Building Effective ESI Protocols: Addressing Modern Data, Metadata, Hyperlinks, and Cross-Platform Communications

Speakers:

- **Daniel B. Garrie, Esq.,** Founder, Law & Forensics; Neutral, JAMS; Adjunct Faculty, Harvard
- **Michael Gold, Esq.,** Partner, Jeffer Mangels Butler & Mitchell LLP
- **Warren Kruse,** MSc, CISSP, DFCP, EnCE, CCPA**,** Managing Director, iDiscovery Solutions
- **David Ko, Esq.,** Partner, Keller Rohrback
- **Patricia Antezana, Esq.,** Counsel, Reed Smith LLP

(c) 2026 Lexeprint Inc. All Rights Reserved.

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, as spoken and do not reflect those of their employers or clients.



This presentation is offered for educational and informational uses only.

(c) 2026 Lexeprint Inc. All Rights Reserved.

Speakers



Daniel B. Garrie, Esq.
Founder, Law & Forensics
Neutral, JAMS
Adjunct Faculty, Harvard



Michael Gold, Esq.
Partner, Jeffer Mangels Butler & Mitchell LLP



Warren Kruse,
Managing Director, iDiscovery Solutions



David Ko, Esq.
Partner, Keller Rohrback



Patricia Antezana, Esq.
Counsel, Reed Smith LLP

(c) 2026 Lexeprint Inc. All Rights Reserved.

Agenda

- Overview of ESI Protocols
- Key Issues In Modern ESI Protocols
- Best Practices: Drafting An ESI Protocol That Works For Modern Discovery

(c) 2026 Lexeprint Inc. All Rights Reserved.

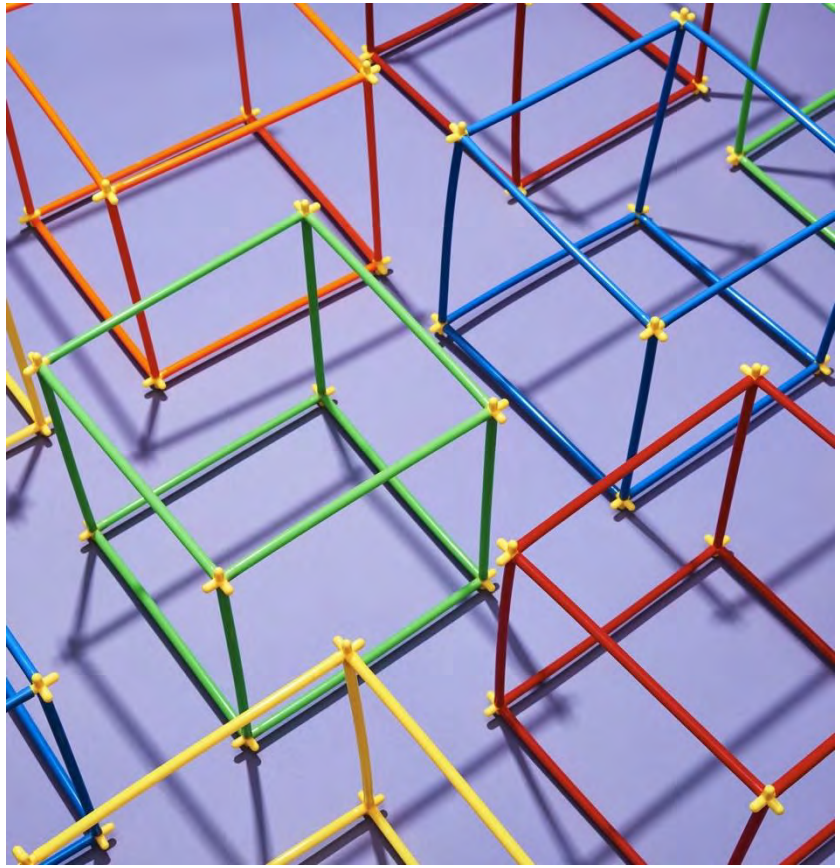


Overview of ESI Protocols

(c) 2026 Lexeprint Inc. All Rights Reserved.

What is an ESI Protocol?

- An ESI protocol is a negotiated document that expressly states how discovery of electronically stored information (ESI) will occur and may include parameters for preservation, collection, processing, review, and production during litigation.
- It serves as a roadmap for both parties.
- The parties will usually negotiate the protocol's terms before or during the FRCP 26(f) meet and confer and, upon agreement, ask that the court adopt it as an order.



(c) 2026 Lexeprint Inc. All Rights Reserved.

Why Implement ESI Protocols?

- Protocols may allocate:
  - Cost
  - Burden
  - preservation risk
  - re-production risk
- Silence in a protocol is not neutral, it usually favors the producing party.
- Courts increasingly expect parties to anticipate modern data issues, not litigate them later.



