

Using ESI at Trial

Presented by:
George Bellas
www.bellas-wachowski.com

1

Why You are Here Today:

Illinois Code of Professional Responsibility

RULE 1.1. Competence

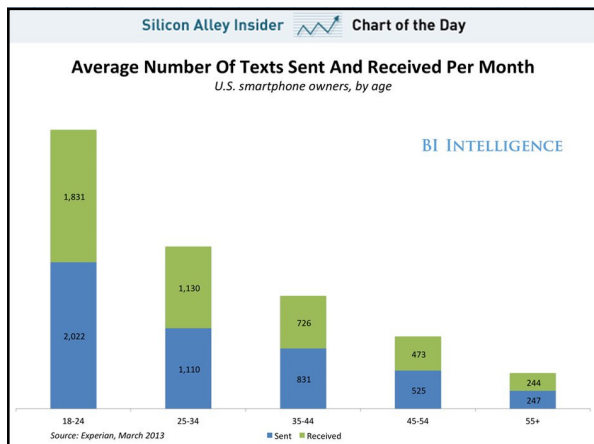
(a) A lawyer shall provide competent representation to a client. **Competent representation requires the legal knowledge, skill, thoroughness and preparation necessary for the representation.**

2

Comments to Rule 1.1 (added in 2015)

Comment 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.

3



Problem is growing: BIG DATA

- 2.5 quintillion bytes created each day:
 - 1,000,000,000,000,000 (10¹⁸)
 - Equals 2,500,000 Terabytes!
- 90% of the data in the world today has been created in the last 2 years alone.
- Data is generated everywhere:
 - Sensors used to gather climate information,
 - Posts to social media sites,
 - Digital pictures and videos,
 - Purchase transaction records,
 - Cell phone GPS signals Just to name a few.

5

Sources of ESI -Storage Devices:

- Desktop Computers/Hard Drives/Laptops
- Backup Tapes
- Portable Flash Drives, Floppy, Zip and Jaz Diskettes
- Optical Media - CDs, CD-Roms, DVDs
- Home Computers
- PDAs, Blackberry® smartphones and Cell Phones
- Digital Cameras and Flash Media
- Voicemail
- Fax Machines, Copiers and Printers
- iPod® and iPad® mobile digital devices, Kindle™ and Nook™ eReaders, etc.

6

Finding the Needle in a Growing Haystack



In the Digital World, think “ESI” not “documents”

- “Electronically Stored Information” (“ESI”) is discoverable information – **F.R.C.P. 34**
- ESI is subject to production under Rule 34(a)
- Under Rule 34(b) the form of production of ESI:
 - can be specified by the requesting party in a request, or
 - thereafter by a responding party in a response
 - but if you don’t specify, **it must be produced in the form in which is ordinarily maintained** (ie. as ESI)

ESI Examples:

- Emails
- Cell Photos & PDAS
- Voice Mail
- Online Business
- Instant Messages
- And much more... **any other data or data compilations stored in any medium that can be translated into a reasonably useable form (FRCP 34(a)).**

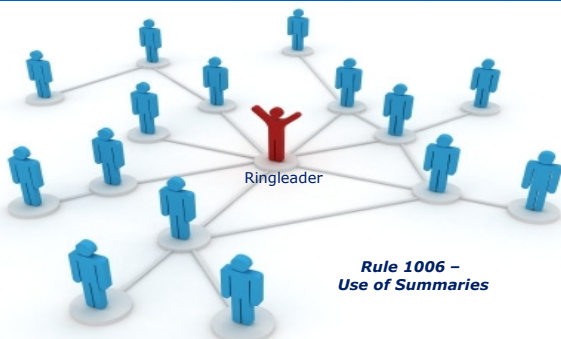


Finding the ESI

- **Thumb Drive** - 4 Gbyte
 - Given as promotional item
 - Holds 4 pickup trucks of printed text
- **Laptop/Desktop**
 - Holds up to a terabyte
- **Cell Phone**
 - 256 Gbytes of data
- **Cloud Storage**
 - Unlimited storage

10

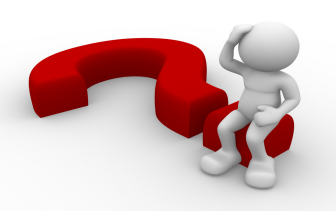
Linking Data for Evidence



Ringleader

*Rule 1006 -
Use of Summaries*

Metadata ??





