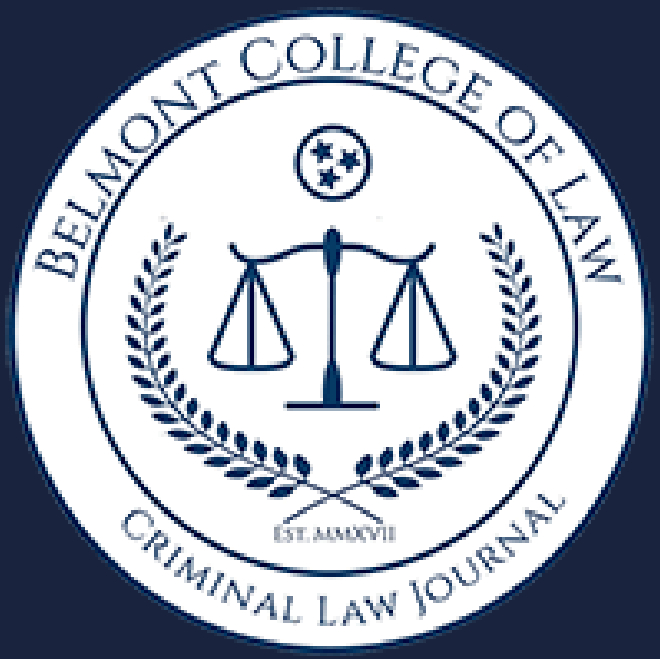
CYBER LAW IN THE CRIMINAL JUSTICE SECTOR

From Investigation to Litigation

March 6, 2020



BELMONT CRIMINAL LAW JOURNAL

TABLE OF CONTENTS

WHAT IS EDISCOVERY?

Definition and Scope of eDiscovery

eDiscovery is defined as the process of discovery in civil litigation that is carried out in electronic formats. It covers electronically stored information (ESI) such as, emails, texts, documents, accounting databases, CAD/CAM files, websites, and any other electronic information that could be relevant evidence in a lawsuit.

EDiscovery runs from the time a lawsuit is foreseeable to the time the digital evidence is presented in court.

The Process

A. Data is identified as relevant by attorneys and placed on legal hold.

B. Both parties determine the scope of discovery, identify the relevant ESI, and make eDiscovery requests and challenges. Parties may limit the scope of discovery by agreeing to search parameters.

C. Evidence is then extracted and analyzed using digital forensic procedures, and is usually converted into PDF or TIFF form for use in court.

History of eDiscovery

With a significant amount of information transmitted digitally, lawyers have placed an increased importance on eDiscovery to support many types of cases over the last few decades. As digital documents have climbed to the forefront of litigation, eDiscovery has collected an interesting history.

Iran Contra: In February 1989, Oliver North stood trial on twelve counts related to lying to Congress about his role in the Iran-Contra Affair. Here, emails served as a crucial piece of evidence in Mr. North's case. Specifically, emails that North had deleted from his computers at the National Security Council. The email server in the White House kept archives of all sent and received email and the deleted emails became evidence in the investigation of the Iran-Contra affair.

Microsoft Trial: In the 1998 Microsoft monopoly trial, Bill Gates became defensive on the stand as his own emails were read back to him. In these emails, recovered from Microsoft's email servers, Bill Gates asked his employees to think of creative ways to sabotage the company's rivals.

Deflategate: In 2015, New England Patriot's quarterback Tom Brady instructed his assistant to destroy his cellphone. Brady's act was seen as willful obstruction of justice and, "a deliberate effort to ensure that investigators would never have access to information that he had been asked to produce."

Understanding the EDRM

In 2005, two consultants, George Socha and Tom Gelbmann created the Electronic Discovery Reference Model. It is the best and most commonly accepted description of the eDiscovery process. Not all litigation will follow all of the steps described, but it remains a useful guide. The EDRM consists of nine stages. The process begins with information governance, identification, preservation, and collection. The data management functions include processing, review, analysis, production, and presentation.

Step 1: Information Governance

Step 2: Identification

Step 3: Preservation

Step 4: Collection

Step 5: Processing

Step 6: Review

Step 7: Analysis

Step 8: Production

Step 9: Presentation

Step 1: Information Governance

Information governance is a more recent addition to the EDRM. In recent years, large organizations have begun looking for ways to reduce eDiscovery costs before litigation happens, which means managing ESI from its initial creation through its final disposition.

Step 2: Identification

Locating potential sources of electronically stored information (ESI), the volume of data that might be discoverable, the custodians and locations of discoverable evidence. The key is not only identifying the evidence but addressing the potential scope and technical issues of the project at hand.

