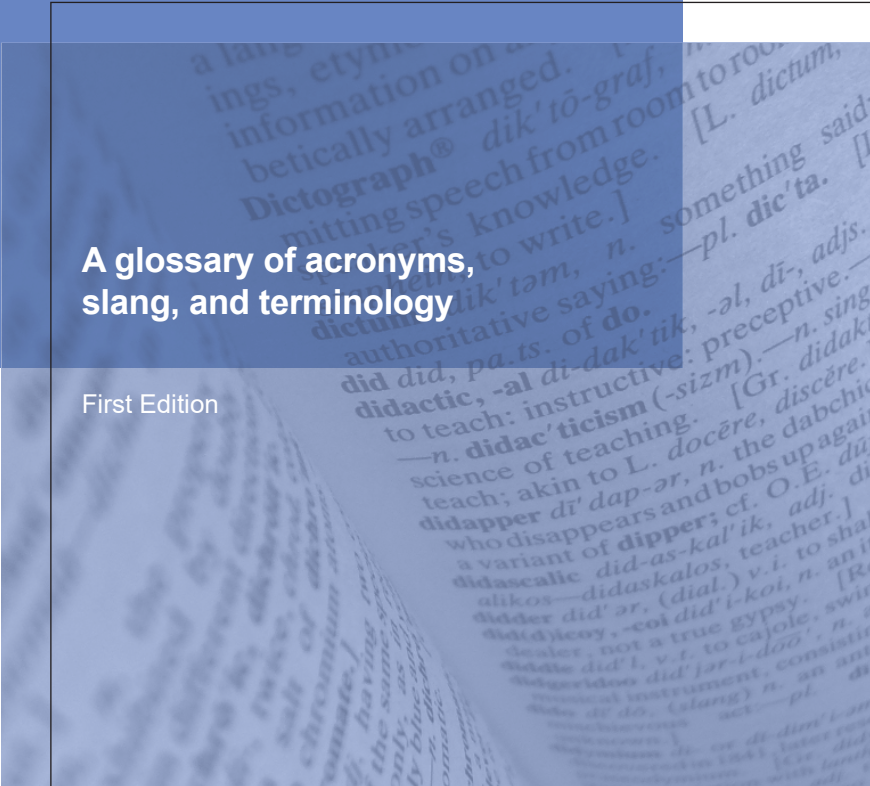


LATHAM & WATKINS LLP

The
BOOK
of
JARGON[®]
eDiscovery

A glossary of acronyms,
slang, and terminology

First Edition



Latham & Watkins operates worldwide as a limited liability partnership organized under the laws of the State of Delaware (USA) with affiliated limited liability partnerships conducting the practice in France, Hong Kong, Italy, Singapore, and the United Kingdom and as an affiliated partnership conducting the practice in Japan. Latham & Watkins operates in Israel through a limited liability company. Latham & Watkins operates in South Korea as a Foreign Legal Consultant Office. Latham & Watkins works in cooperation with the Law Firm of Salman M. Al-Sudairi, a limited liability company, in the Kingdom of Saudi Arabia. © Copyright 2023 Latham & Watkins. All Rights Reserved.

The Book of Jargon® — eDiscovery is one in a series of practice area glossaries published by Latham & Watkins. The definitions provide an introduction to each term and may raise complex legal issues on which specific legal advice is required. The terms are also subject to change as applicable laws and customary practice evolve. The information contained herein is not legal advice and should not be construed as such.

502(d): a provision of the Federal Rules of Evidence that protects against the (inadvertent or otherwise) waiver of Privilege during Discovery. Implemented in 2008 to decrease the costs of Privilege review in eDiscovery, the rule enables a court to “order that the privilege or protection is not waived by disclosure connected with the litigation pending before the court — in which event the disclosure is also not a waiver in any other federal or state proceeding.” Because the rule protects against the waiver of Privilege without requiring a party to show that it took reasonable steps in its Privilege review to protect against waiver, 502(d) is a powerful tool in protecting a client’s Privileges.

30(b)(6): a provision of the Federal Rules of Civil Procedure that specifies the requirements for deposing an organization. The rule requires a corporation, partnership, association, governmental agency, or other entity to designate a witness who can “testify about information known or reasonably available to the organization” on topics articulated by the serving party. Testimony offered by a 30(b)(6) witness is binding on the organization. Most recently amended in 2020, the rule requires the serving party and members of the organization to Meet and Confer in good faith about the matters for examination. 30(b)(6) depositions may implicate matters related to eDiscovery, including a company’s Legal Hold process, ESI collection, search, review, and Production.

