Effect of a Court Order.** A federal court may order that the privilege or protection is not waived by disclosure connected with the litigation pending before the court — in which event the disclosure is also not a waiver in any other federal or state proceeding."
- Rule 502(b): Inadvertent Disclosure does not operate as a waiver if it is truly inadvertent, the holder of the privilege took reasonable steps to prevent disclosure, and the holder promptly took reasonable steps to rectify the error.

25

Privilege Waivers and Careless Production

- Practice Tips:
  - Address the Rule 502 Order at the onset of your case and have it in place. See, e.g., In re Qualcomm Litigation, 2:17-CV-00108-GPC-MDD. (Apple waived its privilege because it could not show that it took any steps to prevent disclosure under Rule 602(b)(2).
  - Irth Sols., LLC v. Windstream Commc'ns LLC, No. 2:16-CV-219, 2017 WL 3276021, at *16 (S.D. Ohio Aug. 2, 2017)(claw back agreement was ambiguous and deficient and privilege waived as to those documents but not subject matter waiver. Counsel is the "guardian" of the waiver and the court will hold counsel accountable when the normal inadvertent waivers become "chasms.")
  - We have provided examples of 502 Orders.

26

Evidentiary Considerations

- Proportionality is now a requirement for permissible discovery. Relevancy is no longer enough. *In re Bard IVC Filters Prod. Liab. Litig.*, 317 F.R.D. 562, 564 (D. Ariz. 2016).
- The 2015 amendments, however, do not change the parties' responsibilities.
- Rather, "[t]he parties and the court have a collective responsibility to consider the proportionality of all discovery and consider it in resolving discovery disputes." *Id.*

27

Meet and Confer

- The Rule 26 e-discovery amendments Rules 26(a) and (f), Fed.R.Civ.P. require the parties to meet and confer, discuss issues regarding preserving discoverable information, form of production and privilege waivers.
- The Case Management Order should formalize the parties' ESI requirements.

  Model Joint Discovery Management Order, included.

28

Meet and Confer

- Rule 16 (b) Scheduling Order includes provisions for disclosure, discovery or preservation of ESI.
- A party should try to understand the opposing party's computer system and request expedited disclosure of computer information. *See also Rule 26(d) and (e), Fed.R.Civ.P.*

29

MIDP

- The Judicial Conference of the United States has authorized a **Mandatory Initial Discovery Pilot** (MIDP) Project to test robust initial discovery. Only two states, at present. Arizona and N.D. Illinois.
- Counsel must **pounce** on all aspects of discovery at the first meeting with the client and identify the sources of documents, send out litigation hold letters, prepare early and ensure the client and opposing party are complying. See Sample Acknowledgement of Hold and Compliance, attached.

30

Hearsay Rule 801

- When is ESI a Statement ?
  - A "statement" is (1) an oral or written assertion or (2) nonverbal conduct of a person, if it is intended by the person as an assertion. Rule 801(a).
  - Made by the "declarant" as "a person who makes a statement." Rule 801 (b).

31

"Statement" Offered by the "Person"

- While requirements of hearsay are often overlooked in the traditional documentary evidence, when it comes to ESI, the question of whether something is a statement offered by a person, is all the more complex.
  - Neither the header nor the text of a fax was hearsay. *United States v. Khorozian*, 333 F.3d 498, 506 (3d Cir.2003).
  - Images and text found on the websites "are not statements at all—and thus fall outside the ambit of the hearsay rule." *Telewizja Polska USA, Inc. v. Echostar Satellite Corp.*, 2004 WL 2367740, at *5 (N.D. Ill. Oct. 15, 2004).

32

Computer-Generated Information

- When a document contains only "computer generated information" and not the repetition of prior recorded human input or observation, there is no "out-of-court asserter."
- Where records are generated by computer, traditional hearsay principles do not apply.
- Scientific advances of modern technology have enabled devices to make and record the occurrence of electronic events. Computer-generated records of a business are more appropriately analyzed as a scientific test for purposes of determining **admissibility.**

Chewning v. Commonwealth, 2014 Va. App. LEXIS 82, *1, 2014 WL 931053

33

"Statement" offered as an Assertion"

