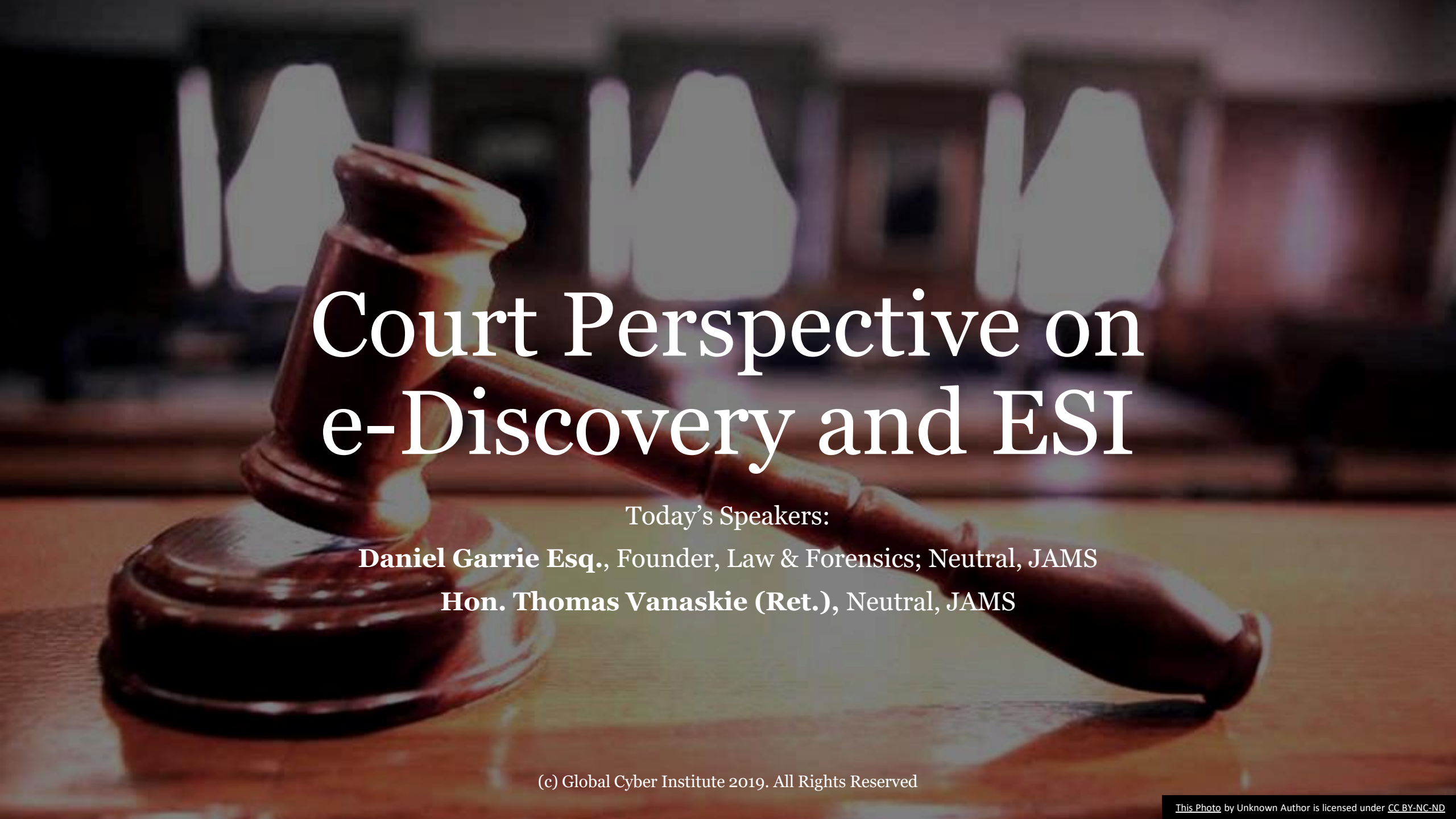


Court Perspective on e-Discovery and ESI

Today's Speakers:

Daniel Garrie Esq., Founder, Law & Forensics; Neutral, JAMS

Hon. Thomas Vanaskie (Ret.), Neutral, JAMS

(c) Global Cyber Institute 2019. All Rights Reserved

This Photo by Unknown Author is licensed under CC BY-NC-ND



Daniel Garrie Esq.
Founder, Law & Forensics
Neutral, JAMS



Hon. Thomas Vanaskie (Ret.)
Neutral, JAMS

(c) Global Cyber Institute 2019. All Rights Reserved

"In 2005 and even after the 2006 (FRCP) rule change, lawyers were still coming into court – those of a certain age – pointing to their bald head and saying, 'I'm sorry judge I still don't understand how to deal with emails and ESI.'"

Hon. Andrew J. Peck (Ret.), Southern District of New York

(c) Global Cyber Institute 2019. All Rights Reserved



What is E-Discovery?

- Electronic Discovery or “E-Discovery” is the general term used to describe the preservation and production of electronically stored information (“ESI”), typically done during the discovery phase of litigation.
- ESI can include: e-mails, texts, chats, instant messages, files, website activity and history, information posted on social networking websites, videos, audio, images, spreadsheets, powerpoints, database (structured) data, and (very importantly) metadata (data about data).

(c) Global Cyber Institute 2019. All Rights Reserved

This Photo by Unknown Author is licensed under CC BY-NC-ND



Common Mistakes Made in the Courtroom

(c) Global Cyber Institute 2019. All Rights Reserved

This Photo by Unknown Author is licensed under CC BY-SA



This Photo by Unknown Author is licensed under CC BY-NC

Federal Rules of Evidence

- Rule 104. Preliminary Questions

(a) In General. The court must decide any preliminary question about whether a witness is qualified, a privilege exists, or evidence is admissible. In so deciding, the court is not bound by evidence rules, except those on privilege.

(b) Relevance That Depends on a Fact. When the relevance of evidence depends on whether a fact exists, proof must be introduced sufficient to support a finding that the fact does exist. The court may admit the proposed evidence on the condition that the proof be introduced later.