Metadata – What is it?

Electronically stored data that describes characteristics of ESI, found in different places in different forms.
Can be supplied by applications, users or the file system.

Metadata can describe how, when and by whom ESI was collected, created, accessed, modified and how it is formatted.

- *The Sedona Conference Glossary: E-Discovery and Digital Information Management*

Metadata Defined

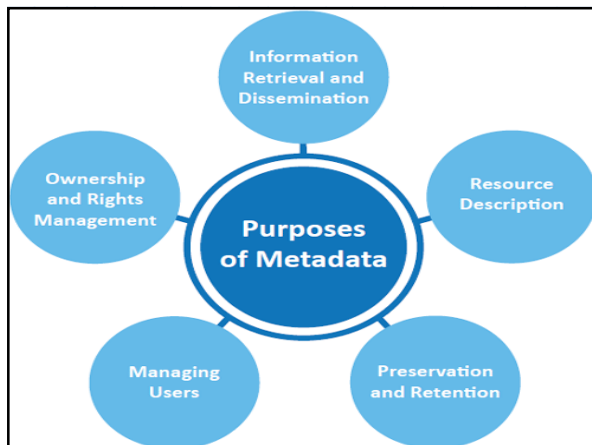
Sedona Guidelines Best Practices & Commentary defines **metadata** as:

- **Appendix F:** Information about a particular data set which describes how when and by whom it was collected creates accessed or modified and how it was formatted.
- **Appendix E:** All the contextual processing and use information needed to identify and certify the scope authenticity and integrity of active or archival electronic information or records.

Metadata: How Important Is It?

- It is important whenever lawyers send, produce or receive ESI containing metadata in response to a discovery request or subpoena.
- Useful when the history, tracking, or management of an electronic document matters.
- **We must get and produce the document in a form that maintains the metadata.**
 - *The Sedona Conference: Commentary on Ethics & Metadata*

16



Why Metadata is Important

- **Establish And Defend Against:**
 - Allegations Of Fraud/Forgery
 - Allegations Of Infringement
 - Allegations Of Spoliation
 - Motions For Sanctions and Adverse Inferences
- **Create Timelines:**
 - Who Knew What When
 - When Document Created and Modified
 - Who Created Document
 - When Document Was Sent

Metadata - ESI on ESI

- Computers contain and monitor a great deal of information about electronic files so that the system may locate them and manage the data.
- Information such as who last retrieved the file, when it was last modified, when and who created it, and which computer it was created on, is tracked and made accessible.
 - System Metadata, that is connected to, but not "in" the data itself.
 - Used by the computer to manage the file.
- **Copying the file, without taking the proper measures to preserve the current state of the metadata, can result in changing metadata that may have been essential, discoverable information.**

19

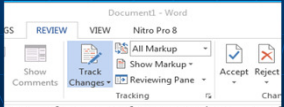
Important Metadata

- There are on average 3 files created for each ESI file:
 - (1) a machine readable text file possessing searchable text from original file,
 - (2) the image of what the text looks like should they be printed or even viewed, and
 - (3) the metadata from the original files.
- These files, and the actual image, make up the production.
 - Note: although the extra text and metadata files may NOT contain any evidentiary worth, they add ease of handling value to document management systems.
- What you want:
 - Dates (When),
 - Parent/Child relationships (attachments)(What)
 - Custodians/Authors (Who),
 - File Path/File Names (Where)

20

Metadata that is "Embedded"

- Data that the application itself monitors, that may or otherwise may not be detectable, depending on how the application is viewed.
 - i.e. Microsoft Word "track changes" mode, or "comments" mode.
- This information moves with the file when it is copied.
 - May or may not be discoverable, or pertinent.
 - Or Who made the last contract change?