- "Read" and "Received" Receipts.
  - In a case against a former supervisor, plaintiff (lieutenant) sued former employer for violations of Title VII of the Civil Rights Act for a hostile work environment. After discovery, defendants sought an MSJ and moved to strike plaintiff's affidavit on admissibility grounds.
  - A read receipt sent from defendant's email address to plaintiff was triggered when an email was opened. Plaintiff claimed the Read Receipt was "unauthenticated hearsay."
  - The Judge ruled that FRE 801(a)'s definition that a statement must be 'intended . . . as an assertion' and found it "questionable that the Read Receipt was intended to be assertive." Fox v. Leland Vol. Fire/Rescue Dept. Inc., *638 Fed.Appx. 290, 129 Fair Empl.Prac.Case (BNA) 87* 7:12-CV-354-FL. (E.D.N.C. Mar. 10, 2015).

34

Is ESI being Offered for its Substantive Truth?

- Rule 801(c): "Hearsay is a statement, other than one made by the declarant while testifying at the trial or hearing, ***offered in evidence to prove the truth of the matter asserted.***" (emphasis added).
  - **Note**: where evidence may be hearsay if not offered for a particular purpose beyond the truth of the statement, it is imperative that you articulate the non-hearsay purpose for which e-mails and other electronic information is offered.

35

Examples under 801(c)

- E-mail between defendant and co-worker not hearsay because not offered to prove truth but to show existence of a relationship between defendant and co-worker and that it was customary for them to communicate by e-mail. *United States v. Siddiqui*, 235 F.3d 1318, 1323 (11th Cir. 2000).
- Email from lobbyist to Defendant not hearsay not offered to prove truth but the nature of the lobbyist's work on behalf of client. *United States v. Safavian*, 435 F. Supp. 2d 36, 44 (D.D.C. 2006).
- "Many courts conclude that an electronically generated record that is solely the creation of a computerized system or process is not hearsay." See, e.g., Jonathon L. Moore, TIME FOR AN UPGRADE: AMENDING THE FEDERAL RULES OF EVIDENCE TO ADDRESS THE CHALLENGES OF ELECTRONICALLY STORED INFORMATION IN CIVIL LITIGATION, 50 Jurimetrics J. 147, 167 (2010).

36

ESI's Exclusion from hearsay Fed.R.Evid. 801(d)

- Rule 801(d)(1) identifies three types of prior statements by witnesses who testify and are subject to cross examination that are excluded from the definition of hearsay.
- Similarly, Rule 801(d)(2) establishes five types of admissions by a party opponent that are also excluded from the definition of hearsay.
  - ESI has been found to qualify as admissions by a party opponent. *Siddiqui,* 235 F.3d at 1323 (e-mail authored by defendant was an admission); *Safavian,* 435 F.Supp.2d at 43–44 (e-mail sent by defendant was an admission); *Telewizja Polska USA,* 2004 WL 2367740 (N.D.Ill. Oct.15, 2004) (website exhibits admission against interest).

37

ESI Exceptions under Rules 803, 804, 807

- Rule 803(1):

Present sense impression. A statement describing or explaining an event or condition made while the declarant was perceiving the event or condition, or immediately thereafter.

  - Note: Given the modern world's focus on updating friends and strangers constantly on such platforms as Twitter, Instagram. Facebook, LinkedIn, Snap Chat, this exception is highly relevant to many types of electronic communication, whether e-mail or social media.

38

Rule 803(2) Excited Utterance

- "A statement relating to a startling event or condition made while the declarant was under the stress of excitement caused by the event or condition."
  - We have seen colleagues, friends, and family on their phones, handheld devices, and computers frantically typing away while we attempt to have a conversation with them or while witnessing an event. Because of this, under certain circumstances the excited utterance exception may apply to text and e-mail messages—something not seen with traditional "hard" documents.

39

Don't Rely On a Single Exception

- Example: E-mail from employee to boss about substance of telephone call with defendant in mail/wire fraud case qualified as a present sense impression (but not an excited utterance). *United States v. Ferber*, 966 F.Supp. 90 (D.Mass.1997).

40

Rule 803(3)

- "A statement of the declarant's **then existing state of mind, emotion, sensation, or physical condition…."**
- Given ESI's propensity for horrendous over shares and in-the-moment emotional displays, Rule 803(3) may allow admitting ESI such as electronic correspondence. *See e.g., Safavian*, 435 F.Supp.2d at 44 (admitting e-mail that contained statements of defendant's state of mind).

