PROGRAM MATERIALS
Program #3610
March 10, 2026

Ethical Duties and Electronically Stored Information

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 150, Boca Raton, FL 33487
Phone 561-241-1919

Ethical Duties and Electronically Stored Information

Thomas Plunkett, EnCE, CISSP
Director, Digital Forensics

TPlunkett@ArcherHall.com
855.839.9084

ARCHERHALL
AIM HIGH

Digital Forensics & eDiscovery experts
serving attorneys in all 50 states

- Cellphones
- Computers & Tablets
- External Hard Drives
- Smart Devices
- Emails & SMS
- Social Media Accounts
- Cloud Data
- Electronic Medical Records

BUSINESS LITIGATION

EMPLOYMENT LAW

SCHOOLS AND HIGHER-ED

MEDICAL MALPRACTICE

IP THEFT

BANKRUPTCY

About the Speaker

Tom Plunkett

- MS Information Systems, 2002
- Certified Information Systems Security Professional (CISSP), 2007
- EnCase Certified Forensic Examiner (EnCE), 2008

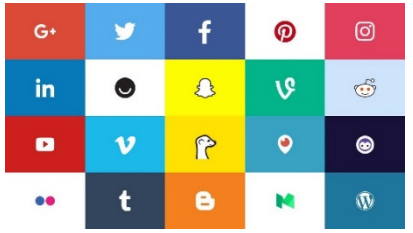
- Adjunct Professor, MS Cyber Security Leadership, University of San Diego
- Former Information Security Officer, County of Riverside, CA
- Former Cyber Counterintelligence Officer, Los Alamos National Lab
- Former CH46-E Helicopter Crewchief, USMC

Agenda

- Definitions
- Overview of Formal Opinion 2015-193
- Things to Consider

Electronically Stored Information (ESI)

- Any data that resides on electronic or digital media.
- Includes data stored on:
  - Computer Disks
  - Printer or Fax memory
  - Tape storage
  - Databases
  - Network Storage
  - Mobile Devices
  - Cloud Services
  - Social Media
  - ANY Digital media that may be invented



Sources of ESI - Devices

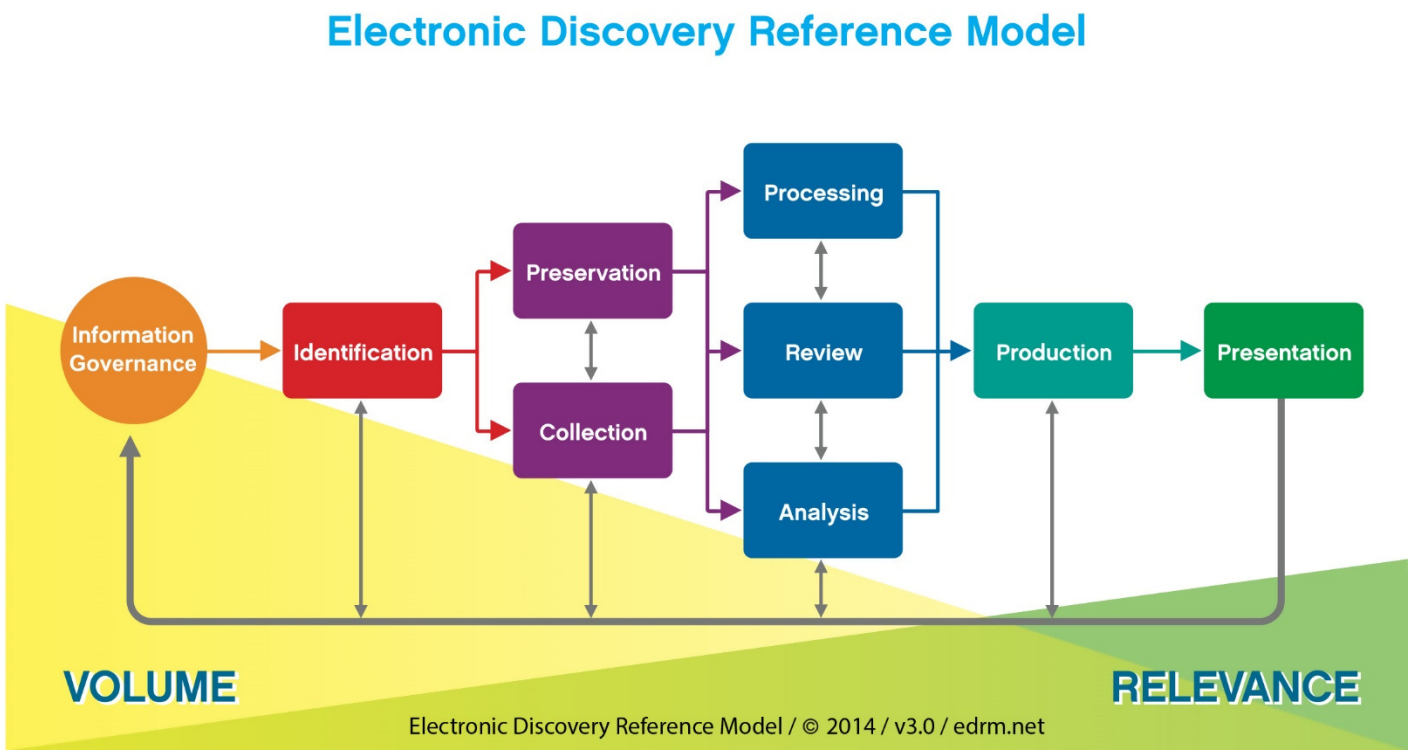
Desktop	Smart Phone	Personal Digital Assistant
Laptop	Digital Camera	Answering Machine
Music Player	Tablet	GPS
Network Equipment	Video Camera	Security System
Not-so-smart Phone	Vehicle CANbus	eReader
Printers	Video Game System	IOT Devices

