

Digital Evidence

Week 5 – History & Ethics of E-discovery and Digital Evidence

Shawn Davis
ITMS X83 – Spring 2026

Slides contain original content from Davis, S. and
E-discovery: An Introduction to Digital Evidence



Last Week - Review

- Kahoot Review – 11 questions
 - 30 seconds for multiple choice
 - 20 seconds for true and false

Overview

1. How Did E-discovery Begin?
2. Overview of Metadata in E-discovery
3. E-discovery Perspectives
4. How to Read a Case
5. Overview of the EDRM
6. The Enron Case

Objectives

- Describe the origins of e-discovery as well as the laws and language surrounding it
- Define types of metadata
- Describe e-discovery from a civil and a criminal perspective
- Use the FIRAC legal analysis method to read a case
- Use the Electronic Discovery Reference Model

Part I

How Did E-discovery Begin?

When Did E-discovery Begin

- The term “e-discovery” is fairly new
- Timeline:
 - Took off in 70s-80s as computers became integral to business operations
 - Gained further momentum in 90s as email became more pervasive in corporate environments
 - George Socha & Tom Gelbmann co-developed Electronic Discovery Reference Model (EDRM) in 2005
 - FRCP amended in 2006 to address E-discovery

Question:

- What is the main federal law to deter hacking??
 - Computer Fraud and Abuse Act (CFAA)
- CFAA introduced important considerations when collecting evidence

The Computer Fraud and Abuse Act

- Computer Fraud and Abuse Act (CFAA) - created to address the problem of computers being hacked
 - Before this act, the Counterfeit Access Device and Abuse Act of 1984 targeted fraud and computer crimes
 - U.S. Congress adopted CFAA in 1986 as an amendment to the 1984 act
- **Computer abuse:** illegal use of computers or related services to steal or modify data

The Computer Fraud and Abuse Act

- As part of the National Information Infrastructure Protection Act of 1996:
 - Wording was added to the CFAA to cover extortion that threatens harm to a protected computer

The Computer Fraud and Abuse Act

- Additional changes were made in 2001 and 2006
 - With the addition of the U. S. PATRIOT Act
- The Identity Enforcement and Restitution Act of 2008
 - Made an amendment to the CFAA allowing prosecution if the victim and perpetrator are in the same state
 - Allows victims of identity theft to seek restitution

The Computer Fraud and Abuse Act

- Early mainframes were designed to be accessed remotely via what?
 - Telnet and FTP
- What is the issue with Telnet and FTP??
 - Not encrypted
- What should admins use now?
 - SSH and SFTP

The Computer Fraud and Abuse Act

- The Computer Emergency and Response Team at Carnegie-Mellon University estimated:
 - Computer intrusions increased almost 500% between 1991-1994

The Computer Fraud and Abuse Act

- In early days of Internet, hackers broke into networks just to show they could
 - Defense attorneys argued that data was only copied so it wasn't stolen
 - These arguments led to passing the CFAA
- A **protected computer** is one used by a financial institution or government agency or used for commerce or communication

The Computer Fraud and Abuse Act

- Seven types of computer offenses covered by CFAA?
 - Accessing a computer or network without authorization or by exceeding authorization
 - Accessing a computer or network to collect financial, credit or other information from a government or protected computer
 - Making a computer or network unavailable for its intended use
 - Transmitting programs, information, codes, or commands to intentionally cause harm or damage to networks or computers

The Computer Fraud and Abuse Act

- Seven types of computer offenses covered by CFAA (cont'd):
 - Accessing information on a computer or network to commit fraud or cause damage
 - Intentionally obtaining and trafficking in passwords
 - Threatening harm to a computer or network for use in extortion or a similar practice

Question:

- What are some famous hacks that have violated the CFAA?
 - Aaron Swartz – Downloaded 2.7mil papers from MIT
 - Andrew Auernheimer – Found hole in AT&T's site and obtained 120k email addresses of AT&T iPad users
 - Matthew Keys – Provided creds to Tribune server and encouraged Anonymous members to use it

Question (Cont):