ESI protocols = less litigation = happy judge & clients

(c) 2026 Lexeprint Inc. All Rights Reserved.

Core Components of a Defensible ESI Protocol

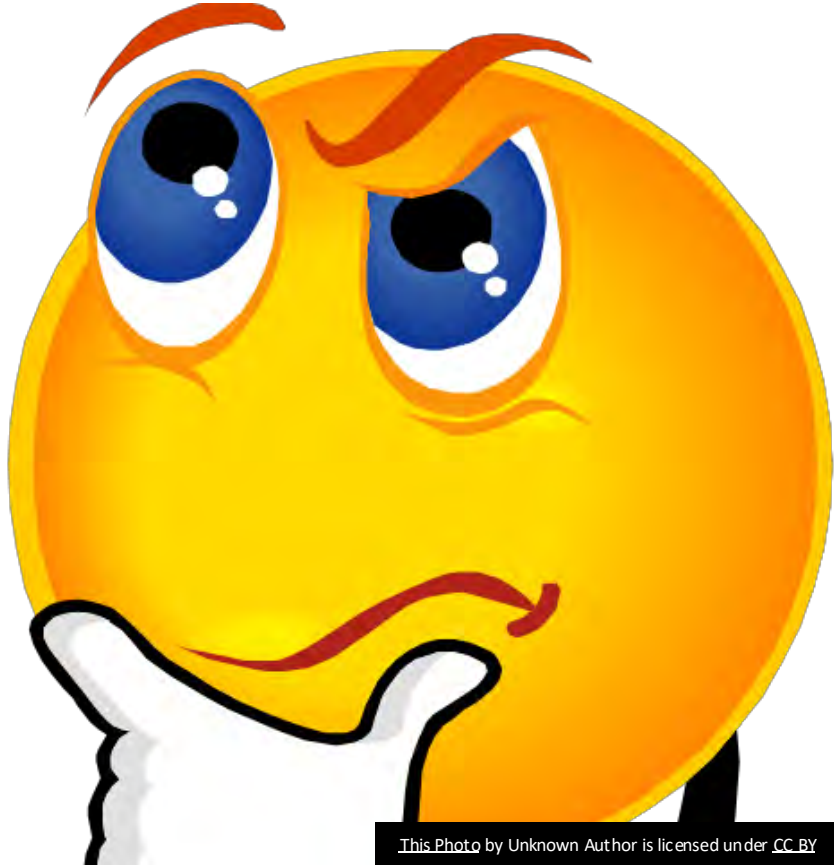
- An effective protocol must expressly address:
  - Data sources (systems, platforms, repositories)
  - Data relationships (messages ↔ files ↔ links ↔ versions)
  - Preservation scope and exclusions
  - Collection methodology and limitations
  - Production formats and metadata
  - Treatment of hyperlinks and linked content
  - Context preservation for collaboration data
  - Procedures for modifying scope as discovery evolves



(c) 2026 Lexeprint Inc. All Rights Reserved.

Why Protocols Got Harder

- Legacy protocols assume:
  - email is the primary record of communication
  - documents are static files
  - attachments are self-contained
- Modern litigation involves:
  - cloud-native collaboration platforms
  - dynamic, versioned content
  - links instead of attachments
  - conversations that span multiple tools
- Using "standard" protocol language without modification is no longer defensible



This Photo by Unknown Author is licensed under CC BY

(c) 2026 Lexeprint Inc. All Rights Reserved.



Key Issues In Modern ESI Protocols

(c) 2026 Lexeprint Inc. All Rights Reserved.

Collaboration Platforms Redefine "Where the Evidence Lives"

- Key characteristics:
  - Dynamic, multi-user editing (content changes over time)
  - Traditional "custodian" concept may not fit shared workspaces
  - Conversations can occur *inside* documents (comments/notes)
  - Files stored separately from the messages that reference them
  - Hyperlinks often replace attachments
  - Platforms may be portals to other systems (SharePoint/OneDrive/Dropbox, etc.)
  - Permissions and access are often more probative than authorship



(c) 2026 Lexeprint Inc. All Rights Reserved.