Active Learning (or Continuous Active Learning): a type of machine learning in which an algorithm analyzes a document reviewer’s Coding decisions to predict and rank Coding outcomes for unreviewed data. A form of AI, Active Learning also efficiently sorts, prioritizes, and codes unreviewed data. Basically, Active Learning is lawyers leading machines and machines leading lawyers.

Analytics: a system or tool that uses algorithms to group, categorize, rank, assess, organize, and review data. Analytics allows users to view visual patterns and themes in their data, providing thematic insight at all stages of a matter. Analytics also contributes to how you receive suggestions of what to binge-watch on TV.

Artificial Intelligence (AI): an area of technology in which machines simulate human intelligence to perform functions and learning. AI is increasingly playing a large role in matters involving eDiscovery, as it can help users identify relevant or important documents faster, understand patterns in data, and achieve cost savings. For example, Active Learning is a type of AI used in eDiscovery workflows.

Asymmetrical Production: litigation matters characterized by one party collecting, reviewing, Processing, and producing a disproportionate amount of ESI compared with its adversary. Due

to the nature of some cases (e.g., class actions), Asymmetrical Production is sometimes expected; in other cases, a party will use Asymmetrical Production as part of a litigation strategy to request a large document Production from the other party. It is the modern version of burying someone in paper.

Attachment: a document or File that is associated with another File (e.g., an Attachment to an Email). Most commonly, Attachments to a single record are treated as a single unit during Processing, Production, and review. Attachments are associated with a Parent document and together make up a Document Family. An Attachment is also what you inevitably forget to include in a message to your boss.

Attribute: a characteristic of an ESI File, such as “title” or “date modified.” Attributes are displayed in a record’s Metadata.

Backup Tapes: a copy of ESI that is available to recover data in disaster or emergency systems. The Backup Tapes format will vary by system and IT Infrastructure. Backup Tapes are often not readily accessible and can require special Processing or collection. For this reason, they may become a source of contention during Discovery Meet and Confers, as searching and/or recovering ESI from Backup Tapes can result in undue burden or expense for a party. These days, “Backup Tapes” is a bit of a misnomer, as many entities back up their media on disks or other forms of storage.

Batch: ESI that is reviewed, processed, or produced in a single group. In large-scale document reviews, assigning Batches to reviewers can help streamline the review.

Bates Number: an identification number assigned to each page of a produced ESI File (or File name in the case of a File produced in Native Format). Typically, Bates Numbers will begin with a prefix identifying the producing party or matter. It is generally recommended to produce documents with a Bates Number or stamp to keep track of produced ESI and for identification if the ESI is later referenced in depositions, court filings, or other matters.

Beginning Document Number (BegDoc): the first identifying number assigned to a document or File produced in a Production.

Blowback: ESI that was printed to produce hard-copy documents. Blowback is also the reaction you will get if you ask someone to print out a whole PST File and leave it on their chair.

Boolean Search: a search conducted in databases using keywords and connectors (e.g., “and,” “or,” “not”) to include or exclude terms from search results.

Bulk Tagging: a process used to apply the same code or tag to a group of documents. While Bulk Tagging can efficiently categorize groups of documents prior to Production, it is still important to check document Productions to ensure that the Bulk Tagging was accurately applied.

Burn: copying ESI to other media, like a CD or hard drive. Increasingly, rather than copy ESI to other media when producing documents, parties are opting to exchange data via SFTP.

BYOD: acronym for Bring Your Own Device, a policy instituted at workplaces that permit employees to use personal devices for work purposes. BYOD can affect the process of collecting ESI from personal devices as well as the analysis of whether a party has “Possession, Custody, or Control” over the ESI. BYOD is not to be confused with BYOB (Bring Your Own Beer) or BYOD (Bring Your Own Dancefloor).

Chain of Custody: a record documenting the control, transfer, possession, and location of ESI or other evidence from the time it is identified to its Production or presentation in court. A well-documented Chain of Custody can establish the authenticity of the ESI and defend against potential Spoliation claims.

Child / Children: an Attachment to a single record (the Parent). Since FRCP 34 requires parties to produce ESI “in a form or forms in which it is ordinarily maintained or in a reasonably usable form,” it is a best practice to produce Parents along with their Children (no matter how embarrassing the parental record may be to the offspring).

Clawback Agreement: an agreement or stipulation typically negotiated (or incorporated into a Protective Order) between adverse parties to provide a procedure to “retrieve” privileged documents that were inadvertently produced in a litigation. Entering into a Clawback Agreement can help parties prevent or protect against the waiver of Privilege. To obtain the full force and effect of 502(d), parties should typically have their Clawback Agreements so-ordered by the court.

Coding: the process in which tags or codes are applied to documents during a review to preserve the attorney’s analysis of the document’s relevance, Privilege, importance, or other identifying characteristic.