(c) Conducting a Hearing So That the Jury Cannot Hear It. The court must conduct any hearing on a preliminary question so that the jury cannot hear it if:

(1) the hearing involves the admissibility of a confession;

(2) a defendant in a criminal case is a witness and so requests; or

(3) justice so requires.

(d) Cross-Examining a Defendant in a Criminal Case. By testifying on a preliminary question, a defendant in a criminal case does not become subject to cross-examination on other issues in the case.

(e) Evidence Relevant to Weight and Credibility. This rule does not limit a party's right to introduce before the jury evidence that is relevant to the weight or credibility of other evidence.

(c) Global Cyber Institute 2019. All Rights Reserved



This Photo by Unknown Author is licensed under CC BY-NC-ND

Federal Rules of Evidence

- Rule 902. Evidence that is Self-Authenticating

The following items of evidence are self-authenticating; they require no extrinsic evidence of authenticity in order to be admitted:

(13) Certified Records Generated by an Electronic Process or System. A record generated by an electronic process or 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). The proponent must also meet the notice requirements of Rule 902(11).

(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).

(c) Global Cyber Institute 2019. All Rights Reserved

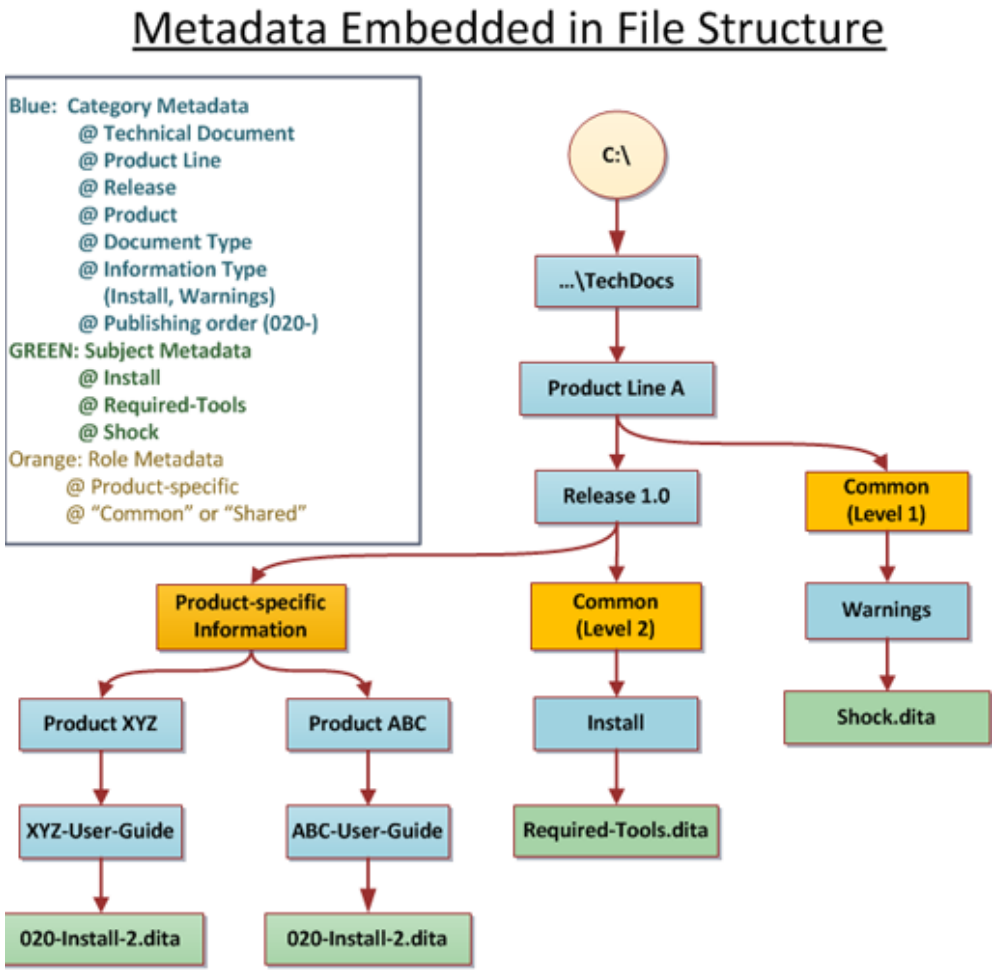


Not Determining the Owner/Creator of ESI

- As systems grow more interconnected and complex, determining the actual owner or creator of ESI will also become more difficult.
- Under Federal Rules of Evidence 803(6), there is a need for testimony from a custodian or other qualified witness, able to testify as to the source of the information, business circumstances associated with the record's creation and the degree of regularity of the business practice and the record making and maintaining of records.
- It becomes a threshold issue to determine who – or what – is the creator (or creators) of content so that a determination of authenticity can proceed.

(c) Global Cyber Institute 2019. All Rights Reserved

This Photo by Unknown Author is licensed under CC BY-SA-NC



Authentication Tools

- Hashing:
  - A hash algorithm takes a le as input and calculates a unique identifier for that le called a "hash value." Any modification to the le – even changing a single bit out of ten gigabytes – will result in a completely different hash value, indicating that the file has been changed. Hashing is not a test for authenticity in its own right. Rather, hashing can be a means of efficiently determining whether two files are exact duplicates of each other, or whether a single file has been altered.
- System Metadata:
  - System metadata are created by the operating systems that run computers, servers and other devices. All electronic files include metadata that convey information, such as the dates a file was created, last modified and last accessed. It's a useful checkpoint for determining authenticity. However, metadata can be unreliable and is usually subject to manipulation and non-obvious deletion.
- Encryption:
  - Encryption uses a secret key to scramble the contents of a le so that only those with access to the key may read the file.