41

Rule 803(6): Business Records

Records of **regularly conducted activity**

- Prepared in the **normal course of business**;
- Made **at or near the time of the events** it records;
- Based on the **personal knowledge of a person with a business duty** to transmit the information; and
- Made in the regular course of a regularly conducted business activity, for which it was the regular practice of the business to maintain a memorandum.

42

Must be made for Business' Needs

- **Of Note:** For this exception to apply the business record must have been made for the business' needs, and not for the personal purposes of the person who made it.
- Business and personal work on business computers, phones, tablets, is all the more common and intermingled. As such, practitioners need to be cautious in analyzing electronic information, especially e-mails, as to whether the true purpose was for business or was instead personal.

43

Example: not in ordinary course

- Driver 1 filled out an SR1 form with DMV to report auto accident and DMV suspended the license of Driver 2, who demanded a formal hearing. While it was within the OCB for the DMV to prepare an SR1, it was not in the OCB for the driver to do so. SR1 was inadmissible. Matthew Bender Practice Guide, 1-15 MB Practice Guide: CA E-Discovery and Evidence 15.25 (2017)

44

Email Chains as Business Records

- This exception under Rule 803(6) can lead to admission of multiple levels of hearsay present in things such as **e-mail chains**: *State of New York v. Microsoft,* 2002 WL 649951 (D.D.C. Apr. 12, 2002) (when the maker "as well as every other participant in the chain producing the record are, acting in the regular course of [the] business.").
- Every participant in the email chain must have generally been acting in the course of regularly conducted business. Rambus Inc. v. Infineon Tech. AG, 348 F.Supp.2d 698, 706 (E.D.Va.2004).
- An email chain prepared by an employee may not be a qualified business record where employer did not require employee to send and maintain emails summarizing a phone call after the call was made. *State of New York v. Microsoft,* 2002 WL 649951 (D.D.C. Apr.12, 2002).

45

Retrieval from Computer Files

- The ESI retrieved from computer files must be the same one as originally had been entered into its computer.
- "In the case of a paper record, the inquiry is into the procedures under which the file is maintained, including custody, access, and procedures for assuring that the records in the files are not tampered with. The foundation is well understood and usually is easily established. *See* EDWARD J. IMWINKELRIED, EVIDENTIARY FOUNDATIONS § 4.03[1] (5th ed. 2002); 5 WEINSTEIN § 900.07[1] [b] [i]; American Exp. Travel Related Servs. v. Vinhnee (In re Vinhnee), 336 B.R. 437, 444-445, 2005 Bankr. LEXIS 2602, *13-14.
- The same is true for ESI: the entity's policies and procedures for the use of the equipment, database, and programs, how the database is controlled and how the original program was accessed are important questions. Changes to the database, was it backed up, logged, recorded, audited, all become important in determining the originality of the ESI.

46

Retrieval from Computer Files

- Courts, however, may determine that the ESI presented may more appropriately be directed to the weight a jury would give to the evidence, not its authenticity.
- Possibility of alteration does not and cannot be the basis for excluding emails as unidentified or unauthenticated as a matter of course. *United States v. Safavian*, 435 F.Supp.2d 36, 40–41 (D.D.C.2006).
- Foundation for a computer generated business record did not require the maker of the record, or custodian; a witness qualified to explain the record keeping system of organization is enough. *United States v. Kassimu*, 2006 WL 1880335 (5th Cir.2006).
- Computerized check-in and reservation records admissible as business records; data reflected in the printouts was kept in the ordinary course of the business. *United States v. Fujii*, 301 F.3d 535 (7th Cir.2002).

47

Rule 803(8): Public Records and Reports

- Records, reports, statements, or data compilations, in any form, of public offices or agencies….
- Courts apply a more deferential treatment toward electronic public records. *See, e.g., EEOC v. E.I. DuPont de Nemours and Co.,* 2004 WL 2347556 (E.D. La. Oct. 18, 2004); *Lester v. Natsios,* 290 F.Supp.2d 11 (D.D.C.2003).
- Computerized records of a governmental agency may be presumed trustworthy. *United States v. Oceguerra–Aguirre*, 70 Fed.Appx. 473 (9th Cir.2003) (burden on the party challenging records to establish untrustworthiness.)

48

Rule 803(16): Ancient Documents Does it Apply to ESI?