Confidentiality: a designation assigned to a document governing its treatment and restricting who may view its content. Confidentiality is usually negotiated or specified in a Protective Order. In matters involving sensitive, proprietary, or trade-secret data, parties should consider the degree of Confidentiality applied to the documents prior to their Production.

Consent Form: a document provided to Custodians in which they may consent to the collection, Processing, review, and export of their personal data or ESI. The requirements of what must be in a Consent Form vary by jurisdiction, and applicable Data Privacy regulations should be consulted.

Custodian: the person or entity in charge of the record or control of an ESI File. Sometimes, but not always, a Custodian is the author of the document. Other times they are a much-loved elementary school staff member.

DAT File: a Load File that contains Metadata associated with ESI and is typically used for loading documents into Review Platforms.

Data Format: the form of Production that parties use to produce their ESI. Types of Data Format include Native, image, or other specified forms of Production.

Data Map: a representation of an entity or organization's sources of ESI and data systems. At the start of a litigation or investigation, it is often helpful to gain a full picture of an entity or organization's Data Map.

Data Privacy: an individual's right to decide how their data and information will be used. There is a growing body of regulations, both in the United States and internationally, designed to safeguard individuals' Data Privacy rights. In eDiscovery matters, parties should be aware of any applicable Data Privacy regulations in order to implement proper precautions.

Data Set: a group of Files and formats comprising an ESI collection that move as a unit from one eDiscovery stage to the next. Given the explosion of ESI, there may be dozens or even hundreds of File types collected in any given Data Set.

Data Source: the party that possesses a particular type of ESI, or the Custodian or application where the data is located.

Date Created: a Metadata field that is typically collected and produced and provides information regarding when a File was created. In some cases (e.g., a contract dispute), Date Created may be an extremely helpful field to understand, as it may indicate when a particular event occurred.

Date Last Modified: a Metadata field that is typically collected and produced and usually contains the date when a File was last edited and saved.

De-Duplication (or De-Duping or De-Dupes): a process used to compare ESI Files based on characteristics and remove Files that are exact (or near) duplicates. De-Duplication helps cull ESI data populations, streamlining the review process.

See also Near-Duplicates.

Discovery: a process in the US legal system whereby parties identify, collect, review, and produce relevant information and evidence during a litigation or investigation. FRCP 26-37 provide a framework for the process. Many courts and local jurisdictions also maintain procedures and practices governing Discovery. The process includes the collection, review, and Production of ESI and potentially depositions and other forms of written Discovery (e.g., responses and objections, interrogatories, etc.). While extremely important, Discovery is generally the bane of junior associates' existence.

Document Family: a collection of Files or ESI that comprise a single record. For example, an Email with two Attachments is a Document Family.

See also Family.

Document Population: a group of documents that constitute the records that need to be collected, processed, reviewed, or produced in a matter.

Early Case Assessment (ECA): a process run at the early stages of a matter to get a sense of potential issues and often to limit the volume of documents that must be processed and reviewed. ECA typically involves analysis of Data Sets.

EDRM: acronym for the Electronic Discovery Reference Model, which offers a step-by-step visualization of the eDiscovery process. Phases within EDRM include Information Governance, identification, Preservation, collection, Processing, review, analysis, Production, and presentation.

Electronic Discovery (eDiscovery): the process of identifying, collecting, reviewing, and producing relevant ESI in connection with a pending litigation or investigation. eDiscovery processes may differ depending on local rules, case law, and matters.

Electronically Stored Information (ESI): any information that is stored digitally. The Federal Rules of Civil Procedure specifically state that ESI is subject to Discovery. ESI encompasses many forms of information, including Emails, Text Messages, webpages, and numerous other File types that are not paper documents.

Email: the transmission of digital messages via the internet. Email plays a large role in the eDiscovery process, as it is typically the most requested source of ESI in Discovery.

Email Threading (or Threading): the process of identifying and grouping individual Email messages from the same conversation into a single thread. Notably, a thread includes the original Email and all responses to and forwards of that Email. Email Threading is typically easy to implement as the process is completely automated, and may substantially reduce review time and costs.

Embedded Object: a File copied (or “embedded”) into another File. Typically, the Embedded Object retains its original properties. For example, a meme or a GIF within an Email is an Embedded Object.

Emoji: an image or picture used to express words or thoughts. Emojis may be interpreted differently depending on a viewer’s personal understanding and are gaining increasing importance and relevance in eDiscovery matters. If you need further information about Emojis, just ask anyone under the age of 12 — or anyone over the age of 65.

Encryption: a procedure used to protect ESI when such information is exchanged. Encryption makes ESI Files unreadable to those who do not have permissions to view them. It is typically a best practice to encrypt ESI when producing in a litigation or investigation.