Step 3: Preservation

Parties must ensure that electronically stored information (ESI) that is discoverable for litigation is not altered or destroyed. ESI is often deleted in the course of routine business, but when potentially discoverable information is deleted, a sanctionable offense may arise where spoliation occurs.

Step 4: Collection

Data must be collected in a forensically sound manner so that evidence is not altered or changed.

Step 5: Processing

In order to review evidence in a forensically secure manner, ESI is often converted to forms more suitable for review and analysis, often an image file. The original, native document is preserved as well for more detailed, forensic analysis.

Step 6: Review

The heart of the eDiscovery process. Attorneys must review documents and evidence for relevant information while protecting privileged information from being accidentally produced to opposing counsel.

Step 7: Analysis

Attorneys must review ESI for content and context, identifying key custodians, subjects, patterns, and discussions.

Step 8: Production

Delivering electronically stored information (ESI) to others in appropriate forms. Parties still often produce evidence on hard drives or disks, although electronic production is also employed.

Step 9: Presentation

Once ESI has been reviewed for relevance, a few key pieces or passages may actually be presented at a deposition, hearing, or trial. Evidence is presented to help witness testimony, demonstrate key facts, or persuade a jury or audience.

KEY TERMS DEFINED

Custodian: The individual identified to have created or controlled an electronic file.

Culling Intelligence: Data analytics tools that automatically analyze and organize data by factors such as date, custodian, recipient, potential privilege, etc., so that users can quickly cull out the irrelevant documents and narrow the scope of discovery.

Deduplication: Techniques that remove duplicate files from a document collection. On average, deduplication can efficiently reduce the amount of data requiring review by 30 percent or more.

Forensic Image: An electronic or digital format for capturing and storing data without corruption or alteration.

Hosting: Hosting refers to keeping data available online for access during a review and for later reference.

Keyword Search: A common approach for searching document collections including keywords and Boolean strings.

Load File: The file used to import data (coded, captured or extracted data from processing) into a database; or the file used to link specific files.

Metadata: Data about data; hidden from direct view, including information such as, author, recipient, creation date, modified date, and other potentially relevant information.

KEY TERMS DEFINED

Native File: A file in its original file format that has not been converted to a digital image or other file format such as TIFF, JPEG, or PDF.

Optical Character Recognition (OCR) Text: Use of software to scan paper or imaged files, such as PDFs, and create searchable text.

Processing: The stage of eDiscovery where data is narrowed down, converted, and prepared for analysis and relevance review. Data must be imported into a software platform for analysis and production.

Production: The stage of eDiscovery where data can be produced to opposing parties in a number of formats, including images like TIFF, file formats like PDF, or native formats. Images are often easy formats to manage.

Personal Storage Table (PST): A common file format used to store messages, calendar events, and other items within Microsoft software.

Predictive Coding or Machine Learning: Refers to a process, not a search technology. Machine learning allows computers to assist in the relevancy review process by recognizing responsive documents.

Quality Control (QC): The process of ensuring that data is reliable and usable.

FEDERAL RULES OF CIVIL PROCEDURE

Rule 26(b)(1): Keep it in Proportion
Rule 26(b)(1) outlines the factors used by courts in determining when to limit the scope of discovery.

Rule 26(d)(2): eDiscovery Methods
The rules clearly state that, “methods of discovery may be used in any sequence,“ and “discovery by one party does not require any other party to delay its discovery.”

Rule 26(f): Setting the Ground Rules
A Rule 26(f) conference happens before any discovery can occur. The courts have made it clear these conferences should happen as early as possible and parties should agree on foundational principles like the forms of production.

Rule 26(g): Reasonable Inquiry
The Federal Rules of Civil Procedure mandates a reasonableness standard of care with respect to disclosure. However, “reasonable” is a matter for the court to decide on the totality of the circumstances.

Rule 34(b): Production of Data
Rule 34(b) allows the requesting party to decide how it wants information to be produced. When the requesting party fails to specify the method of production, the producing party has the option to either produce the information in a form in which it is ordinarily maintained or in an electronically searchable form.

Rule 37(e): Spoilation Sanctions
Rule 37(e) allows sanctions for failure to preserve electronically stored information (ESI), but limits sanctions to intentional, rather than negligent, failures to preserve. Under the amended rule, a court may impose sanctions if a party is found to have “intent to deprive another party” of information and the information cannot be restored or replaced through additional discovery.