- Documents normally excluded as hearsay are admissible if the document is at least twenty years old, and if the party offering the document can show that the document is "genuine," or authentic.
- *The first email may have been as early as: 1965*
- *The first website: 1991*
- *The first retrievable webpage: 1992*
- *So as ESI ages, will all easily retrievable data be potentially admissible simply because they are old?*
- *They still must be authenticated.*

Capra, Daniel J. Electronically Stored Information and the Ancient Documents Exception to the Hearsay Rule: Fix it Before People Find out About it, 17 Yale J. L. & Tech. 1, 2 (2015)

49

Authentication Rule 901

- Proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.
- ESI must be treated just as any other form of documentary evidence.
- To authenticate a document, the proponent must present evidence to demonstrate that the document is what the proponent claims it to be. *People v. Watkins*, 2015 IL App (3d) 120882, 25 N.E.3d 1189 (App. 2015).

50

ESI Requires Authentication

- Electronic records require authentication to be admitted. *United States v. O'Keefe*, 537 F. Supp. 2d 14, 20 (D.D.C. 2008) ("[a] piece of paper or electronically stored information, without any indication of its creator, source, or custodian may not be authenticated under Federal Rule of Evidence 901"); see also, 1-8 Arkfeld on Electronic Discovery and Evidence § 8.11

51

Authentication Methods

- Rule 901(b)(4) through distinctive characteristics and circumstantial evidence. Capra, Daniel J. *Electronically Stored Information and the Ancient Documents Exception to the Hearsay Rule: Fix it Before People Find out About it*, 17 Yale J. L. & Tech. 1, 2 (2015), *citing* United States v. Lundy, 676 F.3d 444, 454 (5th Cir. 2012).
- Rule 901(b)(7) through showing the record from an office where items of this kind are kept. *Id., citing* *United States v. Meienberg*, 263 F.3d 1177, 1181 (10th Cir. 2001); *United States v. Catabran*, 836 F.2d 453, 458 (9th Cir. 1988).
- Rule 901(b)(9) showing the product of the system has an accurate result. *Id.*

52

Focus on the Internet

- Three common forms of internet data often offered into evidence:
- Data that a website owner posts onto his/her own website
  - Must introduce evidence sufficient for a juror to attribute ownership of a specific webpage to a party. *United States v. Vayner*, 769 F.3d 125 (2nd Cir. 2014).
- Data that people post onto a website not owned by them, with the website owner's consent
- Data posted onto a website without the website owner's consent

53

Ways to Establish Authentication

- Appearance, contents, substance, internal patterns or other distinctive circumstances; See Commentary to Rule 901(b)(4)
- Witness Testimony (901(b)(1));
- Self-authentication;
- Webmaster;
- Content Provider.

54

Authentication Methods for Websites

- Websites can be authenticated using the "wayback machine," which archives copies of websites every few weeks. https://archive.org/web/
- In *Marten Transport Ltd. V. For Platform Advertising*, Case No. 13-2464 (D. Kans. April 29, 2016), the Court found that screenshots from the defendant's website could be authenticated. In fact an expert was not necessary. https://www.bloomberglaw.com/public/desktop/document/Marten_Transp_Ltd_v_PlattForm_Adver_Inc_No_142464JWL_2016_BL_1371?1462657373

55

Authentication Methods for Websites

- Internet screenshots may be authenticated by a declaration that the screenshots were taken by the individual on a specified date and that they are true and correct depictions of the named web addresses. *Sam's Riverside, Inc. v. Intercon Sols., Inc.*, 790 F. Supp. 2d 965, 978 (S.D. Iowa 2011).
- However, this only authenticates the existence of the content on the screenshot, it does not authenticate the content itself.

56

Email Authentication

- Regarding email and online chat room exhibits, "[t]he testimony of a witness with knowledge that a matter is what it is claimed to be is sufficient to satisfy this [reasonably likely] standard." *United States v. Gagliardi*, 506 F.3d 140, 151 (2d Cir. 2007).
- FRE 409(b)(4) permits email authenticity by referring to its "appearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances."