Custodial Assumptions No Longer Hold

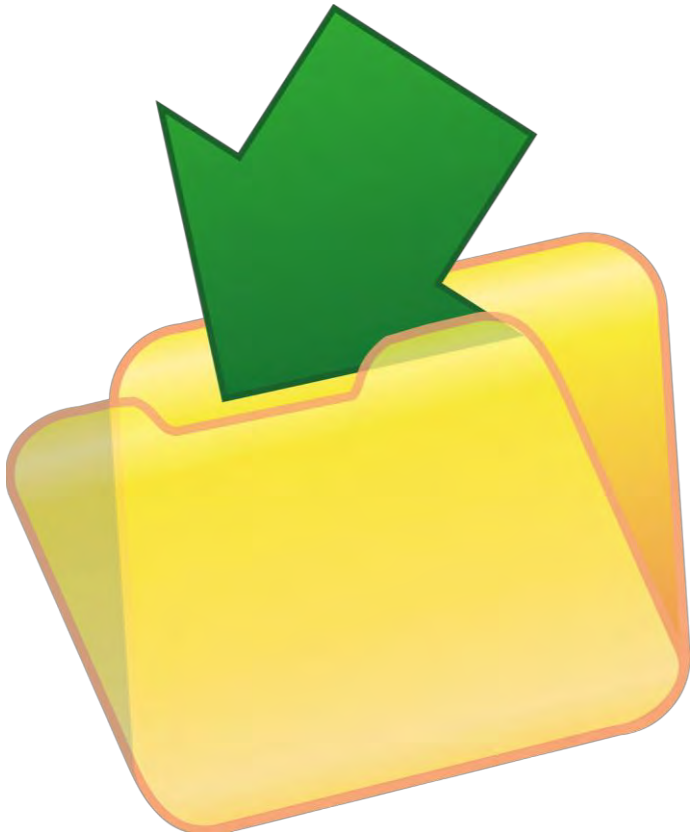
- Channels, teams, and workspaces are often organizational assets, not custodial files
- One-to-one or small-group chats may function more like custodial data
- A protocol must clearly define:
  - what is custodian-based
  - what is system-based
  - how relevance is assessed for shared spaces
- Failure to define this invites over-collection or under-production arguments



(c) 2026 Lexeprint Inc. All Rights Reserved.

Preservation Challenges Are Structural, Not Accidental

- Duty to preserve applies, but the hard part is scope
- Challenges:
  - proliferating channels/workspaces
  - private channels not visible to non-members
  - data stored outside the "platform" (e.g., Teams → SharePoint/OneDrive)
- Identify sources via:
  - custodian interviews/questionnaires
  - IT indices of teams/channels
  - sampling potentially relevant spaces
- Reasonable preservation requires targeting, not blanket holds
- Protocols should document why certain spaces were included or excluded



(c) 2026 Lexeprint Inc. All Rights Reserved.

Why "Just Produce Metadata" Isn't Specific Enough

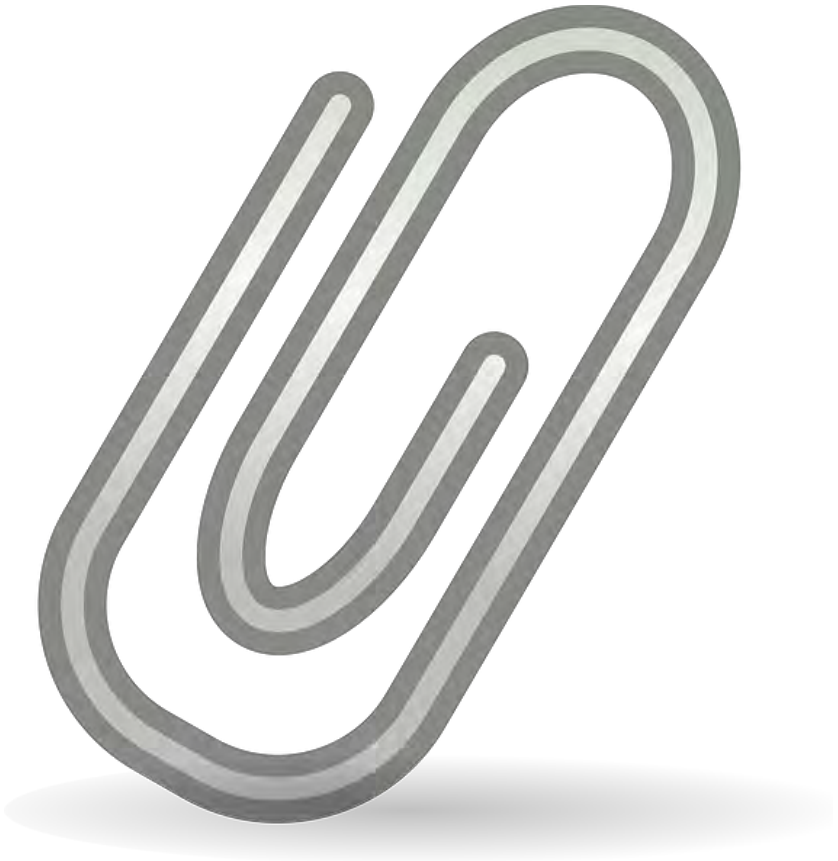
- Metadata disputes often stem from imprecision
- Modern platforms generate layered metadata: message IDs, channel IDs, participant handles, edit history, change logs, access permissions, version histories for linked files
- Metadata categories:
  - system metadata
  - application metadata
  - user-generated metadata
  - audit and activity logs
- "Producing metadata" is meaningless unless the protocol specifies:
  - which fields
  - from which system
  - in what format
  - for what purpose



(c) 2026 Lexeprint Inc. All Rights Reserved.