- Fidel Salinas – Queried govt website with vuln scanning software
 - Initially charged with 44 felonies and sentences to 440 years in prison
 - ❖ Later reduced to 6mths in prison and 10k fine
- Lori Drew – Opened fake myspace account to bully teen girl
- Anastasio Laoutaris – Former IT admin launched kill switch to disable Eaton Corp's servers

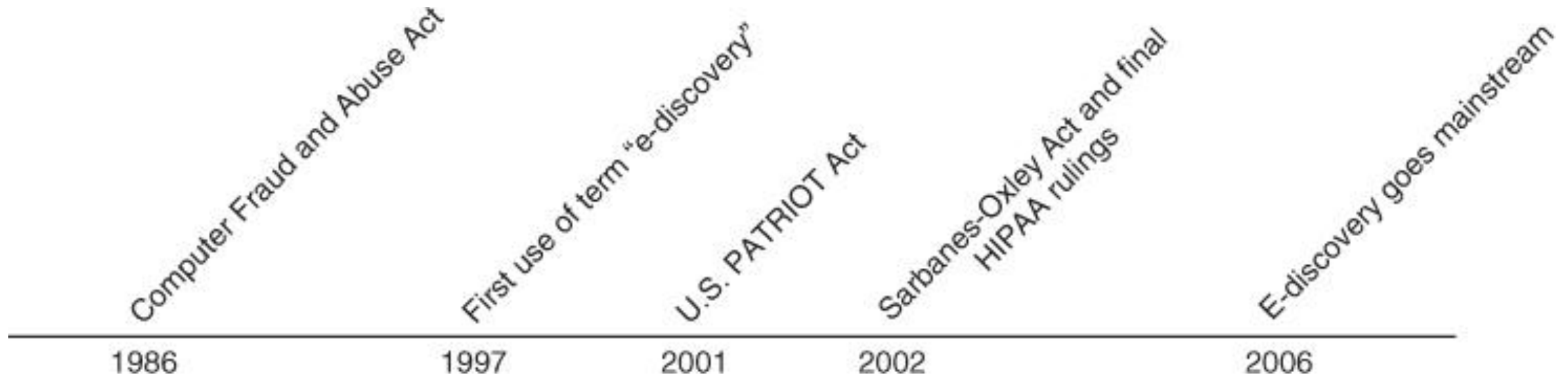
Two Famous Cases Found to Not Violate CFAA

- hiQ Labs v. LinkedIn
 - Case about hiQ scraping up public data from LinkedIn
 - 9th Circuit found that scraping even after a cease and desist does not necessarily constitute a CFAA violation
 - Scraping often does violate website terms though

Two Famous Cases Found to Not Violate CFAA

- Van Buren v. United States
 - Georgia police sergeant had used valid creds to lookup license plate in police DB for personal reason
 - Supreme Court ruled didn't violate CFAA because he have authorization—even if for an improper purpose
 - Still a considered a misuse of data and could allow for termination
 - **Established current precedent case law for CFAA**
 - Violation: Accessing information not entitled to obtain
 - Non-violation: Accessing information allowed to see but with a bad motive

Timeline of E-discovery Law



EDI, ESI, and E-discovery

- **What is EDI and its purpose?**

- Electronic Data Interchange - created in the mid-1970s to make exchanging information electronically easier
- Purpose was to automate business transactions, such as purchase orders, request for proposals, invoices, and packing slips

EDI, ESI, and E-discovery

- Health Insurance Portability and Accountability Act (HIPAA)
 - Require companies to protect health related information
- What are some healthcare related hacks?
 - 1.4mil records in UnityPoint Health phishing attack
 - Millions of records from LabCorp hack
 - Ransomware against Allscripts

EDI, ESI, and E-discovery

- What did Sarbanes-Oxley require publicly held corporations to do?
 - Hold onto email for five years
 - Hire independent auditors for financials
 - Protect whistleblowers
 - Be able to turn over data when requested by courts
 - Fines/jail for tampering/destroying documents during investigations
- Was enacted in part due to the Enron and WorldCom cases