57

Rule 409 and Email Authentication

- Email **received by or sent to** a particular person may be authenticated by circumstantial evidence including:
  - Party opponent's production;
  - Subsequent messages in the email chain indicating the sender or recipient sent or received the email;
  - The addressee sent a reply;
  - Testimony that the email accurately and fairly depicts the correspondence;
  - Email address is the same as in other emails sent or received by the same person;
  - Nickname;
  - Sender would have had exclusive (or almost exclusive) knowledge about email contents.
  - Witness testimony that defendant spoke to them about email contents. *U.S. v. Siddiqui*, 235 F.3d 1318 (11th Cir. 2000).

58

Chat Rooms, other electronic based Messages

- Foundation for Chat Rooms and other electronic based messages:
  - screen name used when participating in chat room conversations (either generally or at the site in question);
  - when a meeting with the person using the screen name was arranged, the individual showed up;
  - the person using the screen name identified [himself] as the [person in the chat room conversation];
  - the individual had in [his] possession information given to the person using the screen name; and
  - the hard drive of the individual's computer had evidence of use.

Saltzburg, Michael M. Martin & Daniel J. Capra, Federal Rules of Evidence Manual at § 901.02[9].

59

Electronic Messages (other than Email)

- A defendant's objection to government admission of text messages based upon authenticity was overruled because there was enough circumstantial evidence to support admission and the jury could decide authenticity. *Ariz. V. Damper*, 225 P.3d 1148 (App. 2014).

60

Electronic Messages (other than Email)

- Objection under Rule 901(b)(2-5) that exhibit offered could not be attributed to Defendant's handwriting or voice, the Court admitted the Chat Room printouts as they were properly authenticated by Defendant through email address. *United States v. Simpson*, 152 F.3d 1241, 1250 (10th Cir. 1998).
- Printed contents of a Facebook page were properly authenticated when plaintiff acknowledged herself as owner and author of her page in her deposition. *Targonski v. City of Oak Ridge*, 921 F. Supp. 2d 820, 834 (E.D. Tenn. 2013).

61

Authentication of Admissibility of Computer Generated Records

- Eleven-part Test for Authentication:
  - 1. The business uses a computer.
  - 2. The computer is reliable.
  - 3. The business has developed a procedure for inserting data into the computer.
  - 4. The procedure has built-in safeguards to ensure accuracy and identify errors.
  - 5. The business keeps the computer in a good state of repair.
  - 6. The witness had the computer readout certain data.
  - 7. The witness used the proper procedures to obtain the readout.
  - 8. The computer was in working order at the time the witness obtained the readout.
  - 9. The witness recognizes the exhibit as the readout.
  - 10. The witness explains how he or she recognizes the readout.
  - 11. If the readout contains strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact.

American Exp. Travel Related Servs. v. Vinhnee (In re Vinhnee), 336 B.R. 437, 444-445 (9th Cir. BAP 2005).

62

Authentication Under Rule 901(b)(4)

- Examination of Metadata: "contextual, processing, and use information needed to identify and certify the scope, authenticity, and integrity of active or archival electronic information or records." Sedona Conference Guidelines.
- Examples of ESI Metadata: file name, location (e.g., directory structure or pathname), file format, type, size, dates (e.g., creation date, date of last data modification, date of last data access, and date of last metadata modification), and file permissions (e.g., who can read the data, who can write to it, who can run it). See, e.g., Federal Judicial Center, *Managing Discovery of Electronic Information: A Pocket Guide for Judges,* Federal Judicial Center (2007); Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 547, 2007 U.S. Dist. LEXIS 33020, *49-50, 73 Fed. R. Evid. Serv. (Callaghan) 446.

63

Authentication Under Rule 901(b)(4)

- It may not be enough to have an affidavit from an e-discovery expert responsible for data collection, if that person was not the actual custodian and could only speak to data collection procedures.
- For authentication of evidence, the court need not determine that the evidence is necessarily what the proponent claims, but only that there is sufficient evidence that the jury might ultimately do so.
- Email messages between two defendants in a healthcare fraud cause were sufficiently authenticated by government witnesses who performed billing services for defendants' lab and could corroborate email addresses with defendants' characteristics.

United States v. Bertram, 250 F. Supp. 3d 638 (D. E.D. Ky 2017)

64

Hash Files as Authentication

- "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances." Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 546-547, 2007 U.S. Dist. LEXIS 33020, *46-48, 73 Fed. R. Evid. Serv. (Callaghan).
  - **Hash Values** are unique numerical identifiers assigned to a file, a group of files, or a portion of a file, based on a standard mathematical algorithm applied to the characteristics of the data set.