(c) Global Cyber Institute 2019. All Rights Reserved

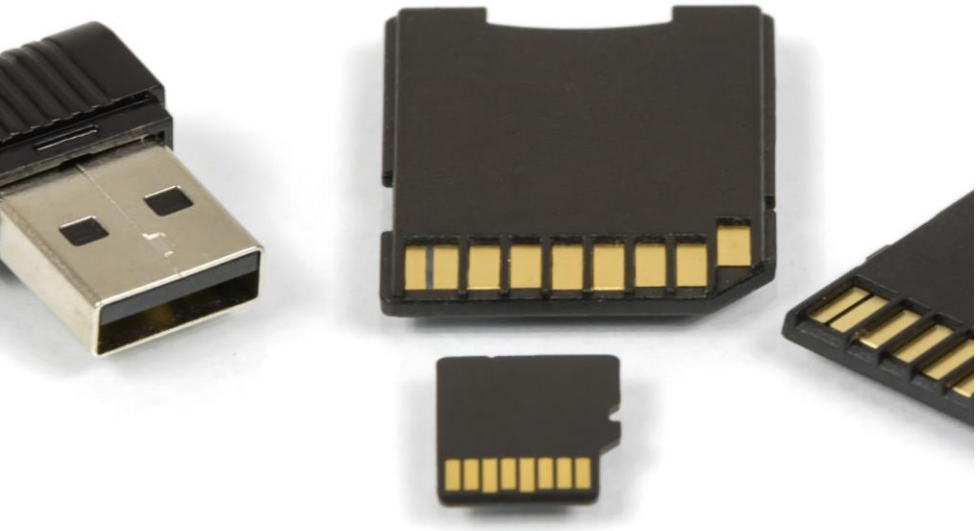


This Photo by Unknown Author is licensed under CC BY-NC-ND

Not Understanding the Limits of Technology

- Although technology can provide many tools to assist in establishing authenticity, it is important to understand these tools and their potential role in the authentication process, as well as their limitations.
- On the next slide, we'll take a look at some of these tools.

(c) Global Cyber Institute 2019. All Rights Reserved



Not Understanding the Limits of Technology (cont.)

- Digital Signatures
  - A document or file may be digitally signed using the party's private signature key, creating a digital signature that is stored within document. It indicates that someone with access to the key has signed the document, but keys can be stolen or borrowed (copied), frequently without the knowledge of the owner of the key.
- Storage
  - The act of storing the information does not establish authenticity; the validity of the information depends on the process that placed it there.
    - Look back to FRE 902(13) and (14).
- Trusted Time Stamping
  - The process of creating a cryptographic binding between a verifiable time value and an associated data-set or record. It is a way to demonstrate the unchanged condition of ESI, or conversely to demonstrate change if it has occurred.

(c) Global Cyber Institute 2019. All Rights Reserved

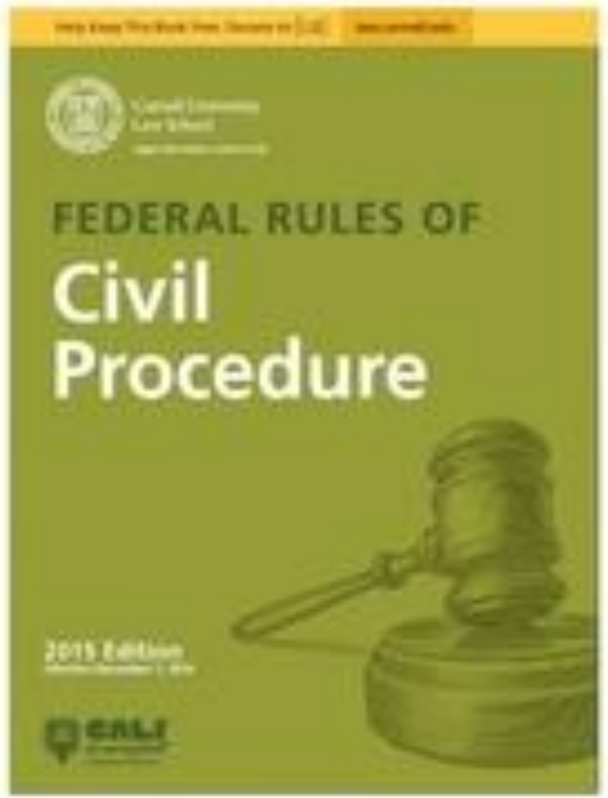


Not Understanding the Threat Landscape

- In many ways, the threats of manipulating ESI are similar to the issues (e.g. forgery) faced with paper records.
- Types of threats include:
  - Anti-Forensics
  - System Interconnectivity
  - Large, Complex, Systems Containing Massive Quantities of Data
  - Hard Drive Wiping Programs

(c) Global Cyber Institute 2019. All Rights Reserved

This Photo by Unknown Author is licensed under CC BY



This Photo by Unknown Author is licensed under CC BY-NC-ND

Federal Rules of Civil Procedure

(c) Global Cyber Institute 2019. All Rights Reserved

Rule 26. Duty to Disclose; General Provisions Governing Discovery



(b) Discovery and Scope of Limits

(1) *Scope in General.* Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and **proportional to the needs of the case**, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible in evidence to be discoverable.

(2) *Limitations on Frequency and Extent.*

[. . .]

(B) *Specific Limitations on Electronically Stored Information.* A party need not provide discovery of electronically stored information from sources that the party **identifies as not reasonably accessible because of undue burden or cost.** [. . .]

(C) *When Required.* On motion or on its own, the court must limit the frequency or extent of discovery otherwise allowed by these rules or by local rule if it determines that:

(i) the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive;

(ii) the party seeking discovery has had ample opportunity to obtain the information by discovery in the action; or

(iii) the proposed discovery is outside the scope permitted by Rule 26(b)(1).