EDI, ESI, and E-discovery

- The first discussion in a major law journal of e-discovery being used in civil litigation appeared in 1997
- E-discovery became a popular topic in civil litigation discussions and articles around 2001

Part II

Overview of Metadata in E-discovery

Overview of Metadata in E-discovery

- Metadata Encoding and Transmission Standard (METS) - the standard used for objects in a digital library
 - Developed by the Digital Library Association and maintained by the Library of Congress
- METS profiles are found in:
 - PDF files
 - Photographs
 - CDs
 - Other digital records

Overview of Metadata in E-discovery

- METS has five categories for metadata:
 - *Descriptive metadata* - lists metadata embedded in the document or external descriptive metadata stored on an Internet server
 - *Administrative metadata* - describes how a document was created and stored, the original source object, and intellectual property rights

Overview of Metadata in E-discovery

- *File groups* - groups electronic versions of a file, such as TIF versions, PDF versions, etc
- *Structural map* - shows users how to navigate all files
- *Behavior* - deals with any executable portions of documents

Overview of Metadata in E-discovery

- OS metadata is what is stored by computer and network operating systems
 - A typical OS keeps track of a file's MAC times
 - Show when the data was modified, accessed, and created
 - Both an OS and NOS can show investigators the last time a file was accessed and whose login was used to modify a file

Overview of Metadata in E-discovery

- Is OS/NOS metadata generally captured in civil cases?
 - No
- What type of metadata is captured?
 - Only the metadata embedded within documents is captured

Overview of Metadata in E-discovery

- Metadata is used mainly for organizing the discovery process
 - Content of documents and e-mails is often more important than the metadata
- Deleted information might be deemed “not readily accessible” or too costly to retrieve
 - It is most likely not produced

Overview of Metadata in E-discovery

- What are some metadata items that are useful?
 - Author(s)
 - GPS
 - Application used to create it
 - Creation timestamp
 - Company name

Part III

E-discovery Perspectives

E-discovery Perspectives

- What four types of people have perspectives that affect E-discovery projects?
 1. The legal professional - understands law
 2. The e-discovery professional - comes from a corporate background
 3. The digital forensics professional - understands forensics standards, software, and procedures
 4. The IT professional - knows where information and files are stored on OSs and NOSs
 - Might have limited legal knowledge

E-discovery from a Criminal Perspective

- Criminal e-discovery tends to focus on digital forensics and forensic bit level images
- Civil cases do not require forensic imaging as much
- What do civil cases focus on retaining?
 - Logical copies of evidence
 - Embedded metadata

E-discovery from a Criminal Perspective

- OS metadata is analyzed to identify:
 - Evidence
 - Alterations to evidence
 - User activity
- Embedded document metadata is used to organize case material
 - To establish a timeline in order to corroborate people's locations and determine who had access

E-discovery from a Criminal Perspective

- The Federal Rules for Criminal Procedure (FRCrP) are applied to criminal cases
 - Especially Rule 41: Search and Seizure
- Rule 41 specifies what?
 - How to get and carry out a search warrant
 - Explains motions to suppress evidence and how evidence must be returned

E-discovery from a Criminal Perspective

- Rule 41 is tied directly to which Amendment of the U.S. Constitution?
 - 4th Amendment protects residents from unreasonable search and seizure

E-discovery from a Criminal Perspective

- Search and seizure law helps ensure that volatile electronic evidence isn't compromised
 - Investigators work with network administrators to view network logs
 - They can determine who was logged in at the time of the incident
- May also talk to physical staff to find out information
 - Example: whose keycard was used to get into a restricted area

E-discovery from a Civil Perspective

- Do internal corporate investigations usually fall into the civil or criminal category?
 - Civil and a search warrant is not needed
 - Most companies have policies specifying that when a complaint is filed, an internal investigation can begin
 - Employees can not simply begin investigating a colleague

E-discovery from a Civil Perspective

- If criminal activity is discovered during the investigation, corporate legal counsel is notified, who will then notify the authorities