65

Authentication and Identification Rules 902, Fed.R.Evid.

- Rule 902: Effective December 1, 2017, there are new documents that are "self-authenticating," including:
  - (13) Certified Records Generated by an Electronic Process or System; and
  - (14) Certified Data Copied from an Electronic Device, Storage Medium, or File. Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent also must meet the notice requirements of Rule 902(11).

66

Authentication Failures for ESI: Don't Make these Mistakes

- Proponent failed properly to authenticate exhibits of electronically stored business records. *In re Vinhnee*, 336 B.R. at 437;
- Proponent failed to authenticate exhibits taken from an organization's website. *United States v. Jackson*, 208 F.3d 633, 638 (7th Cir.2000);
- Affidavits used to authenticate exhibits showing content of web pages were factually inaccurate and affiants lacked personal knowledge of facts. *St. Luke's Cataract and Laser Institute PA v. Sanderson*, 2006 WL 1320242, at *3–4 (M.D.Fla. May 12, 2006);
- Objection sustained to witness affidavit offered to authenticate exhibit that contained documents taken from defendant's website. Affiant lacked personal knowledge. *Wady v. Provident Life and Accident Ins. Co. of Am.*, 216 F.Supp.2d 1060 (C.D.Cal.2002);
- Proponent of computer records failed to show that they were from a system capable of producing reliable and accurate results. *Indianapolis Minority Contractors Assoc., Inc. v. Wiley*, 1998 WL 1988826, at *7 (S.D.Ind. May 13, 1998).

67

Original Writing and Best Evidence Rule 1001, Fed.R.Evid.

- Original writing rule has particular applicability to electronically stored information.
- Computer based business records are comprised of material originally produced on a computer, through a variety of software programs.
- Admissibility of computer-based records may require a duplicate of the data or an image file if there is a question on the original source.

68

Rule 1001, Fed.R.Evid.

- Under Rule 1001(d) the "original" of information stored in a computer is the readable display of the information on the computer screen, the hard drive or other source where it is stored, as well as any printout or output that may be read, so long as it accurately reflects the data.

69

Rule 1002, Fed.R.Evid.

- To prove the content of a writing, recording, or photograph, the **original** writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of Congress.
  - Printouts of text messages cut and pasted by an officer onto a word-processing program were admitted. The Appellate Court agreed that, under the original writing rule, an original was required; however, the Court still found the officer's version was acceptable under the "best evidence" Rule because it could be the best evidence of the "conversations" between the defendant and the officer. *Laughner v. State*, 769 N.E.2d 1147 (Ind.Ct.App.2002), *abrogated on other grounds by Fajardo v. State,* 859 N.E.2d 1201 (Ind.2007).

70

Failure to Object under Rule 1002 Could Lead to Waiver

- Failure to properly object to introduction of evidence in violation of the original writing rule could result in a waiver of the error on appeal. *See* State v. Braidic, 119 Wash.App. 1075, 2004 WL 52412 (2004)(Defendant convicted of sex offenses with minor. At trial, victim's mother testified, without objection, to content of chat room text messages between defendant and victim. Appellate court noted applicability of original writing rule to require original to prove the contents of the chat room records, but found that defense counsel's failure to object did not constitute ineffective assistance of counsel).

71

Rule 1004, Original Gone

- The original is not required, and other evidence of the contents of a writing, recording, or photograph is admissible if—

(1) Originals lost or destroyed. All originals are lost or have been destroyed, unless the proponent lost or destroyed them in bad faith; or

(2) Original not obtainable. No original can be obtained by any available judicial process or procedure; or

(3) Original in possession of opponent;

(4) Collateral matters. The writing, recording, or photograph is not closely related to a controlling issue.

72

Expert Witnesses

- In 2010, Rule 26 of the Federal Rules of Civil Procedure governing expert witness discovery went into effect.
- Rule 26 no longer allows full discovery of draft expert reports or broad disclosure of communications between attorneys and expert witnesses, as had been the case since 1993. Instead, draft expert reports and communications between counsel and expert witnesses are now protected by the work-product doctrine. While prohibiting discovery of draft expert reports and significantly limiting discovery of Attorney-Expert communications, Rule 26 continues to require full disclosure of the expert's opinions and the facts or data used to support them.
- The 2010 amendment to Rule 26(a)(2)(C) mandates counsel-prepared disclosures for **non-reporting experts** that must include: "(i) the subject matter on which the witness is expected to present evidence under Federal Rule of Evidence 702, 703, or 705; and (ii) a summary of the facts and opinions to which the witness is expected to testify."