21

E-Mails: Evidence

- May prove that a business-related event or activity did, or did not, occur.
- May identify participants in a business activity or who had knowledge of an event.
- May have legal or compliance value.
- May support facts that you claim to be true.

22

Introduction of E-Mail into evidence at trial

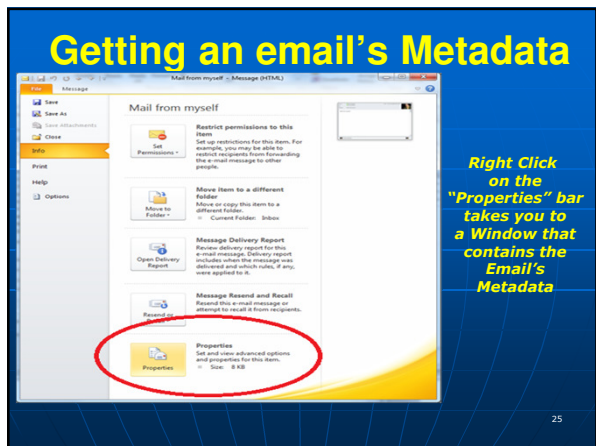
- A print out of an email is not the original.
- How is it authenticated?
- How is it admitted.
- The practical issue we need to address for trial is how do we introduce an email at trial.

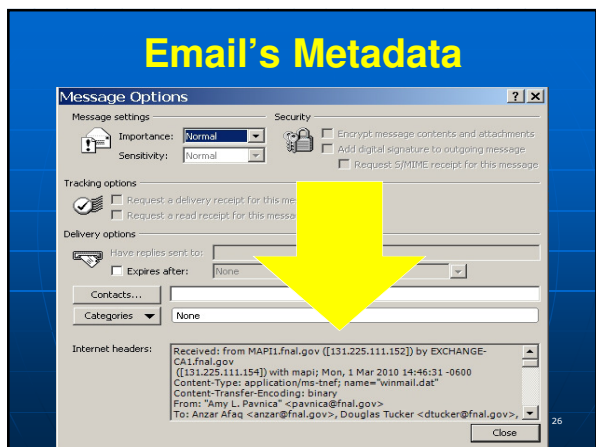
23

Email – Where’s the Original?

- How do you get to see the original
- The printout is not the original
- The metadata tells the story.







What Metadata should be produced?

- See handout for a summary of the ruling in the *National Day Laborers* case.
- Describes the metadata that should be provided in an FOIA request, but is applicable to any request for production.

Side Note:
Metadata & Your Law License

- Failure to remove metadata from your e-filings is getting attention from the ABA.
 - Ethics opinions are warning lawyers about failing to remove metadata from docs before sending them to your opponent or e-filing.
 - PACER reports many filings have failed to remove metadata

28

Native File Format

- Production of information in a usable format is useful.
- Demand production of data in a **native file format**.
 - This preserves the Metadata.
- The truth is that production in NFF is cheaper and easier to use than paper with Bates numbers.

29

Native File Format

- A lot of ESI loses much of its characteristics when reduced to paper.
 - Cannot be referred to as a "document"
- ESI is inherently searchable.
- Efficiency requires us to use creative techniques to search ESI.

30

Williams v Sprint – Metadata Discoverable

"[m]etadata varies with different [application software]...At one end of the spectrum is a word processing application where the metadata is usually not critical to understanding the substance of the document. The information can be conveyed without the need for the metadata.

At the other end of the spectrum is a database application where the database is a completely undifferentiated mass of tables of data."

■ (US Magistrate Judge David Waxse, D. Kan. 2005) (Arkfeld 2-14)

Ethical Issues

- **Duty of Confidentiality** – Some metadata may be "work product" (e.g. track changes on a letter to opposing counsel)
- **Duty of Competence** – A lawyer shall have competence on electronic issues as well.
- **Duty of Supervision** – Applies to your supervision of vendors as well.
- **Duties of Receiving Attorney** – Varies by jurisdiction about *inadvertent disclosures*.