E-discovery from a Civil Perspective

- Civil e-discovery bypasses many search warrant procedures required in criminal cases
 - Lawyers on both sides are involved from the beginning
- Two cases that caused the court system to take a look at the cost burden of e-discovery:
 - Zubulake case
 - Rowe Entertainment v. The William Morris Agency

Zubulake v. UBS Warbug LLC

- Case about gender discrimination
- Heard before 2006 FRCP amendments
- Defendant failed to save some emails on backup tapes
- Plaintiff asked UBS to bear cost burden of the discovery, but UBS said it was excessive
- UBS eventually found at fault and had to bear 75% of discovery cost (about 300k)

E-discovery from a Civil Perspective

- Courts developed a test consisting of seven factors to determine cost shifting:
 1. The extent to which a request is tailored to discovery relevant information
 2. The availability of information from other sources
 3. The total cost of production, compared with the amount in controversy
 4. The total cost of production, compared with the resources available to each party
 5. Each party's ability and incentive to control costs

E-discovery from a Civil Perspective

- Courts developed a test consisting of seven factors to determine cost shifting (cont'd):

6. The importance of issues at stake in the litigation

7. The benefits to both parties of obtaining the information

Part IV

How to Read a Case

How to Read a Case

- Challenge for IT personnel involved in e-discovery:
 - Reading case law
- IT personnel need to understand how to read a case and determine what issues are relevant
- Law students use a basic tool called IRAC for reading, analyzing, and writing legal cases
 - This book uses a modification of IRAC called FIRAC
 - Stands for facts, issues, rules and references, analysis, and conclusions

How to Read a Case

- When reading or reviewing a case, use a word processor's highlight feature
 - Finding important items is easier later
 - Example:
 - Facts could be highlighted in purple
 - Conclusions could be highlighted in red

FIRAC

F

Facts

Determine the actual facts in the case. Answer who, what, when, where, and how.

I

Issues

What are the issues resulting from the case? What needs to be considered?

R

Rules and References

What rules are applied to the case? What other cases or events are used?

A

Analysis

What analysis was applied to the facts, issues, and rules presented?

C

Conclusions

What conclusions were drawn and why?

FIRAC

Facts

Issues

Rules and references

Analysis

Conclusions

FIRAC In-Class Review

- Open our course on Canvas
- Go to Modules / Week 5
- Open US v. Trotter.doc
- Read the case and keep track of what the highlights mean

FIRAC In –Class Review

Facts

United States Court of Appeals,
Eighth Circuit.

Issues

UNITED STATES of America, Appellee,
v.

Rules and references

Analysis

John Larkin TROTTER, Appellant.

Conclusions

No. 05-4202.

Submitted: Feb. 16, 2007.

Filed: Feb. 23, 2007.

Paul Kaiser, St. Charles, MO, for Appellant.

Before RILEY, MELLOY, and SHEPHERD, Circuit Judges.

PER CURIAM.

John Larkin Trotter was charged with intentionally causing damage to a protected computer without authorization, in violation of 18 U.S.C. § 1030(a)(5)(A)(i). Trotter pleaded guilty, reserving the right to challenge the constitutionality of § 1030(a)(5)(A)(i) as applied. The district court FN1 sentenced Trotter to eighteen months' imprisonment and ordered Trotter to pay approximately \$19,000 in restitution. On appeal, Trotter argues § 1030(a)(5)(A)(i) is unconstitutional as applied to his conduct: an attack on a not-for-profit organization's computer network that was connected to the Internet and used to communicate with out-of-state computers.

FIRAC In –Class Review

Facts

Issues

Rules and references

Analysis

Conclusions

II. Discussion

We review a constitutional challenge to a statute de novo. *United States v. Mugan*, 441 F.3d 622, 627 (8th Cir.2006). Title 18 U.S.C. § 1030(a)(5)(A)(i) prohibits a person from knowingly causing “the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer.” A “protected computer” is defined, in pertinent part, as a computer “which is used in interstate or foreign commerce or communication.” 18 U.S.C. § 1030(e)(2)(B).