73

Forensic Expert Witnesses

- Admissibility of forensic experts
  - They preserve and analyze electronic data
  - They can be used as expert witnesses, litigation
  - Use the standard in *Daubert v. Merrell Dow Pharmaceuticals Inc.,* 509 U.S. 579, 595 (1993) and its progeny and Rule 702, Fed.R.Evid. on forensic experts.

74

Disclosure of Facts or Data of Expert

- Rule 26(a)(2)(B)(ii) has been amended to require **disclosure of the "facts or data" considered by the expert witness**. *Yeda Research & Dev. Co. v. Abbott GmbH & Co. KG*, 292 F.R.D. 97 (D.D.C. 2013). Other information is no longer necessary to disclose.
- But beware of the communications between client and expert and counsel and expert. *Dongguk Univ. v. Yale Univ.*, 2011 WL 1935865 (D. Conn. May 19, 2011) (communications with counsel were "either facts or assumptions, provided by attorney and relied on by [the expert] in forming her opinion" and had to be disclosed).
  - Emails between counsel and Expert should remain neutral, as should they between Expert and client to avoid any possibility that they should be disclosed;
  - A privilege log should be maintained of any and all emails between client and expert and attorney and expert.

75

Minimize the Firm's and Client's Exposure by Tackling ESI Immediately

- **Multiple Sources for E-Discovery Sanctions.**
  - Rule 26(g) – failure to conduct a reasonable inquiry;
  - Rule 37(e) – spoliation of ESI;
  - Rule 37(b)(2) – violating a court order and a judge's inherent authority are all possible ways a court can sanction you.

76

Do Not Delegate E-Discovery Duties to Your Client

- Ask client whether they have litigation hold in place, whether they have gathered ALL documents, and be proactive in your investigation and due diligence. See, e.g., *Brown v. Tellermate Holdings Ltd.,* 2014 WL 2987051 (S.D. Ohio July 1, 2014) (Counsel has an "obligation to do more than issue a general directive to their client to preserve documents which may be relevant to the case. Rather, counsel had an affirmative obligation to speak to the key players at [the defendant] so that counsel and client together could identify, preserve, and search the sources of discoverable information.")

77

Sanctions: Failure to Preserve

Nuvasive, Inc. v. Madsen, Inc., No. 13cv2007, 2016 WL 305096 (S.D. Cal. Jan. 26, 2016).

- Nuvasive failed to prevent the destruction of text messages requested by Defendants.
- Under the new Rule 37(e), Fed.R.Civ.P., Plaintiff stated the Motion for Sanctions should be argued under the new rule, which requires intent to harm.
- The Court agreed and found Plaintiff at fault but did not find that it had intentionally failed to preserve text messages. Absent intent, the Court could not impose an adverse inference.
- The Court allowed the parties to present evidence to the jury regarding the loss of ESI and instructed the jury that it may consider such evidence.

78

Failure to Preserve Text Messages

- Waymo LLC v. Uber Techs., Inc., No. C 17-00939 WHA, 2018 WL 646701 (N.D. Cal. Jan. 30, 2018).
  - Uber attempted to minimize its paper trail by using "ephemeral" messaging (like Snapchat, Slack, WhatsApp, Messenger—in other words, messages that do not remain on the sender's or receiver's device).
  - Court issued a series of jury instructions to address Uber's failure to preserve text messages and other discovery misconduct.

79

Sanctions: Deletion of Instant Messages

Franklin v. Howard Brown Health Ctr., No. 17 C 8376, 2018 WL 4784668 (N.D. Ill. Oct. 4, 2018), report and recommendation adopted, No. 1:17 C 8376, 2018 WL 5831995 (N.D. Ill. Nov. 7, 2018)

- Workplace Discrimination and termination. During discovery Plaintiff sought Emails and text messages but DID NOT refer to instant messaging. And IMs were the primary source of harassment. They were destroyed as part of the regular and brief document management plan.
- Defendant failed to institute legal hold after trigger.
- Employees determined which data should be preserved
- Key employee computers wiped one week after lawsuit was promised.
- Sanctions may occur even without the intent to deprive.