Arthur Andersen, LLP v. United States

United States Supreme Court

In the aftermath of the collapse of Enron, the Supreme Court overturned Arthur Andersen's conviction for criminal obstruction of justice for shredding documents before being subpoenaed by the Securities Exchange Commission (SEC). The Court held that the trial court's jury instructions erroneously omitted the element of scienter–actual knowledge of the proceeding and intent to obstruct the proceeding required element.

Mancia v. Maylower Textile Services Co.

U.S. District Court, District of Maryland

The court determined that failure of opposing counsel to cooperate and resolve disputes on their own was the cause of increased costs in eDiscovery. The judge advised counsel on both sides to cooperate during the eDiscovery phase for efficiency. This opinion served as the basis for requiring attorneys from both parties to participate in regular conferences before court proceedings begin.

Rimkus Consulting Group Inc. v. Cammarata

U.S. District Court, Southern District of Texas

In this case, a consulting group was trying to enforce a noncompete agreement against a group of former employees. Rimkus accused the former employees of deleting relevant emails and requested sanctions. The court ruled that sanctions were appropriate because the party acted in bad faith. The *Rimkus* opinion highlights a major split among federal courts as to when sanctions are appropriate.

Da Silva Moore v. Publicis Groupe & MSL Group

U.S. District Court, Southern District of New York

U.S. Magistrate Judge Andrew Peck approved procedures for the use of predictive coding in conducting eDiscovery. Da Silva Moore filed a petition for Peck to recuse himself for bias on the basis that Peck had made previous public comments in favor of predictive coding. On appeal, the appellate courts agreed with Peck, and the U.S. Supreme Court declined to intervene.

Zubulake v. UBS Warburg L.L.C.

U.S. District Court, Southern District of New York

In this case, the defendants initially argued that recovering and reviewing electronically stored information (ESI) from backup tapes would be too costly. The court outlined a 7-factor test and compelled the defendants to produce the evidence. The costs of recovery and review of the emails at issue were shared by both parties.

Victor Stanley Inc. v. Creative Pipe Inc.

U.S. District Court, District of Maryland

Stanley sued Creative Pipe for copyright and patent infringement over the design of an end frame for a park bench. The court held that Creative Pipe had waived attorney-client privilege in producing several electronic documents because it failed to establish a privilege search protocol with the opposing party, declined to use a "clawback" agreement, and had not proven that its process for searching privileged documents was reasonable. Stanley prevailed, winning more than $2 million in damages and more than $1 million in monetary sanctions for destruction of electronic evidence by Creative Pipe.

EDISCOVERY RESOURCES

Daily eDiscovery Blog
https://cloudnine.com/ediscoverydaily

The Florida eDiscovery Case Database
https://ediscovery.law.ufl.edu

Association of eDiscovery Specialists
https://www.aceds.org

Electronic Discovery Reference Model
https://www.edrm.net

The Sedona Conference
https://thesedonaconference.org

Craig Ball's Blog on eDiscovery and Computer Forensics
https://craigball.net

University of Florida eDiscovery Conference
https://ufediscoveryconference.com

An Overview

Cyber crimes are offenses against computer data and systems, or offenses related to computers and the internet. Computers are an essential element of the crime.

Criminals use new technologies to commit cyberattacks against governments, businesses and individuals.

These crimes are not restricted by borders and cause serious harm to victims worldwide. "Pure cybercrime" refers to crimes against computers and information systems, where the aim is to gain unauthorized access to a device or deny access to a legitimate user.

Traditional crimes have evolved as criminal organizations integrate the internet into their activities for efficiency. Crimes such as fraud, theft, illegal gambling, and the sale of fake pharmaceuticals are frequently done over the internet.

WHAT IS CYBERCRIME?

The FBI has highlighted a few issues for priority in the area of cybercrime.

Online Predators

The FBI's online predators and child sexual exploitation investigations are managed under our Violent Crimes Against Children Program, Criminal Investigative Division. These investigations involve all areas of the Internet and online services, including social networking venues, websites that post child pornography, Internet news groups, Internet Relay Chat channels, online groups and organizations, peer-to-peer file-sharing programs, bulletin board systems, and other online forums.

Identity Theft

Identity theft occurs when someone unlawfully obtains another's personal information and uses it to commit theft or fraud. Today, the internet facilitates identity theft.The FBI uses both its cyber and criminal resources—along with its intelligence capabilities—to identify and stop crime groups in their early stages.

"Going Dark"

Law enforcement has the legal authority to intercept and access communications and information pursuant to court orders, but often lacks the technical ability to carry out those orders because of a fundamental shift in communications services and technologies. This scenario is often called "Going Dark" and can hinder access to valuable information that may help identity and save victims, reveal evidence to convict perpetrators, or exonerate the innocent.