FIRAC In –Class Review

Facts

Issues

Rules and references

Analysis

Conclusions

subject to regulation by Congress. *Id.* In *Mitra*, the defendant argued the intrastate nature of his attack took it outside the constitutional applicability of the statute. Judge *922 Easterbrook, writing for the court, explained the location of the attack is not determinative because “[o]nce the computer is used in interstate commerce, Congress has the power to protect it from a local hammer blow, or from a local data packet that sends it haywire.” *Id.* Likewise, the nature of the organization using the computer is irrelevant; once the computer is used in interstate commerce, Congress has the power to protect it.

III. Conclusion

For the reasons stated herein, the judgment of the district court is affirmed.

C.A.8 (Mo.),2007.

U.S. v. Trotter

478 F.3d 918

US v. Trotter

- What is this case/opinion about?
 - Trotter was a Salvation Army IT supervisor that damaged their network and sent obscene emails
 - Repair cost the Salvation Army over \$19k
 - Trotter appealed in saying that he didn't violate the CFAA since the Salvation Army is a nonprofit and was therefore not a "protected computer."
 - Court disagreed and affirmed trial court's judgement

Part V

Overview of EDRM

Overview of the Electronic Discovery Reference Model

- Electronic Discovery Reference Model (EDRM)
 - Objective: Shrink huge amounts of data down to a manageable scale
 - Created by George Socha and Tom Gelbmann in 2005
 - Serves as a roadmap for handling overwhelming amounts of electronic evidence in civil cases
 - Widely used in the business and legal communities
 - Useful in reducing the volume of information to what is relevant

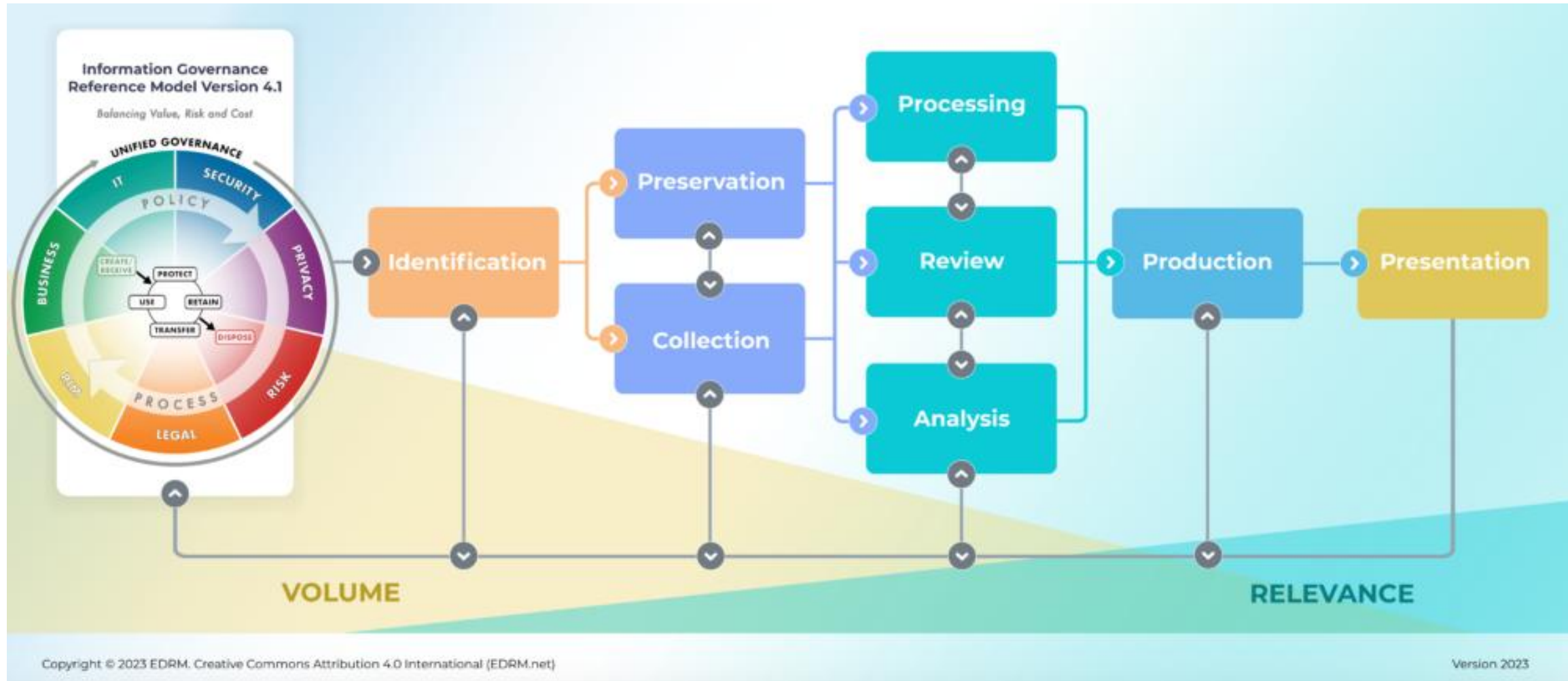
Overview of the Electronic Discovery Reference Model