Types of ESI

Audio	Databases	Folders	PDF, XPS	Voice Mail
Blog Postings	Deleted Data	Geolocation Data	Schematics	Web Pages
Chat messages	Device Settings	Images	Social Media Postings	Word Processing Docs
Computer Applications	Diagrams	Internet Activity	Spreadsheets	Disk Images
Computer Programming Code	Drawings	Logs	Text Messages	Virtual Disks
Connected Device Information	Email	Network Information	Video	Presentations

Electronic Discovery or eDiscovery

- The process of locating, securing, and searching ESI to use as evidence in a legal proceeding.

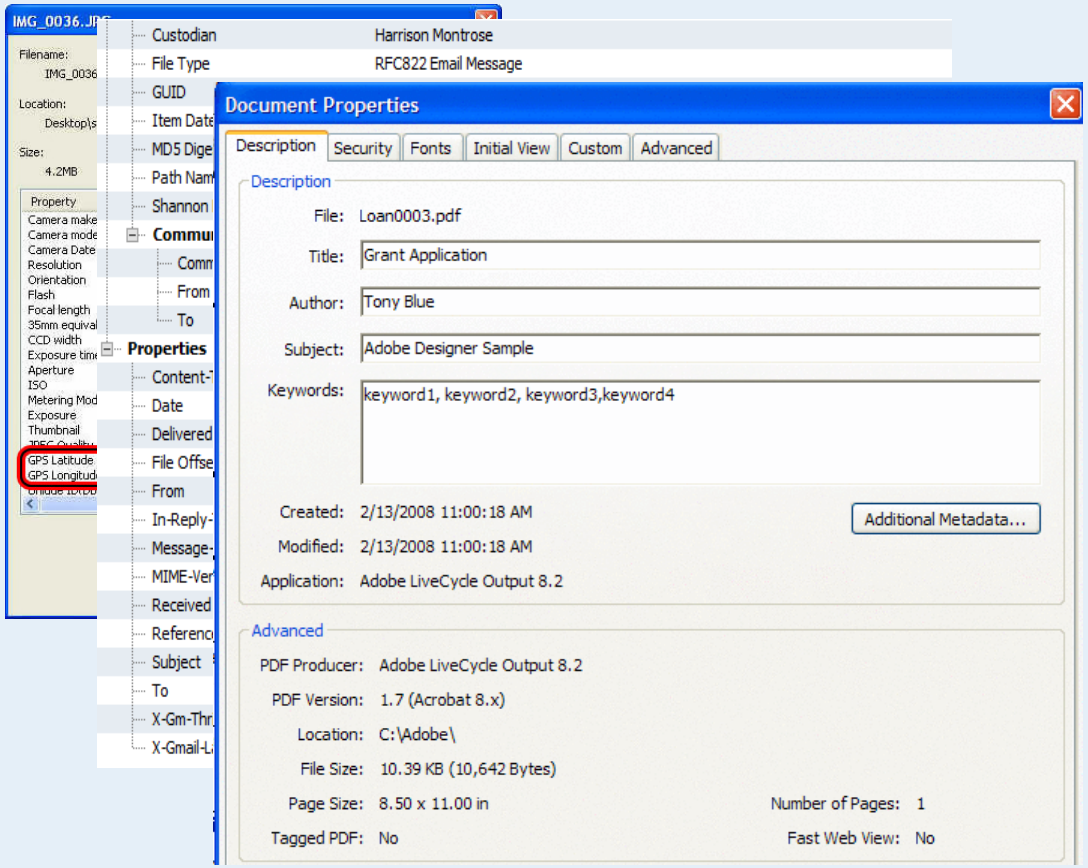


Digital Forensics

- The use of specialized techniques for recovery, authentication and analysis of ESI.

Metadata

- Information about Data
- Internal
  - Stored within the file itself
  - Comprehensive
- External
  - Stored in the file system
  - Summary



Agenda

- Definitions
- Overview of Formal Opinion 2015-193
- Things to Consider

Hypothetical Case Example

- Distributor sues Manufacturer
- Attorney defends Client in litigation brought by Client's Chief Competitor
- Opposing counsel demands E-Discovery
  - Defense attorney refuses. Judge insists.
  - Attorneys agree upon joint search with clawback agreement
  - Attorney prepares a list of keywords. Opposing adds terms
- Attorney has represented Client before
  - Client is a large company with IT department
  - Client's CEO tells Attorney there is no electronic information it has not already provided to Attorney in hard copy form

Hypothetical Case Example

- Allows opposing side's vendor unsupervised access to clients network
  - Does not give IT any special instructions
- Attorney does not review the results of the search that are provided
- Spoliation accusations; seeking sanctions
- Attorney hires expert
  - Expert finds regular deletion of potentially responsive ESI