32

ESI as Evidence

33

Pitfalls in handling ESI:

- Access or allow the client to access potential sources of original electronic evidence
 - *Do not even turn the device on. Leave it! If it's on, pull the plug, pull the battery, or call in an expert.*
- Ask for a "copy" of the original device without specifying the criteria for the copy.
- Allow IT to redeploy a machine that is potentially at issue
 - *If they really must, have them pull the hard drive and preserve at least that, documenting the original computer information.*
- Plug in any device a client sends you - curiosity can be a case-killer
 - *Antivirus and indexing software can change access dates, etc.*

ESI handling Do's

- Create a clear **chain of custody** that starts at the custodian and stays current
 - This form should stay WITH the ORIGINAL EVIDENCE at all times, and be updated whenever it changes hands or location
- Use expert resources to assist in proper handling of electronic evidence
 - Specialized training, even with minimal efforts, can save critical data & avoids spoliation arguments
- Inform the client of the necessity to carefully handle evidence
- Suggest client utilize internal procedures that are clearly documented or third party resources to ensure preservation

Introduction of ESI into evidence

- Same rules of evidence apply to ESI.
- Authenticity goes to whether the evidence is what it purports to be ...
- Content and authorship goes to the weight of the evidence.
- What rules should be applied to ESI to be used in evidence at trial?
 - Commentators and scholars are debating this subject.

36

What rules should be applied to ESI

- Commentators and scholars are currently debating this subject.
- New rules are being suggested.
- You must look to the record system it comes from . . . and this is where the costs climb.

37

Admissibility of ESI

Lorraine v. Markel American Insurance Company, 241 F.R.D. 534 (D.MD. 2007)

- a landmark decision about the admissibility and authentication of digital evidence was set down in a 100-page opinion by Magistrate Judge Paul W. Grimm
- established a detailed baseline for the use of ESI before his court (and in courts using the FRE).
- Given the guidelines and references provided by the judge, it now becomes difficult for counsel to argue against the admissibility of electronic evidence.

38

e-Admissibility – Nothing New! *Traditional Rules Still Apply*

- Relevant
- Authentication
- Hearsay
- Best Evidence Rule (. . . but what's the original document?)
- Probative Value & Unfair Prejudice

39

Authentication of e-Evidence What is the Original?

- A digital file cannot exist independently from the media upon which it is recorded.
- The original is just the binary code.
- Software is needed to “review” or view the document.
- ESI consists of the human created content and the **metadata**.

40

When you find the ESI, what's next?

Preservation: You must take steps to protect ESI against potential loss.

Extraction: Should the ESI be removed from the Client's possession?

Evaluation: How much of the ESI selection be cleared prior to my looking at it?

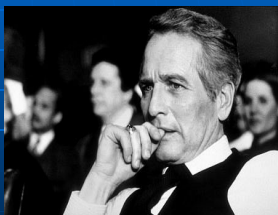
Production: How do I weed out the unnecessary, immaterial ESI and only provide my opponent with the ESI that is both pertinent and valuable?

41

The Verdict – Dealing with Fudged Evidence

Forged Hospital Record

How do we deal with this problem in the 21st Century when all records are stored in electronic format?



42

Getting Hospital Records

- Send request to the hospital Legal Counsel or Chief Information Officer, **not** the Records Custodian
- Detail the information you are seeking:
 - ie, need to know when medical and nursing licensed personnel documented on the chart and the time the changes were made - so you want the information surrounding the file that shows the changing of the file

43

Getting Hospital Records (Part 2)

- Request Audit Trail Information
- Request Logging Information
- Request the Data Dictionary
- *AND ASK FOR UPDATED AUDIT TRAIL BEFORE TRIAL*

44

Getting Hospital Records (Part 3 – The hard part)

- No standards in the industry
 - All medical providers have different databases and these buzz terms with get them to sit up, notice and balk...but most likely won't produce anything. For example, audit trail information may not exist.
 - The data dictionary will be useless without the key to corresponding tables. The facilities might not even have canned reports that they can spit out.
- You could request a "Coma Delimited File" that would contain the information you are seeking, but in a spreadsheet type format that neither you nor possibly anyone else could understand.
- Bottom line . . . Very expensive and hard to get.