(c) Global Cyber Institute 2019. All Rights Reserved

This Photo by Unknown Author is licensed under CC BY-SA-NC

Rule 26 (b)(1) – Narrows the Scope of Discovery



This Photo by Unknown Author is licensed under CC BY

- Retains
  - The standard that “parties may obtain discovery regarding any non privileged matter that is relevant to any party’s claim or defense”
- Drops
  - The requirement to produce evidence “reasonably calculated to lead to the discovery of admissible evidence”
  - Adds a "proportionality" requirement to the scope of permissible discovery

(c) Global Cyber Institute 2019. All Rights Reserved



This Photo by Unknown Author is licensed under CC BY

Factors To Determine What Is "Proportional"

- The factors used to determine proportionality include:
  - The importance of the issues at stake in the action,
  - the amount in controversy,
  - the parties' relative access to relevant information,
  - the parties' resources,
  - the importance of the discovery in resolving the issues, and
  - whether the burden or expense of the proposed discovery outweighs its likely benefit

(c) Global Cyber Institute 2019. All Rights Reserved



Limitations on Broad Discovery Requests or Objections

- Parties can no longer use broad objections to avoid discovery; the days of simply stating the ‘request is not proportional’ are over. Correspondingly, a party may not simply state that information requested is relevant and expect to be granted discovery.
- Both parties need to be prepared to argue why and how requests are, or are not, proportional and relevant. One thing is sure: courts are as committed as ever to ensuring that parties receive the appropriate amount of information they need to successfully argue their cases.

(c) Global Cyber Institute 2019. All Rights Reserved



Rule 34(a)

- (a) In General. A party may serve on any other party a request within the scope of Rule 26(b):
    - to produce and permit the requesting party or its representative to inspect, copy, test, or sample the following items in the responding party's possession, custody, or control:
        - 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; or
        - any designated tangible things
- "Possession, custody, or control" can mean something very different depending on which Circuit you're in.
- Three current tests:
    - "Legal Right"
    - "Legal Right plus Notification"
    - "Practical Ability."

(c) Global Cyber Institute 2019. All Rights Reserved



This Photo by Unknown Author is licensed under CC BY-SA

Rule 34(b)(2)

(2) *Responses and Objections*.

(B) *Responding to Each Item*. For each item or category, the response must either state that **inspection and related activities will be permitted** as requested or **state with specificity** the grounds for objecting to the request, including the reasons. The responding party may state that it will produce copies of documents or of electronically stored information instead of permitting inspection. The production must then be completed no later than the time for inspection specified in the request or another reasonable time specified in the response.

(C) *Objections*. An objection must state **whether any responsive materials are being withheld** on the basis of that objection. An objection to part of a request must specify the part and permit inspection of the rest.

(c) Global Cyber Institute 2019. All Rights Reserved



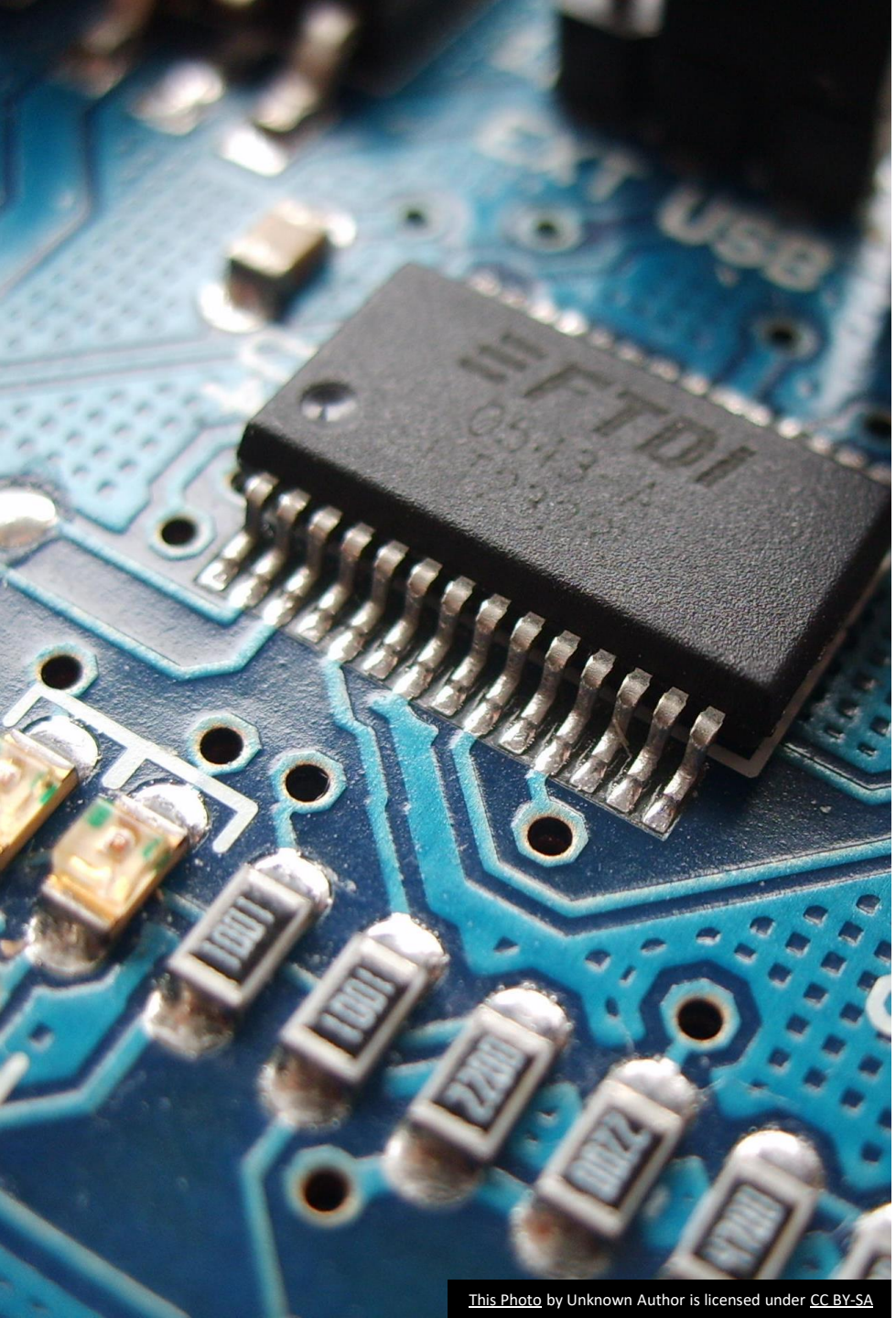
This Photo by Unknown Author is licensed under CC BY

Rule 34 & The Request For Production

4 Primary Takeaways From the Updated Rule 34

1. Provide greater specificity in objections;
    - A responding party may need to identify what in a request is "vague and ambiguous" or "unduly burdensome" — not simply that the request as a whole is.
2. Produce responsive documents within a "reasonable time"; and
    - Under the new rules, parties can no longer state that documents will be produced in the future without committing to a certain date. Parties that wish to produce documents in lieu of inspection, now must specify when that production will occur.
3. Give an express confirmation on whether documents are being withheld based on a stated objection.
    - This heightened standard forces litigants to consider their objections to requests for production, which will help expedite the litigation process.
4. A good practice is to state what you **are** producing, the steps you **are** taking to collect and produce data, and then let the other side critique the sufficiency. Trying to determine what you are "withholding" based on the vagueness of the request can be a fruitless exercise.