Hyperlinks Are the New Attachments

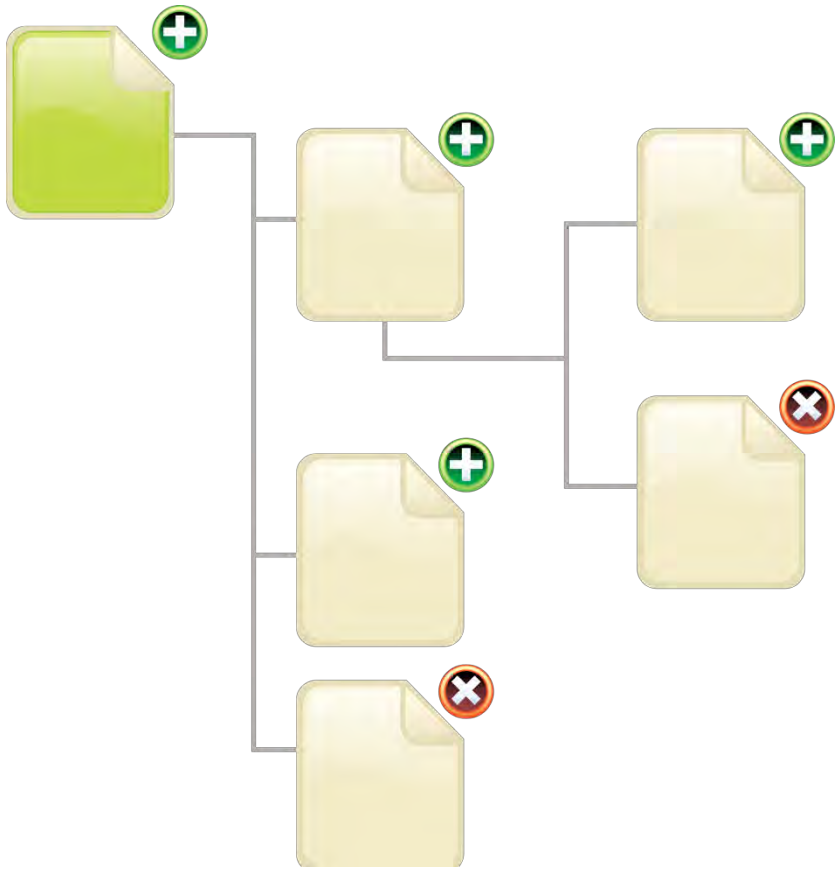
- Collaboration platforms commonly share content via hyperlinks, not static attachments.
- Recent cases indicate that courts will not automatically treat hyperlinks like traditional attachments.
- Hyperlinked content may be:
  - inside the platform environment
  - elsewhere in the org's systems
  - entirely outside the org (internet / third party)



(c) 2026 Lexeprint Inc. All Rights Reserved.

“Family Relationships” Don’t Always Map Cleanly

- Email model: parent message + attached child document (stable)
- Modern model: message + link to a file that:
  - can be edited by multiple users
  - can have hundreds of versions
  - can move locations or lose permissions
- Protocols must define:
  - what constitutes the “family”
  - which version(s) are produced
  - how relationships are preserved in the load files



(c) 2026 Lexeprint Inc. All Rights Reserved.

Cross-Platform Communications: Context Is Evidence

- One conversation can span:
  - chat messages
  - document comments
  - shared files
  - calendar invites
  - follow-up emails
- Evidence can include:
  - Replies/threads
  - edits/deletions
  - comments inside documents
  - who had access (active vs passive)
- If you produce "text only," you may destroy meaning and sequence



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

(c) 2026 Lexeprint Inc. All Rights Reserved.

Best Practices: Drafting An ESI Protocol That Works For Modern Discovery

(c) 2026 Lexeprint Inc. All Rights Reserved.

Don't Make An Agreement You Can't Keep

- Recent case law shows that courts tend to rely on and will enforce the parties' agreement on discovery matters.
- *In re Keurig Green Mountain Single-Serve Coffee Antitrust Litigation,* 341 F.R.D. 474 (S.D.N.Y. Apr. 11, 2022), Keurig was sanctioned under FRCP 37(b)(2)(A) for its own failure to comply with the preservation provision it agreed to within the ESI protocol.
- *In re StubHub Refund Litigation*, 2023 WL 3092972 (N.D. Cal. Apr. 25, 2023). In *StubHub*, the parties agreed to produce hyperlinked documents as attachments in the ESI protocol. However, the defendant could not comply with the protocol due to storage limitations, and many of the hyperlinked documents were unrecoverable.
    - Granting the plaintiff's motion to compel, the court emphasized the importance of adhering to the ESI protocols generally to expedite discovery. The court also cautioned parties against making commitments they couldn't meet and warned that sanctions could result from failing to produce requested documents.