- What are the nine stages of the EDRM??
 1. Information management/governance
 2. Identification
 3. Preservation
 4. Collection
 5. Processing
 6. Review
 7. Analysis
 8. Production
 9. Presentation

Overview of the Electronic Discovery Reference Model

- Some EDRM stages overlap or take place simultaneously
 - Example: collection and preservation are done in a loop
 - These two tasks are a repetitive process
 - Processing, review, and analysis are also done in a loop
 - See Figure on the following slide

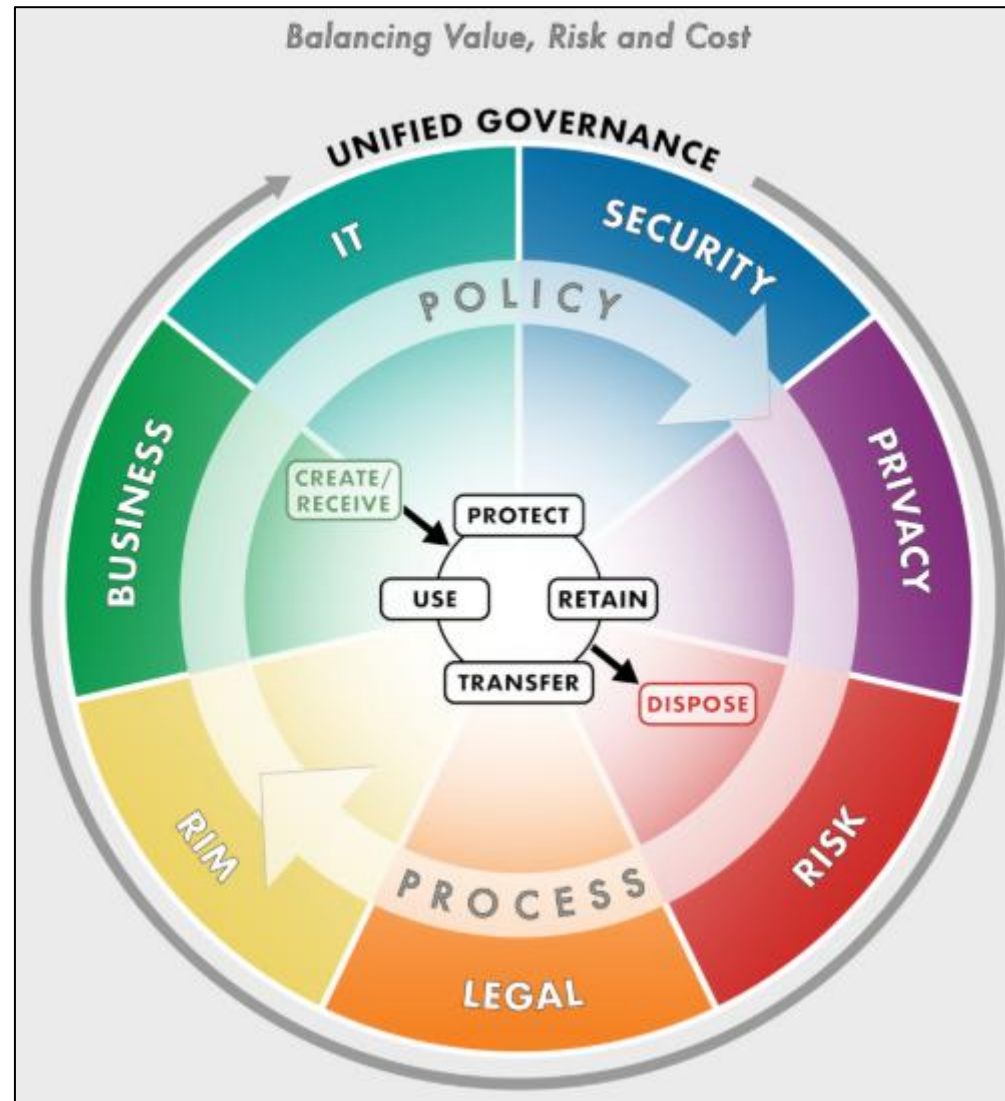
EDRM



1. Information Management/Governance Stage

- Information management - how a company organizes and manages data
- Information governance is - a way of ensuring that data is managed correctly
- During the development of the EDRM model, participants decided information management needed its own model
 - Information Governance Reference Model (IGRM) was created

The Information Governance Reference Model



1. Information Management/Governance (Cont.)

- IGRM model reflects the common lack of communication and collaboration in dealing with information management
 - Shows each group's effect on the process
 - Three main groups:
 - Business users
 - Legal, regulatory, and risk-management departments
 - IT support staff
 - Privacy and security have recently been added

2. Identification Stage

- In the EDRM, the identification stage starts with identifying:
 - Key players
 - Custodians
 - Locations of data and data sources
 - Traceability of data to people and departments
- Prepare an identification plan and establish team

2. Identification Stage (Cont.)

- Who would be on the identification team?
 - Corporate legal counsel
 - Outside counsel
 - IT personnel
 - Records management personnel
 - Data custodians
 - HR
 - Executives
 - Service Providers/Discovery Consultants

3. Preservation Stage

- The preservation and collection stages are intertwined
 - **Duty to preserve:** a provision of the FRCP stating that a company must retain all documents and data pertaining to the case