(c) Global Cyber Institute 2019. All Rights Reserved



This Photo by Unknown Author is licensed under CC BY-SA

Rule 37(e)

- Rule 37 (e): **Failure to preserve electronically stored information.**

  If electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve the information, and the information cannot be restored or replaced through additional discovery, the court may:

  (1) Upon a **finding of prejudice** to another party from loss of the information, order measures no greater than necessary to **cure the prejudice**; **OR**

  (2) Only upon a finding that **the party acted with the intent to deprive another party of the information's** use in the litigation:

  (A) presume that the lost information was unfavorable to the party;

  (B) instruct the jury that it may or must presume the information was unfavorable to the party; or

  (C) dismiss the action or enter a default judgment.

(c) Global Cyber Institute 2019. All Rights Reserved



This Photo by Unknown Author is licensed under CC BY-SA

Parties Must Take "Reasonable Steps"

- At first glance, the requirement that a party only take "reasonable steps" to preserve **relevant** ESI—and not perfect steps to preserve—seems like a prudent obligation under amended Rule 37(e).
- However, it has proven to be difficult for courts to determine when a party has met its "reasonable steps" obligation. Making this determination can be difficult because the definition of "reasonable steps" varies from case to case, and party to party.

(c) Global Cyber Institute 2019. All Rights Reserved



This Photo by Unknown Author is licensed under CC BY-SA-NC

Parties Must Take "Reasonable Steps"

- In 2012, the Second Circuit's decision in *Chin v. Port Authority of New York & New Jersey*, 2012 WL 2760776 (2d Cir. July 10, 2012), overturned a previous ruling by Judge Shira Scheindlin (Ret.), Southern District of New York, and halted the momentum of a growing body of law holding that the failure to issue a litigation hold notice is *per se* gross negligence.
- Instead, the Second Circuit reasoned, lower courts should adhere to the earlier standard under which the trial court would consider the failure to issue a litigation hold notice as one of several factors in analyzing the totality of the circumstances causing the document destruction. Failure to issue a hold notice is therefore no longer necessarily grossly negligent.

(c) Global Cyber Institute 2019. All Rights Reserved



Sanctions Require a Finding of Intent or Bad Faith

- Even if ESI is destroyed, courts will not impose sanctions (harsher actions listed in 37(e)(2)) unless there is a finding that the party acted intentionally to prevent the evidence from being used by an opposing party. The courts have set a high bar for what constitutes intent, it takes more than suspicious conduct.
- While honest mistakes are not enough to warrant sanctions, when it happens that a party acts irresponsibly to preserve evidence, a court may infer a finding of intent.

(c) Global Cyber Institute 2019. All Rights Reserved

This Photo by Unknown Author is licensed under CC BY-NC



This Photo by Unknown Author is licensed under CC BY-NC-ND

Inherent Power of the Court to Impose Sanctions

- "Courts of justice are universally acknowledged to be vested, by their very creation, with power to impose silence, respect, and decorum, in their presence, and submission to their lawful mandates. These powers are governed not by rule or statute but by the control necessarily vested in courts to manage their own affairs so as to achieve the orderly and expeditious disposition of cases."
  - *Chambers v. NASCO, Inc.*, 501 U.S. 32 (1991) (internal citations omitted)
- In applying this principle to the spoliation of ESI, Judge Francis found that "If, notwithstanding this reasoning, Rule 37(e) were construed not to apply to the facts here, I could nevertheless exercise inherent authority to remedy spoliation under the circumstances presented."
  - *CAT3, LLC v. Black Lineage, Inc.*, __F.Supp.3d__(S.D.N.Y. 2016)(2016 WL 154116)

(c) Global Cyber Institute 2019. All Rights Reserved



Ethics & ESI

Model Rules of Professional Responsibility

(c) Global Cyber Institute 2019. All Rights Reserved

This Photo by Unknown Author is licensed under CC BY-NC-ND



This Photo by Unknown Author is licensed under CC BY

Why Does E-Discovery Create Ethical Issues?

- Over 99% of information now in digital form – nearly 70% may never be reduced to paper (hard copy) form.
- Information now created in a variety of formats: word processing, spreadsheets, databases, text messages, digital images, audio, video, websites, social networking, tweets, faxes, YouTube, etc. - known as Electronically Stored Information (ESI)
- All of this ESI is stored on a multitude of devices, including desktop computers, laptops, mobile devices, flash drives, voicemail, email, printers, scanners, copiers, CDs, DVDs AND on an employee's home computer and personal devices.
- The field of electronic discovery is still in its infancy , but the Model Rules of Professional Conduct can act as a roadmap to chart a safe course from the starting point of a case to the end of the litigation journey.

(c) Global Cyber Institute 2019. All Rights Reserved



Ethics & ABA Model Rules

(c) Global Cyber Institute 2019. All Rights Reserved

This Photo by Unknown Author is licensed under CC BY-NC-ND



This Photo by Unknown Author is licensed under CC BY-NC-ND

Rule 1.1: Competence

- A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.
- Cmt [8] "...[t]o 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..."

(c) Global Cyber Institute 2019. All Rights Reserved



This Photo by Unknown Author is licensed under CC BY

1.1, Cmt [8]: Maintaining Competence

- 25+ states adopted the amended cmt 8 or otherwise require attorneys to stay abreast of changes in technology relating to law practice.