(c) 2026 Lexeprint Inc. All Rights Reserved.

Protocols Are Not One Size Fits All

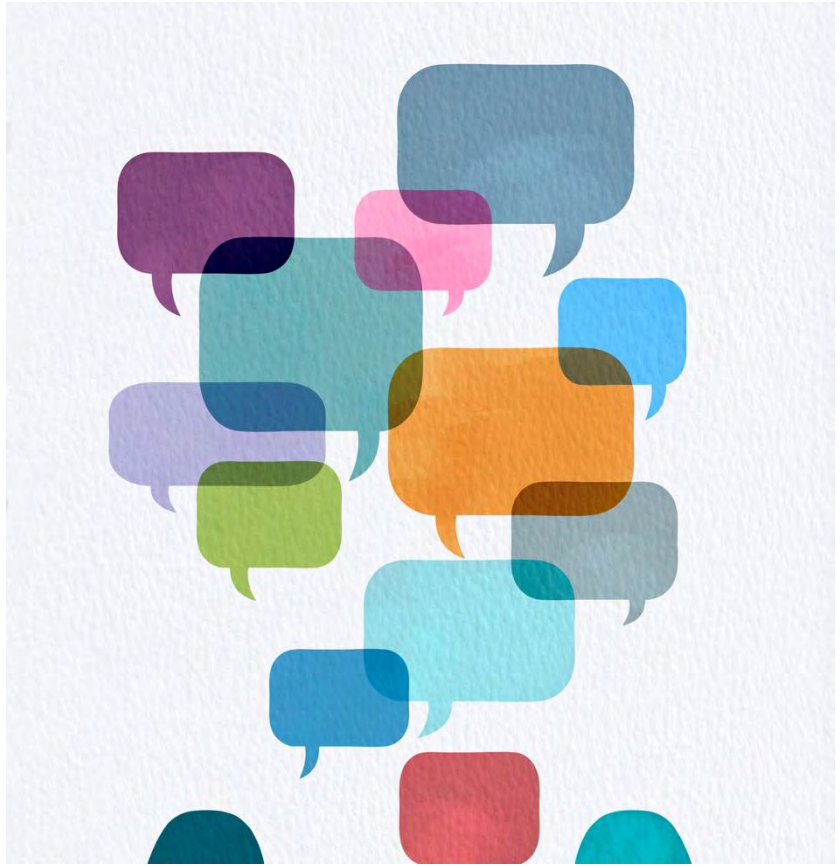
- If you have protocols from past cases or the court, you can use them to create a basic template.
- But make sure to tailor it to meet the needs of your current case.



(c) 2026 Lexeprint Inc. All Rights Reserved.

Speak the Same Language Or Find An Expert That Does

- Attorneys are obligated to be technologically competent, "including the benefits and risks associated with relevant technology." ABA Model Rule 1.1, cmt. 8
- But that does not mean attorneys have to be self-sufficient in the area of ESI.
  - When developing an ESI protocol, it is invaluable to consult with an e-discovery specialist or practitioner. There is fluency that comes with working in the space and distinctions that can be costly to your client if you don't understand what is being asked.



(c) 2026 Lexeprint Inc. All Rights Reserved.

Consider Using E-Discovery Neutral to Develop the ESI Protocol

- Objective Expertise:
  - A neutral (e.g., special master, mediator, or ESI consultant) can provide specialized knowledge of ESI best practices, technology, and legal requirements.
  - Neutral's recommendations carry weight without appearing biased toward any party.
- Helps parties identify, negotiate, and resolve ESI issues before costly disputes escalate.
- Encourages creative, case-specific approaches.
- Helps bridge gaps between parties, fostering a collaborative environment and reducing adversarial tension.



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

(c) 2026 Lexeprint Inc. All Rights Reserved.

Understand Your Client's Data Practices

- Before drafting an ESI protocol, it is critical for counsel to have a working knowledge of the client's IT systems and the types of data generated by those systems.
- Counsel should ask their clients:
  - Where is the information housed? Is the data stored on servers, a cloud, or individual desktops?
  - Who is in control of the information? Are there multiple individuals in charge of the information, and where are they located?
  - What form is the ESI in? What are the file types? Are the documents in PDF, readable PDF, word, TIFF, Excel, or some other proprietary system of record?
  - What are the licensing level and export options?