 - Prepare preservation plan
 - Suspend destruction
 - Select preservation method and execute plan

4. Collection Stage

- The collection stage is the collection of potentially relevant ESI that was defined in the identification phase
- Collected in a manner that is:
 - Legally defensible
 - Proportionate
 - Efficient
 - Auditable
 - Targeted

5. Processing Stage

- The processing stage has four subtasks:

1. Assessment

- Assess what information is available
- Audits
- Exception handling
- Roles
- Target formats/media

5. Processing Stage

2. Preparation

- Restoring backups
- Converting file types
- Full-text indexing
- Deduplication

3. Selection

- Deciding what data to move forward with and what data to leave behind
- Reduces the amount of data that will be sent to opposing counsel

4. Output

- Converts data into required formats of the receiving review platform

6. Review Stage

- Document reviewers identify responsive documents to produce to opposing counsel and decide which privileged documents to withhold
 - Privileged documents may include trade secrets or confidential government information
- Legal team begins to understand factual issues in a case at this point

7. Analysis Stage

- This stage can be deployed after many of the prior stages
- Increases productivity by continuously developing and revising strategy
- Quality control/validation
- Updating defensible audit trail

8. Production Stage

- Packages data and puts it into a format both sides have agreed on in ESI protocol
- Technical team involved to ensure they can import the packaged data
 - Consists of load files for images and metadata and the actual data files
- May need to make documents searchable, add Bates numbers, redactions, etc.
- Determine production form (native, near-native, image, paper)

9. Presentation Stage

- Only occurs if ESI will be presented to an audience at a deposition, hearing, trial, etc.
 - Select exhibits/format
 - Prepare/test exhibits
 - Present exhibits
 - Store/maintain exhibits