  - Expert finds that broad terms produce irrelevant but proprietary info to competitor

Guidance From The State Bar

Overview of Formal Opinion 2015-193

- What are an attorney's ethical duties in the handling of discovery of electronically stored information?
  - Basic understanding of, and facility with, issues related to eDiscovery and ESI
  - Duty of competence may vary case-by-case, requiring a higher level of technical knowledge
  - An attorney lacking the required competence for e-discovery 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

Nine Skills of Competency

1. Initially assess e-discovery needs and issues, if any
2. Implement or cause to implement appropriate ESI preservation procedures
3. Analyze and understand a client's ESI systems and storage
4. Advise the client on available options for collection and preservation of ESI
5. Identify custodians of potentially relevant ESI
6. Engage in competent and meaningful meet and confer with opposing counsel concerning an e-discovery plan
7. Perform data searches
8. Collect responsive ESI in a manner that preserves the integrity of that ESI
9. Produce responsive non-privileged ESI in a recognized and appropriate manner

Guidance From The State Bar

Overview of Formal Opinion 2015-193

1. Initially assess e-discovery needs and issues, if any.

- What information could I possibly be looking for?
  - New data formats – cloud hosted – client may not be aware
- Where could that information be located?
  - My client's possession
  - Opposing client's possession
  - 3rd party possession

2. Implement/cause to implement appropriate ESI preservation procedures.
   - Time Sensitive
     - What information could be deleted or wiped?
       - Phone company and Internet Service Provider (ISP) records
       - Backups
       - Emails
   - Appropriate Forensic Preservation
     - Using digital forensics preservation tools.
     - Chain of Custody