80

Sanctions: Altering Emails

CAT3 LLC V. Black Lineage, Inc., 164 F.Supp.3d 488 (S.D.N.Y. Jan. 2016).

- Interpreting Rule 37, Fed.R.Civ.P., on a motion for sanctions as a result of plaintiffs altering emails in a trademark infringement case, the Magistrate Judge granted the Motion in part and barred the plaintiffs from using the altered versions of the emails at trial.
- The original ESI was lost and could not be adequately restored or replaced.
- Judge Francis declined to dismiss the case. Plaintiffs were precluded from relying on the subject emails, and were ordered to pay attorneys' fees and costs incurred by the defendants in establishing the spoliation and obtaining relief.

81

Sanctions: Plaintiff Altered Source Code

BMG Rights Management LLC v. Cox Communications, Inc., 199 F.Supp.3d 958, (E.D. Va. 2016).

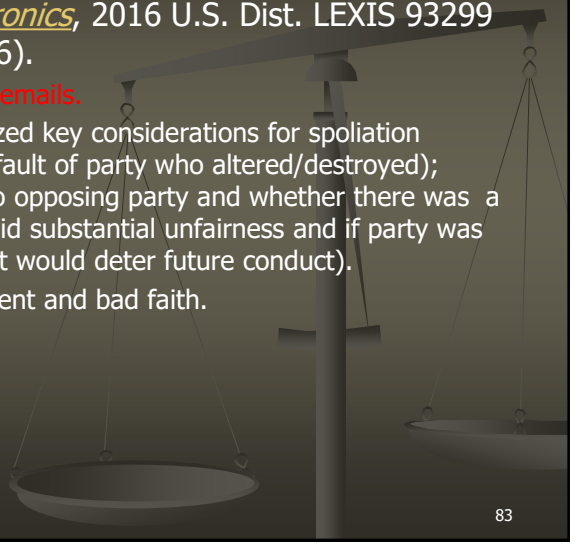
Plaintiff altered the source code of its system during the time of the dispute.

The Judge determined it was spoliation. The Judge granted sanctions, entering an order requiring that a permissive adverse inference instruction should be given to the jury, allowing but not requiring them to consider the absence of the earlier version of the source code.

82

Sanctions: Spoliation

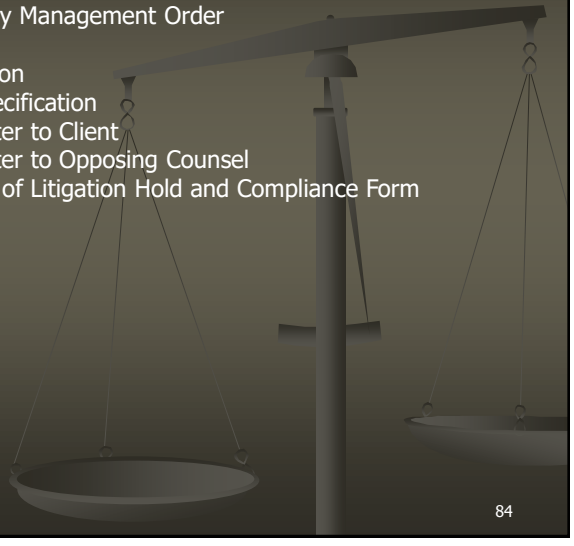
- *GN Netcom v. Plantronics*, 2016 U.S. Dist. LEXIS 93299 (D. Del. July 12, 2016).
  - Defendant destroyed emails.
  - Judge Stark summarized key considerations for spoliation sanctions (degree of fault of party who altered/destroyed); degree of prejudice to opposing party and whether there was a lesser sanction to avoid substantial unfairness and if party was severely at fault, what would deter future conduct).
  - Judge Stark found intent and bad faith.



83

Additional Forms

- Chain of Custody Form
- Sample Model Joint Discovery Management Order
- Sample Interrogatory
- Sample Request for Production
- Template ESI Production Specification
- Template Litigation Hold Letter to Client
- Template Litigation Hold Letter to Opposing Counsel
- Template Acknowledgement of Litigation Hold and Compliance Form
- The Sedona Principles
- Sample Rule 502 Orders



84