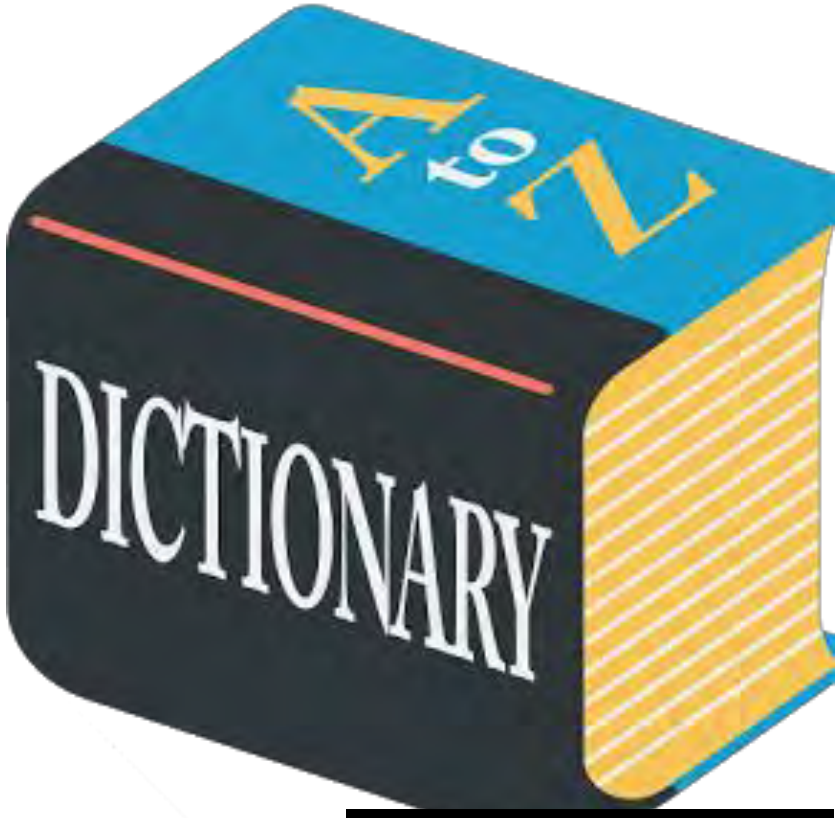


(c) 2026 Lexeprint Inc. All Rights Reserved.

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

Define Data Sources and Relationships

- Identify each platform in scope (Teams, Slack, Google Workspace, etc.)
- Define what's in:
  - channels/teams/workspaces
  - 1:1 chats and group chats
  - files (native storage vs linked)
  - comments/notes within documents
  - Map where data actually resides (platform vs connected storage)



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

(c) 2026 Lexeprint Inc. All Rights Reserved.

Production Must Preserve Conversation Context

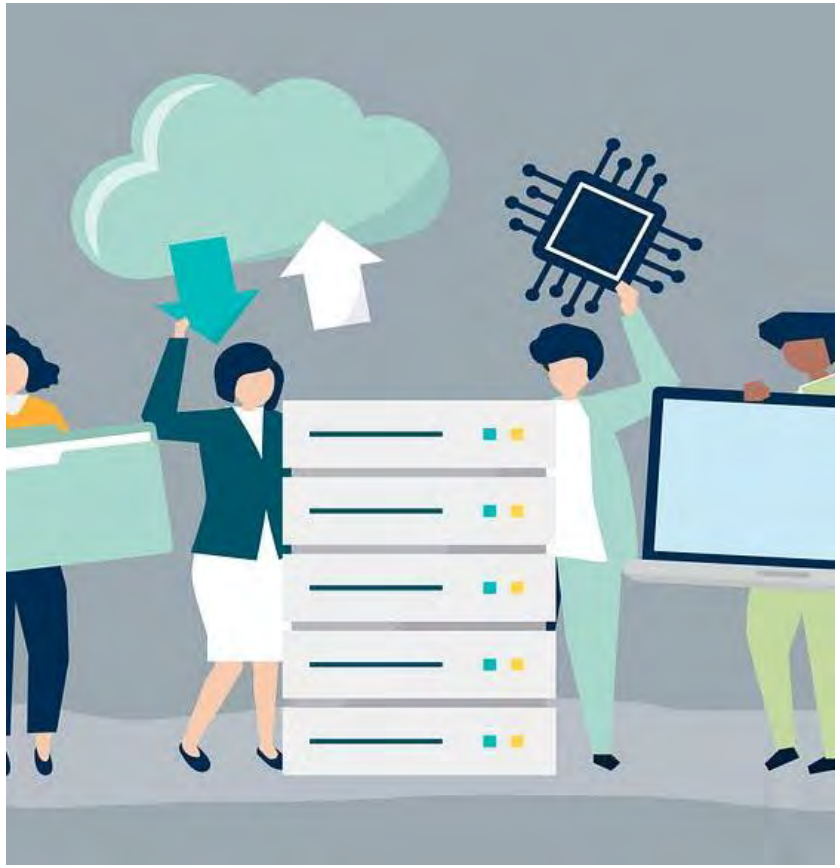
- For collaboration messages, define production to include:
  - message content + timestamp + sender
  - channel/team/space identifiers
  - thread/reply structure
  - participants roster (including handles → real names where possible)
  - edits/deletions/reactions where reasonably available
  - link/attachment references (and linked-file rule)



(c) 2026 Lexeprint Inc. All Rights Reserved.