- For example, the State Bar of California outlined nine areas that attorneys are to be able to perform to ethically represent a client in a matter involving e-discovery:
  - Initially assess e-discovery needs and issues;
  - Implement or cause to implement appropriate electronically stored information (ESI) preservation procedures;
  - Analyze and understand a client's ESI systems and storage;
  - Advise the client on available options for collection and preservation of ESI;
  - Identify custodians of potentially relevant ESI;
  - Engage in a competent and meaningful meet-and-confer with opposing counsel concerning an e-discovery plan;
  - Perform data searches;
  - Collect responsive ESI in a manner that preserves the integrity of that ESI; and
  - Produce responsive nonprivileged ESI in a recognized and appropriate manner.

(c) Global Cyber Institute 2019. All Rights Reserved



This Photo by Unknown Author is licensed under CC BY-SA

1.1, Cmt [8]: Maintaining Competence

The State Bar of California Standing Committee on Professional Responsibility and Conduct Formal Opinion No. 2015-193

- An attorney's obligations under the ethical duty of competence evolve as new technologies develop and become integrated with the practice of law.
- Attorney competence related to litigation generally requires, among other things, and at a minimum, a basic understanding of, and facility with, issues relating to e-discovery, including the discovery of electronically stored information ("ESI").
- On a case-by-case basis, the duty of competence may require a higher level of technical knowledge and ability, depending on the e-discovery issues involved in a matter, and the nature of the ESI. Competency may require even a highly experienced attorney to seek assistance in some litigation matters involving ESI.
- An attorney lacking the required competence for e-discovery issues has three options: (1) acquire sufficient learning and skill before performance is required; (2) associate with or consult technical consultants or competent counsel; or (3) decline the client representation. Lack of competence in e-discovery issues also may lead to an ethical violation of an attorney's duty of confidentiality.

(c) Global Cyber Institute 2019. All Rights Reserved



Rule 5.3: Responsibilities Regarding Nonlawyer Assistance

- A lawyer using nonlawyers outside of his firm to assist in rendering legal services to a client "must make reasonable efforts to ensure that the services are provided in a manner that is compatible with the lawyer's professional obligations."
  - This means due diligence in selecting e-discovery vendors and active supervision of their work.
- The duty of competence also includes the duty to supervise. Lawyers are ethically obligated to supervise their employees and subordinates to ensure compliance with ethical rules, and that obligation extends to electronic communications.

(c) Global Cyber Institute 2019. All Rights Reserved

This Photo by Unknown Author is licensed under CC BY



This Photo by Unknown Author is licensed under CC BY-NC-ND

Duty to Supervise

- This would apply to outside review companies or e-discovery vendors utilized to assist with document review. Failing to provide adequate training, oversight, and quality control of e-discovery vendors or document reviewers can result in preservation and production errors and undermine counsel's duty to provide competent representation.
- Enlisting the services of an outside vendor to assist in review or coding does not discharge an attorney's obligation to provide competent representation.
- Attorneys must take steps to ensure the reasonable accuracy of reviewers' work through adequate oversight and quality control measures. There are well-publicized cases of e-discovery malpractice lawsuits against law firms arising at least in part from vendor errors.

(c) Global Cyber Institute 2019. All Rights Reserved



Rule 1.6: Confidentiality of Information

- "…A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client…"
  - Protecting privilege in the era of electronic discovery is growing increasingly difficult given the volume of data.
  - Cmt [18] acknowledged that “lawyers cannot guarantee electronic security any more than lawyers can guarantee the physical security of documents stored in a file cabinet or offsite storage facility.”

(c) Global Cyber Institute 2019. All Rights Reserved

This Photo by Unknown Author is licensed under CC BY-SA-NC



This Photo by Unknown Author is licensed under CC BY-SA-NC

Rule 1.6, Cmt [18]: Acting Competently to Preserve Confidentiality

- Cmt 18 sets forth a list of nonexclusive factors to be considered in determining whether a lawyer's efforts to prevent disclosure are reasonable, including:
  - the sensitivity of the information,
  - the likelihood of disclosure if additional safeguards are not used,
  - the cost of using additional safeguards, the difficulty of implementing the safeguards, and
  - the extent to which the safeguards adversely affect the lawyer's ability to represent clients.