Criminal Cases and the EDRM

- EDRM process differs in criminal cases
 - Usually rely on surveillance and the other secretive tasks at various stages
 - Instead of records managers or IT staff, law enforcement identifies, preserves, and collects discovery
- In civil litigation, burden of finding evidence is on the requesting party
- In criminal cases, after a case has been filed, law requires the prosecution disclose case evidence to the defendant, even if not requested

Criminal Cases and the EDRM

- Three main legal directives influence the disclosure of criminal discovery:
 - *Brady doctrine* - prosecution is required to disclose all exculpatory evidence to the defense team
 - *Jencks Act* and *Giglio v. U.S* - prosecution is required to disclose all witness impeachment information to the defense team
- In most cases, prosecution also requests a review of the defense team's evidence and expert or witness information

Part VI

The Enron Case

The Enron Case

- Before the scandal in October 2001, Enron was the largest seller of natural gas in the U. S.
- Enron executives were allowed to “maintain agency” over earnings reports sent to investors:
 - Executives didn’t have to report losses or their own financial statements
 - Were able to present a profitable public image while pocketing the profits
 - Investors lost more than \$70 billion
- Enron filed for Chapter 11 bankruptcy in December 2001

The Enron Case

- Enron was investigated by the Securities and Exchange Commission (SEC) in November 2001
 - Falsified earnings, hidden losses, and embezzlement were uncovered
- The accounting and auditing firm Arthur Andersen was charged with obstruction of justice
 - They destroyed documents related to their audit of Enron
- The Sarbanes-Oxley Act was passed as a result of corporate scandals such as Enron

The Enron Case

- Major players in the Enron scandal:
 - Andrew Fastow - former Enron chief financial officer and alleged creator of the deceptive accounting practices; fired when scandal unfolded
 - Kenneth Lay - Enron's former chief executive and chairman since 1986; refused to testify
 - David Duncan - Andersen's chief auditor, shredded key documents related to the case
 - Joseph Berardino - Andersen's chief executive; defended his firm's role in the affair

The Enron Case

- Major players in the Enron scandal (cont'd):
 - Jeffrey Skilling - Enron's chief executive in the first half of 2001; denied knowing anything was wrong
 - Sherron Watkins - Enron employee who was the whistleblower of the scandal; claimed Ken Lay was "duped"
 - Placed blame on Jeffrey Skilling and Andrew Fastow
- More than 300,000 e-mails were part of the evidence used in court
 - A challenge of e-discovery is narrowing search parameters to prevent sifting through terabytes of data

The Enron Case

- Purpose of using this well-known case is to make you aware of a few important points:
 - The volume of e-mails involved in a corporate investigation
 - What steps are involved in the search process
 - How deduping works
 - What's relevant and what's not in investigations

Summary

- The term “e-discovery” is new but the process has been around for a few decades
- The Computer Fraud and Abuse Act was created as a criminal statute to address people who exceeded their privileges or caused damages on a computer or network
- EDI was created to give companies an easier way to exchange information electronically and have a standardized format
- Metadata is data about data

Summary

- The four main e-discovery perspectives are from the point of view of legal professionals, e-discovery professionals, digital forensics professionals, and IT professionals
- Because technology moves so rapidly the law rarely keeps pace with it
- FIRAC, which stands for facts, issues, rules and references, analysis, and conclusions, is a common method of reading and analyzing case files

Summary

- The EDRM is a widely accepted approach to culling massive amounts of digital data
- The duty to preserve requires data custodians to take all precautionary measures to make sure information pertaining to an upcoming case isn't destroyed or deleted

Text References

- Phillips, A., Godfrey, R., Steuart, C., & Brown, C. (2014). E-discovery: An Introduction to Digital Evidence. Boston, MA: Cengage Learning.
- EDRM Model (n.d.). Retrieved from <https://www.edrm.net/frameworks-and-standards/edrm-model/>

Homework

- Review and understand this slide deck on Canvas
- Read Chapter 3 before next class
- Research paper outline is due next Monday prior to midnight
- Your bibliography will be due 3/2 so make sure to keep track of your sources while researching

Questions???