Guidance From The State Bar

Overview of Formal Opinion 2015-193

3. Analyze and understand a client's ESI systems and storage.
   - Computer, Server, Backups, External Drives
   - Smartphone / Cell Phone
   - Cloud Storage/Backup (Google Drive, DropBox, OneDrive, CrashPlan)
   - Cameras / Video Surveillance
   - New Types of ESI

4. Advise the client on available options for collection and preservation of ESI.

- Digital Forensics / E-Discovery Expert
  - Forensic Collection / Preservation to meet court requirements
  - Organizational integrity
- Attorney retains evidence
- Vendor or another attorney supervise collection
- Having IT staff perform collection is usually insufficient

5. Identify custodians of potentially relevant ESI.
   - Your client / opposing party
   - Other employees at the firm
   - IT Employees
   - Telephone / Cell Phone Companies
   - Internet Service Providers
   - Hosted Application Providers (Salesforce, Online Time Card, Facebook, DropBox, etc)
   - Email / Text Message CC Recipients

Guidance From The State Bar

Overview of Formal Opinion 2015-193

6. Engage in competent and meaningful meet and confer with opposing counsel concerning an e-discovery plan.

- Work with your client to determine clear search terms.
- Consult with e-discovery or forensics expert regarding potential search terms and also potential overbroad search terms.
- Review data obtained from your clients before it is released to opposing counsel.
  - Do not rely on claw back

7. Perform data searches

- Search both searchable and non-searchable data
  - Some files may require OCR or manual review
- Alternate spellings / misspellings
- Avoid terms such as single or short words
- Use Boolean Logic (AND, OR, NOT) to be as precise as possible
  - (“peanut butter” AND jelly) w/1 (sandwich OR sammich)
- Indexed searches vs. Plain Text or Raw search

8. Collect responsive ESI in a manner that preserves the integrity of that ESI

- Preserving the Integrity
  - Chain of Custody
  - Limiting Access to Data
    - Write Blocking / Working Copies
- Proving Preservation of Integrity
  - Checksum – output of cryptographic algorithm. Digital Fingerprint
  - Digital Forensic Containers

9. Produce responsive non-privileged ESI in a recognized and appropriate manner.

- Formal Opinion refers to attorneys ethical obligations relating to his own client's ESI, and does not address the scope of an attorney's duty of competence relating to obtaining an opposing party's ESI.
- Native Formats
- PDF Formats
- Common Metadata
  - Created/Modified/Accessed Dates, Location, Custodian, Checksum

What do you think?

- What did the attorney NOT do that should have been done?
- Did he meet the standards of competency?
- Why did the search terms produce overbroad results?
- How could that have been prevented?
- Did spoliation actually occur?
- How could the attorney have prevented the spoliation accusations?

Agenda

- Definitions
- Overview of Formal Opinion 2015-193
- Things to Consider

Ethical Duties & ESI

Things to Consider

- Request for Preservation
  - The standard of competence changes with technology.
    - New forms of ESI emerge frequently
  - E-discovery expertise helps protect client confidentiality and privilege.
    - Reduce chance of overproduction and privilege breach
  - Opposing counsel may not know what they should be preserving – best to describe locations where data may be kept.
  - Opposing counsel may not know that they may need an E-Discovery or Digital Forensics expert to properly preserve their evidence.

- Discovery Process
  - What can I expect to receive in terms of ESI?
    - You get what you ask for - maybe
  - How should I ask for the ESI?
    - Native Documents – with Metadata! – Maybe a load file
  - How should the data integrity be preserved?
    - Forensic containers with all metadata

Ethical Duties & ESI

Things to Consider

- Discovery Process
  - How is data stored?
    - some data may require an expert to retrieve it
  - How do I ask for information that may require an ESI expert to retrieve?
    - Describe the sources and data types
    - Request Forensically Sound productions
  - How do I effectively limit or cull through information captured or received?
    - Information Governance / Retention Policy
    - Date Range
    - Good keywords

We’d love to hear from you!

Tom Plunkett
Director, Digital Forensics

TPlunkett@ArcherHall.com
855.839.9084

ARCHERHALL
AIM HIGH