(c) Global Cyber Institute 2019. All Rights Reserved

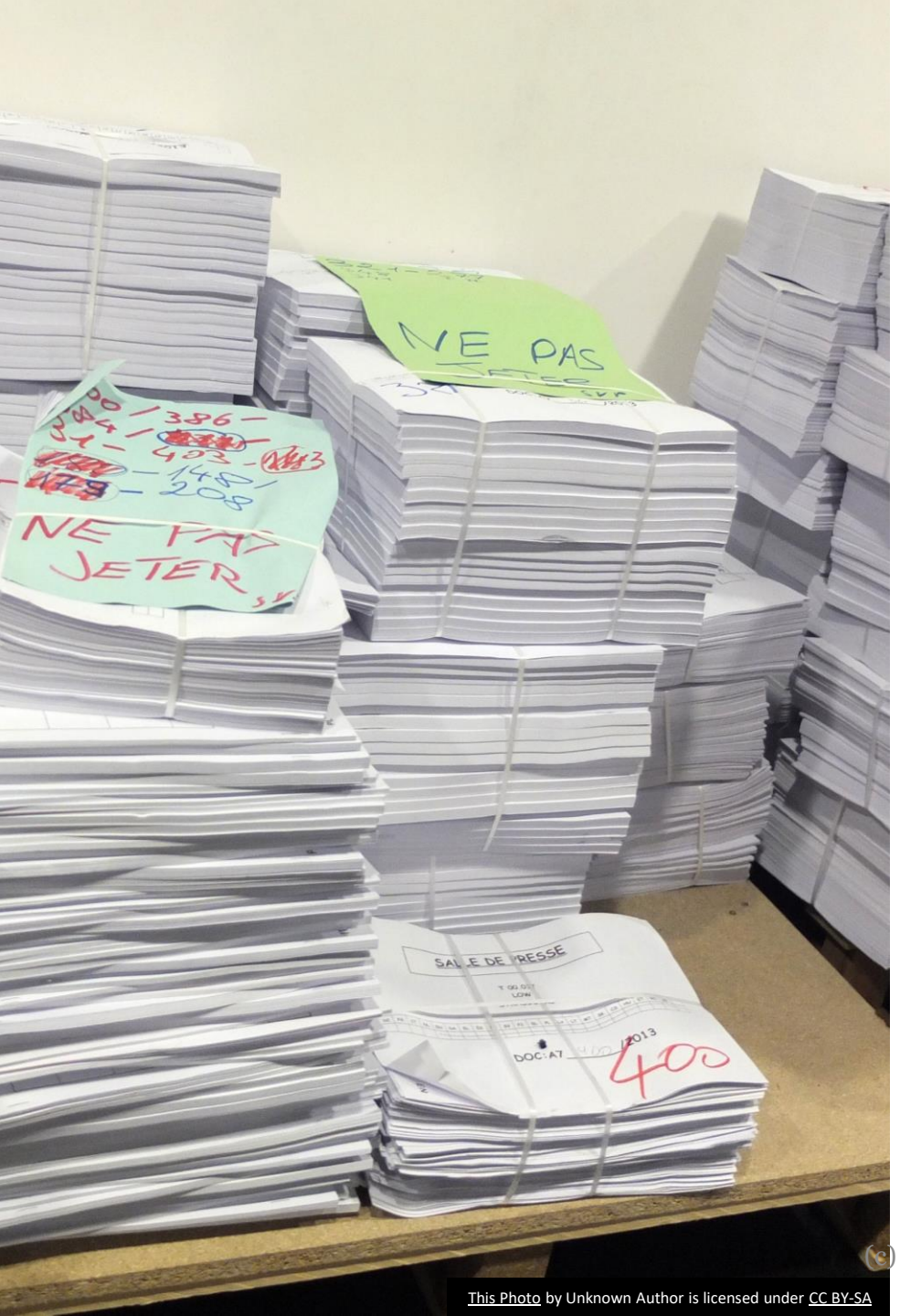


This Photo by Unknown Author is licensed under CC BY-SA

Duty of Confidentiality: Privilege Issues

- Protecting privilege in the era of electronic discovery is growing increasingly difficult given the volume of data
  - Electronic documents can create a greater risk of inadvertent waiver of privilege, and the need to "clawback" documents.
    - Claw-back Agreement: An agreement that protects against waiver of privilege and/or work production protections when inadvertent production occurs.
- Fed.R.Evid. 502 provides that inadvertent disclosure in a federal proceeding does not waive attorney- client privilege provided:
  - The disclosure was indeed inadvertent
  - The holder of the disclosure took reasonable steps to prevent the disclosure
  - The holder promptly took steps to rectify the error

(c) Global Cyber Institute 2019. All Rights Reserved



This Photo by Unknown Author is licensed under CC BY-SA

Duty of Confidentiality: Privilege Issues

FRE 502(d) Orders

FRE 502 was enacted in 2008 in response to widespread complaints that the cost of protecting against waivers of **attorney-client privilege** or **work product protection** during discovery has become prohibitive because of the concern that even an inadvertent or insubstantial disclosure waives protected communications or information, particularly in cases involving e-discovery, which may encompass a large number of documents. Rule 502(a) and (b) explain under what circumstances the unintentional disclosure of privileged information does and does not constitute a waiver of privilege.

Under Rule 502(d), however, the court may issue an order providing that a party's disclosure of documents protected by the attorney-client privilege or work product protection does not waive the privilege (unless there was an intent to waive the privilege). According to the Advisory Committee notes, this is true even when a party produced documents without conducting any screening for privileged material (see *Advisory Committee Notes to FRE 502(d)*).

A Rule 502(d) order is a unique discovery tool because:

- The no-waiver effect also applies in other federal and state court proceedings.
- The parties may incorporate into the order a specific and detailed agreement regarding its scope and effect in the litigation.
- Privileged documents must be returned to the disclosing party "irrespective of the care taken by" the party in reviewing them prior to production.
- The court may issue the order **sua sponte**, without the parties' agreement.

(c) Global Cyber Institute 2019. All Rights Reserved



Case Law

(c) Global Cyber Institute 2019. All Rights Reserved

This Photo by Unknown Author is licensed under CC BY-SA



This Photo by Unknown Author is licensed under CC BY-NC-ND

Klipsch Group v. ePRO E-Commerce, No. 16-3637-cvNo. 16-3726-cv (2d Cir. Jan. 25, 2018)

- Facts: The plaintiff, a manufacturer of headphones, sued a subsidiary of the defendant on the ground that it was selling counterfeit plaintiff headphones. While the trial court was "initially" persuaded by the defendant that the actual damages in the matter were about "$8,000 worldwide," the defendant's "failure to comply with its discovery obligations began to cast doubt on the reliability" of its valuation, causing the court to give weight to the plaintiff's allegation that the defendant had "sold at least $5 million in counterfeit or otherwise infringing" products. The defendant's discovery failure was in not putting into place a litigation hold, so that the defendant's initial production was of a mere 500 documents, including no "original sales documents" but, instead, "spreadsheets created specifically" for the litigation "that purported to list all relevant sales" but did not. An e-discovery vendor eventually retained by the defendant found "an additional 40,000 documents, including 1,236 original sales documents;" some of the documents contradicted the deposition testimony of the defendant's CEO and suggested that defendant "had misidentified the suppliers of the counterfeit products" and "had artificially limited" its discovery vendor's "investigation into its electronic records."
- Holding: the U.S. Court of Appeals for the Second Circuit affirmed the Southern District of New York's order that even though "the likely valuation of actual damages" caused by the defendant's discovery violations was $25,000, the defendant additionally had to pay the plaintiff a total of $5 million as "compensation" for "discovery efforts" the plaintiff had to take solely because of the defendant's misconduct, as well as for "restraint … appropriate to secure" the plaintiff's "likely recovery of treble damages and attorney fees at the conclusion of the case.