Computer Fraud and Abuse Act of 1986 (CFAA)

18 U.S.C. §1030

The Computer Fraud and Abuse Act (CFAA) was enacted in 1986, as an amendment to the first federal computer fraud law, to address hacking. Over the years, it has been amended several times, most recently in 2008, to cover a broad range of conduct far beyond its original intent. The CFAA prohibits intentionally accessing a computer without authorization or in excess of authorization, but fails to define what "without authorization" means.

TABLE 1. SUMMARY OF CFAA PENALTIES

Offense	Section	Sentence*
Obtaining National Security Information	(a)(1)	10 (20) years
Accessing a Computer and Obtaining Information	(a)(2)	1 or 5 (10)
Trespassing in a Government Computer	(a)(3)	1 (10)
Accessing a Computer to Defraud & Obtain Value	(a)(4)	5 (10)
Intentionally Damaging by Knowing Transmission	(a)(5)(A)	1 or 10 (20)
Recklessly Damaging by Intentional Access	(a)(5)(B)	1 or 5 (20)
Negligently Causing Damage & Loss by Intentional Access	(a)(5)(C)	1 (10)
Trafficking in Passwords	(a)(6)	1 (10)
Extortion Involving Computers	(a)(7)	5 (10)

* The maximum prison sentences for second convictions are noted in parentheses.

https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf

Computer Fraud and Abuse Act (CFAA)

1030(a)(7) Summary (Felony)

1. With intent to extort money or any other thing of value
2. transmits in interstate or foreign commerce a communication
3. containing a:
   threat to damage a protected computer
   OR
   threat to obtain or reveal confidential information without or in excess of authorization
   OR
   demand or request for money or value in relation to damage done in connection with the extortion.

1030(a)(2) Summary (Misd.)

1. Intentionally access a computer
2. without or in excess of authorization
3. obtain information
4. from
   financial records of financial institution or consumer reporting agency
   OR
   the U.S. government
   OR
   a protected computer

↓

(Felony)

5. committed for commercial advantage or private financial gain
   OR
   committed in furtherance of any criminal or tortious act
   OR
   the value of the information obtained exceeds $5,000

TABLE 2. PENALTY SUMMARY FOR SECTION 1030(A)(5)

Section	Statutory Penalty
Intentional Damage § 1030(a)(5)(A)	10-year felony if one of six special harms exist; otherwise, misdemeanor 20-year felony for subsequent convictions or serious bodily injury Life imprisonment if cause, or attempts to cause, death
Reckless Damage § 1030(a)(5)(B)	5-year felony if one of six special harms exist; otherwise, misdemeanor 20-year felony for subsequent convictions
Damage § 1030(a)(5)(C)	Misdemeanor 10-year felony for subsequent convictions

Offenders who intentionally or recklessly cause damage, and therefore violate section 1030(a)(5)(A) or (B), are guilty of a misdemeanor and may be

https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf

The Wiretap Act

1968

The federal Wiretap Act governs all wiretaps, including those used by state or local officials pursuant to state court authorizations.

It is a federal crime to wiretap or to use a machine to capture the communications of others without court approval, unless one of the parties has given their prior consent. It is likewise a federal crime to use or disclose any information acquired by illegal wiretapping or electronic eavesdropping.

2511(1)(a) Summary

1. Intentional
2. interception (or endeavoring or procuring another to intercept)
3. of the contents
4. of a wire, oral or electronic communication
5. by use of a device.

2511(1)(c) Summary

1. Intentional disclosure
2. of illegally intercepted communication
3. knowledge or reason to know the intercept was illegal

2511(1)(d) Summary

1. Illegal interception of communication
2. knowledge or reason to know the intercept was illegal
3. use of the contents.

https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf

CYBERCRIME RESOURCES

Federal Bureau of Investigation
https://www.fbi.gov/investigate/cyber

Department of Justice Office of Legal Education
https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf

National Association of Criminal Defense
https://www.nacdl.org/Landing/ComputerFraudandAbuseAct

The International Criminal Police Organization
https://www.interpol.int/en/Crimes/Cybercrime

Electronic Privacy Information Center
https://epic.org/privacy/wiretap/98-326.pdf

Organization of American States
https://www.oas.org/juridico/spanish/cyber/cyb10_slide.pdf

Dept. of Justice Computer Crime and Intellectual Property Section
https://www.justice.gov/criminal-ccips/reporting-computer-internet-related-or-intellectual-property-crime