Collection/Export Plan Must Match Platform Reality

- Specify export method (admin export, eDiscovery tool, API export)
- Document:
  - what locations were searched/collected
  - what date ranges and filters were applied
  - any platform limits or gaps
- Address search methodology limits (keywords vs other methods)



(c) 2026 Lexeprint Inc. All Rights Reserved.

Hyperlink Handling Clause (Pick a Rule)

- Choose and memorialize one approach (or a hybrid):
  - Link-only: produce URL + link text + message context
  - Treat as attachment when in custody/control: collect linked file + preserve relationship
  - Snapshot/version approach: capture the linked file as it existed when shared (where feasible)
- Define exceptions: third-party links, broken links, permissions barriers



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

(c) 2026 Lexeprint Inc. All Rights Reserved.

Metadata Schedule (Field List + Format)

- Attach a metadata field schedule by data type:
  - email
  - chat/messages
  - cloud files
  - meeting artifacts (recordings, transcripts, summaries)
  - hard copy documents
- Specify:
  - field names
  - source system of truth
  - output format (load file / JSON / CSV)
  - time zone standardization



(c) 2026 Lexeprint Inc. All Rights Reserved.

Questions?



(c) 2026 Lexeprint Inc. All Rights Reserved.



Daniel B. Garrie
Law & Forensics – Founder
JAMS – Neutral | Harvard – Faculty

Contact:
E: daniel@lawandforensics.com
W: www.lawandforensics.com

LAW & FORENSICS
A Global Legal Engineering Firm

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

Daniel Garrie is the Co-Founder of Law & Forensics LLC, Head of Computer Forensics and Cyber Security Practice Groups and has been a dominant voice in the computer forensic and cybersecurity space for over 20 years. Prior to Daniel's legal career, he successfully built and sold several technology start-up companies. Since co-founding Law & Forensics LLC in 2008, Daniel has built it into one of the leading boutique cybersecurity forensic engineering firms in the industry. Daniel has both a Bachelor's and a Master's Degree in computer science from Brandeis University, as well as a J.D. degree from Rutgers Law School. Daniel has led forensic teams in some of the most visible and sensitive cyber incidents in the United States.

Daniel regularly testifies as an e-discovery, cybersecurity and computer forensic expert witness, authoring forensic expert reports on multi-million-dollar disputes. His ability to perform complex investigations and effectively communicate the results to a jury has made him one of the most sought-after experts in the country. His testimony has been pivotal in a number of cases. Since 2008, Daniel has served as a Neutral and Special Master and in 2016, he joined JAMS as one of the organization's youngest Neutrals. At JAMS, Daniel serves as an Arbitrator, Forensic Neutral, and technical Special Master with a focus on cybersecurity, cyrptocurrency, and complex software and technology related disputes.

Daniel is well-published in the cybersecurity space, Editor-in-Chief of the Journal of Law & Cyberwarfare, author of more than 200 articles and books including, "Understanding Software, the Internet, Mobile Computing, and the Cloud. A guide for Judges", published by the Federal Judicial Center. He has been recognized by several United States Supreme Court Justices for his legal scholarship and is a trusted source and a thought leader for cybersecurity articles and opinions, being cited over 500 times to date.

(c) 2026 Lexeprint Inc. All Rights Reserved.



Michael Gold
Jeffer Mangels Butler & Mitchell LLP – Partner and Chair of the Cybersecurity and Privacy Group

Contact:
E: MGold@jmbm.com
URL: https://www.jmbm.com

Michael Gold is a partner and Chair of the Cybersecurity & Privacy Group at Jeffer Mangels Butler & Mitchell LLP. He counsels clients in a wide variety of matters, including information security and privacy compliance, supply chain and outsourcing security issues, AI implementation and governance, data breach responses and investigations, regulatory matters, crisis management, and technology contracts.

He has assisted clients in developing policies and processes to comply with information security and privacy laws throughout the world (including the E.U.'s General Data Protection Regulation, the California Consumer Privacy Act of 2018, and other national, state and industry-sectoral laws in the U.S.). He negotiates technology agreements relating to information security and privacy, and has particular experience with advanced digital advertising and marketing and emerging information security technologies. He represents clients in a range of industries, including healthcare, defense, major league sports, accounting and business management, and financial services.