(c) Global Cyber Institute 2019. All Rights Reserved



This Photo by Unknown Author is licensed under CC BY-SA

Lawyer's e-discovery error led to release of confidential info on thousands of Wells Fargo clients

- In 2017, a lawyer representing Wells Fargo in a lawsuit subpoena request inadvertently turned over confidential information for thousands of Wells Fargo bank clients, including customer names, Social Security numbers and financial data to a lawyer for a defamation plaintiff.
- The lawyer used an e-discovery vendor's software to review what she believed to be a complete set of results and marked some documents as privileged and confidential. She did not realize she was using "a view" that showed a limited set of documents. Thus providing documents that had not been reviewed for confidentiality and privilege.

(c) Global Cyber Institute 2019. All Rights Reserved



Questions?

(c) Global Cyber Institute 2019. All Rights Reserved.



Daniel B. Garrie, Esq.
Law & Forensics -- Executive Managing Partner
JAMS – Special Master, Neutral, Arbitrator
Contact:
W: (855) 529 - 2466
M: (215) 280 – 7033
E: daniel@lawandforensics.com
URL: www.lawandforensics.com

LAW & FORENSICS
Computer Forensics, E-Discovery, Cyber Security

B.A., Computer Science, Brandeis Uni.
M.A., Computer Science Brandies Uni.
J.D., Rutgers School of Law

Daniel Garrie is the founder and Executive Managing Partner of Law & Forensics LLC and is a Special Master, Neutral, and Arbitrator with JAMS. At Law & Forensics, Mr. Garrie is paving the way when it comes to the most pressing cyber security, forensic, and legal issues. He is also a Partner at Zeichner Ellman & Krause, where he heads their global cyber security practice. Mr. Garrie is also an adjunct professor at the Cardozo School of Law and at Rutgers Law School.

Mr. Garrie has built and sold several Internet security, e-commerce, and search technology startups. He is also the Steering Committee Member of the Global Cyber Institute. Mr. Garrie works to fulfill the mission of the GCI, which is to teach and develop leaders in the fields of technology and cybersecurity. He also works as a Strategic Partner for Quorumm Ventures and a Board of Governors member for the Organization of Legal Professionals. He is a nationally recognized educator and lecturer on various topics including computer software, cyber security, e-discovery, forensics, emerging internet and mobile technologies, and cyber warfare. He is the Editor in Chief of the Journal of Law & Cyber Warfare, a fellow at the Ponemon Information Privacy Institute, a distinguished neutral with CPR, and on the editorial board of the Beijing Law Review.

Mr. Garrie's scholarship in e-discovery, forensics, and cyber security is frequently cited by the bench and the bar, including: Arrivalstar v. US, US v. Briggs, Coast Professional, Inc. v. US, Genger v. TR Investors, LLC, John B. v. Goetz, and Northruop Grumman Computing Systems, Inc. v. US. Mr. Garrie is also frequently quoted by leading publications including the New York Times, Fortune, Forbes, and the Wall Street Journal on issues relating to cyber security and cyberwarfare.

(c) Global Cyber Institute 2019. All Rights Reserved



Hon. Thomas I. Vanaskie
JAMS – Neutral
Contact:
E: tvanaskie@jamsadr.com
URL: https://www.jamsadr.com/

Hon. Thomas I. Vanaskie (Ret.) joins JAMS after a distinguished 24-year career on the federal bench. Judge Vanaskie was sworn in as a circuit judge for the U.S. Court of Appeals for the Third Circuit in 2010. He previously served more than 16 years as a district judge for the U.S. District Court for the Middle District of Pennsylvania, including a seven-year term as chief judge. In his tenure on the bench, Judge Vanaskie oversaw hundreds of complex cases involving a wide range of practice areas, including appellate, business/commercial, class action/mass tort, employment, federal law, insurance, antitrust, intellectual property, civil rights and personal injury/torts.

Judge Vanaskie is particularly known for his expertise in technology and e-discovery. He is a contributing member of the Sedona Conference Working Group 1 on Electronic Document Retention and Production and Working Group 11 on Data Security and Privacy Liability. From 2001 to 2008, he served on the Information Technology Committee of the Judicial Conference of the United States, the policymaking body for U.S. courts. Judge Vanaskie was appointed chair of the Judicial Conference Information Technology Committee by the late Supreme Court Chief Justice William H. Rehnquist in 2005. He was a member of the Third Circuit Judicial Council and presently co-chairs its Information Technology Committee. Since 2007, he has served as an adjunct professor of law at the Penn State and Dickinson School of Law, presenting a course on electronic evidence. In 2016, Judge Vanaskie was appointed by Chief Justice John Roberts to serve on the Judicial Conference Space and Facilities Committee.

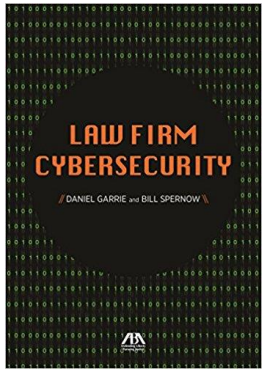
ADR Experience and Qualifications

- On the district court, Judge Vanaskie regularly conducted settlement conferences resulting in the resolution of hundreds of cases. As the chief judge, Judge Vanaskie won approval from his colleagues for the development of a court-sponsored mediation program.
- On the court of appeals, Judge Vanaskie was approached by his district judge colleagues to conduct mediations, and he successfully resolved several difficult and high-profile cases.

(c) Global Cyber Institute 2019. All Rights Reserved

Additional Reading

Books



[Law Firm Cybersecurity]



[Plugged In: Guidebook to Software and the Law]



[Software and the Law: Digital Forensic Investigations and E-Discovery]



[Dispute Resolution and e-Discovery]

Articles



[Arbitration, Mediation Can Resolve Cyber Coverage Disputes]



[Spearfishing Can Be Stopped Once You Remove the Bait]



[Mediators Need to Become 'Bilingual' to Resolve Smart Contracts]

Disclaimer

- This is not legal advice nor should it be considered legal advice
- This presentation and the comments contained therein represent only the personal views of the participants, and do not reflect those of their employers or clients
- This presentation is offered for educational and informational uses only

(c) Global Cyber Institute 2019. All Rights Reserved