45

HIPPA and Electronic Medical Records

- HIPPA refers to this as "protected health information"
- If you want to find out the truth, look for the audit trail . . .
 - Which means it's in the metadata!
- As to admissibility of the records, check out the Sedona Conference Commentary on ESI Evidence (2008)

46

Pre-Trial ESI Plan

Most technical details are easily addressed prior to the start of any significant collection and production.

- Metadata fields... which?
- How documents are produced.
- De-duplication handling
- Etc.
- ***And use of the production at trial.***

47

The Federal Rules

48

Fear Not the Federal Rules

- 12/6/06 Amendments specifically address ESI
- The drafters noted that *"the discovery of ESI is becoming more time consuming, burdensome and costly."*
- Changes the pretrial paradigm
- Provides precedence for your strategy



Self-Authenticating ESI – New Rules 902(13) – (14)

- Rule 902(13) now provides that the following are self-authenticating:
 - *Electronic records generated by a system that produces an accurate result as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12).*
 - This dispenses with the business records foundation.
 - The certification must "contain information that would be sufficient to establish authenticity were the information provided by a witness at trial."

50

Self-Authenticating ESI – Rules 902(13) Example

- **Websites** can be authenticated by:
 - Witness testifies that they logged into the website and reviewed what was there.
 - And the proffered exhibit fairly and accurately reflects what the witness say.
 - A Rule 902(13) certification that provides these facts is a substitute for testimony and shifts the burden to the other party to refute the foundation.
 - Court's role is to rule if there is a sufficient basis for the jury to determine authenticity.
 - **Court must still assess admissibility.**

51

Self-Authenticating ESI – Rules 902(13) & Admissibility

- Hearsay, relevance, best evidence must still be satisfied.
- Admissibility may be addressed in the certification by combining 902(11) and 902(13) certification.

52

Rule 902(14) - Authenticating Digital Copies

- Rule 902(14) is aimed at digital copies, making the following self-authenticating:

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).

53

Rule 902(14) Certification - a Product of Technology

- Advisory Committee Note discusses how to authenticate a digital copy:

Data copied from electronic devices, storage media, and electronic files are ordinarily authenticated by "hash value." A hash value is a number that is often represented as a sequence of characters and is produced by an algorithm based upon the digital contents of a drive, medium, or file.... [I]dential hash values for the original and copy reliably attest to the fact that they are exact duplicates.

This amendment allows self-authentication by a certification of a qualified person that she checked the hash value of the proffered item and that it was identical to the original.

54

Tools for Digital Copying of Mobile Devices

Cellebrite is the tool used by law enforcement for digital copying and extraction of data from mobile devices.

Other tools include Lantern, which may be more discriminating.

U.S. v. Morales, 2017 CCA LEXIS 757 (2017)

Expert testimony is the only reliable source of technical information.

55

Help – Additional Resources:

Seventh Circuit Pilot Program:
www.discoverypilot.com

Sedona Conference and Glossary:
www.thesedonaconference.org/

EDRM:
www.edrm.net/

Merrill Knowledge Source:
www.merrillcorp.com/merrill-knowledge-source.htm



56

Required Reading:

- *The Sedona Principles, Third Edition (2017 Public Comment Version)*.
- *Lorraine v. Markel American Insurance Company*, 241 F.R.D. 534 (D.MD. 2007)

57

George "Geo" Bellas

Geo is the senior partner in the Chicago suburban law firm of **Bellas and Wachowski**, has been involved in many complex commercial and business lawsuits. Geo also works with the nationally prominent personal injury law firm of **Clifford Law Offices** in Chicago where he works on class actions, mass torts and SUV rollover litigation.



In 2001 Geo received one of ATLA's highest honors - the Steven Sharp Award - for his work in educating the public on the defects with the Ford Explorer following the recall of the Explorer and the Firestone tires.

Geo has lectured nationally on the use of technology in litigation and on e-discovery issues. He has served as a panelist at The Sedona Conference in April, 2005. Geo currently serves on the 7th Circuit's E-Discovery Committee.

george@bellas-wachowski.com
847-823-9030 x219

58