Michael was named one of California's "Top 20 Cyber - Artificial Intelligence Lawyers" by the *Daily Journal* (2018), one of the *Daily Journal*'s 20 "Top Cyber Lawyers" in 2020 and again in 2022, one of the "Top Lawyers 2023 and 2025" and "Most Influential Lawyers: Digital Media and E-Commerce Law" by the *Los Angeles Business Journal*, and has been designated a "Top Rated Lawyer in Technology Law" by Martindale Hubbell. He is the co-author of the Bloomberg BNA Portfolio *Records Retention for Enterprise Knowledge Management*.

(c) 2026 Lexeprint Inc. All Rights Reserved.



Warren Kruse, MSc, CISSP, DFCP, EnCE, CCPA
iDiscovery Solutions – Managing Director

Contact:
E: WKruse@idsinc.com
URL: https://idsinc.com

Warren Kruse has spent more than thirty years in the places where truth hides: in hard drives, in network logs, and in the faint digital traces most people never see. As Managing Director at iDiscovery Solutions (iDS), he brings the instincts of a former New Jersey police officer and the precision of a seasoned forensic expert to every matter he leads.

His career has carried him through government agencies, global corporations, and cross-border investigations where the stakes were measured in billions, not budgets. He has unraveled intellectual property theft, exposed fraud, and guided organizations through the pressure of regulatory scrutiny. When the U.S. Securities and Exchange Commission needed a computer forensic expert, they called Warren. He testified. And he delivered.

Warren is not only versed in the field. He has shaped it. He co-authored Computer Forensics: Incident Response Essentials, a foundational text for modern investigators. His work on the Comtraid intellectual property and trade secrets case earned HTCIA's Case of the Year award. Later, the organization honored him with its Lifetime Achievement Award, a recognition reserved for those who elevate an entire profession.

He holds a Master of Science in Digital Investigation Management and a Bachelor of Science in Digital Forensics from Champlain College. He continues to contribute to the field as an active member of the American Academy of Forensic Sciences, HTCIA, ISC2, and The Sedona Conference.

(c) 2026 Lexeprint Inc. All Rights Reserved.



David Ko
Keller Rohrback – Partner

Contact:
E: dko@KellerRohrback.com
URL: https://www.kellerrohrback.com/

KELLER ROHRBACK
LAW OFFICES ◆ L.L.P.

David Ko is a partner in Keller Rohrback's Complex Litigation Group, where he litigates on behalf of plaintiffs in federal and state courts, specializing in cases involving corporate wrongdoing. His work has helped government entities, retirement plans, institutional investors, and consumers secure multimillion-dollar recoveries against major corporations.

David is prominently involved in Keller Rohrback's significant cases. He represents government entities in the National Prescription Opiate Litigation, MDL No. 2804 (N.D. Ohio), which has achieved over $50 billion in settlements. Additionally, he is a lead attorney in the Facebook Consumer Privacy User Profile Litigation, MDL 2843 (N.D. Cal.), resulting in a $725 million settlement, the largest in U.S. privacy class action history. David also led efforts in the JUUL Labs, Inc. Marketing, Sales Practices, & Products Liability Litigation, MDL 2913 (N.D. Cal.), securing nearly $2 billion in settlements for their role in the youth vaping epidemic.

David has significant trial experience, having conducted month-long trials in both federal and state courts. Before joining Keller Rohrback, he clerked for the Honorable Ricardo S. Martinez, U.S. District Judge in the Western District of Washington. He is the past president of the Korean American Bar Association of Washington and is a Fellow of the Washington Leadership Institute.

David is a member of the Washington State Bar Association, King County Bar Association, Asian American Bar Association, and the National Center for Employee Ownership. He frequently speaks at legal conferences, sharing his expertise on opioid litigation and legal ethics. Recognized for his contributions to the legal field, David has been honored in Lawdragon's 500 Leading Plaintiff Financial Lawyers (2023-2025) and selected for the Super Lawyers list in Washington (2022-2025).

(c) 2026 Lexeprint Inc. All Rights Reserved.



Patricia Antezana
Reed Smith LLP – Counsel

Contact:
E: PAntezana@ReedSmith.com
URL: https://www.reedsmith.com/

Patricia focuses on managing e-discovery. With a background in general litigation, Patricia brings a wealth of experience resolving a wide range of discovery issues. She advises clients regarding concerns that arise prior to litigation, including legal holds and preservation, and throughout litigation, including early case assessment, ESI protocols, collections, review, privilege issues, and productions. Patricia has coordinated electronic and hard copy record collection and managed large-scale review projects in numerous complex litigation matters, working closely with case teams to prepare comprehensive and defensible collection and review strategies.