Ephemeral Messages: messages that exist for a short period, usually no more than a day, and then “disappear.” In theory, the messages will disappear after they are viewed. Depending on the platform used, Ephemeral Messages may pose challenges for Preservation or collection efforts.

ESI Order (or Discovery Order): a court-approved order or stipulation outlining the agreed-upon protocols that parties will follow during the Discovery process. ESI Orders typically detail the search and Production parameters to which parties agree to adhere, along with other provisions to which parties stipulate for Discovery. It is crucial that parties comply with the terms of an ESI Order.

Family: a collection of Files or records that are considered one communication during the eDiscovery process.

See also Attachment, Child, and Document Family.

Federal Rules of Civil Procedure (FRCP): rules that govern civil proceedings in United States District Courts. Rules 16, 26, 34, and 37 in particular provide parameters for Discovery and touch on issues related to ESI.

See also Rule 26.

File: data or records that are stored in one place, usually on a computer system.

Forensic Collection: ESI collected in a manner that ensures that the copy matches the original version. eDiscovery Vendors usually perform Forensic Collections. This manner of collection helps protect the integrity of documents, ensuring that their Metadata is not compromised or changed.

General Data Protection Regulation (GDPR): a Data Privacy legal framework passed in 2018 that provides guidelines for the collection, Processing, and disclosure of personal data of EU citizens.

Hash Value: an alphanumeric value created by common algorithms (MD5/SHA) to give each unique document a short, fixed-length string to allow for De-Duplication of documents in a Data Set. Different systems will use proprietary approaches to create Hash Values.

Hold Notice: a written communication sent out, typically within an organization or to relevant Custodians, once there is a Reasonable Anticipation of Litigation. Hold Notices typically instruct recipients to retain any potentially relevant information until the litigation concludes. Sending a Hold Notice is an important part in documenting the steps that parties take to preserve relevant information and protecting clients from later claims of Spoliation.

See also Legal Hold.

Hyperlinked Document: a document linked to other documents, but stored in a cloud-based repository. Hyperlinked Documents allow users to work collaboratively without having to exchange drafts. Parties should Meet and Confer regarding the treatment, collection, and Production of Hyperlinked Documents. Hyperlinks should not be cause for hyperventilation.

Inclusive Email: the “last in time” Email that has unique content and has not been forwarded or replied to. When Email Threading is applied to a Data Set, reviewers typically focus on the Inclusive Email.

In contrast, see Non-Inclusive Email.

Information Governance: the policies and procedures that govern an organization's retention and disposition of relevant business records and information. When developing an Information Governance plan, an organization often must evaluate the risks and value of retaining its records, as well as any industry-specific requirements for retention.

Instant Message (IM): a type of immediate communication between users. While there are a variety of IM platforms, typically Instant Messages are not stored or saved once the communication or chat box is closed. Parties should Meet and Confer regarding the treatment, collection, and Production of IM data, to the extent such data is recoverable.

IT Infrastructure: the technology system, policies, and procedures that govern an organization's Email, network, databases, and business applications.

Journaling: Dear Diary, journaling is ... an archiving solution that allows all messages to be preserved in an external repository. Journaling is used frequently in heavily regulated industries.

Legacy Data: ESI or other data that can only be accessed via platforms that no longer exist or have become obsolete.

Legal Hold (or Litigation Hold / Lit Hold): a formal document sent to Custodians and the IT department at an entity or organization directing the Preservation of all potentially relevant information once there is a Reasonable Anticipation of Litigation.

See also Hold Notice.

Linear Review: a review of every document in a Document Population by a human document reviewer.

Load File: a File that typically contains data related to ESI, like certain Metadata fields and text. A Load File is usually provided with a Production to ensure that information regarding documents is transferred.

See also DAT File.

Managed Review: a document review managed by an eDiscovery Vendor or contract attorney team. The case team at a law firm and the Managed Review team often work closely together to review and produce relevant ESI in a matter.

Meet and Confer: a meeting between counsel for adverse parties to discuss disputes or topics related to Discovery. Many jurisdictions and judges require parties to Meet and Confer to resolve disputes prior to seeking court intervention.

Metadata: a description of the properties of a File. Some of the most common Metadata fields describe the Date Created, Date Last Modified, date last accessed, and who authored the document. Parties typically negotiate exchanging certain Metadata fields prior to a document review and Production. Basically, Metadata is a set of data that gives you data about your data.

Native / Native Format: the original File type of a document. Spreadsheets and presentations are often produced in Native Format due to challenges with imaging. Parties should be aware that Native Productions may contain hidden data, such as macros, live hyperlinks, presentation speaker notes, or track changes. Generally, parties should negotiate Production Format in advance, as some parties will demand both Native and TIFF Productions.

Natural Language Search: the process of using plain language to search for or locate documents. For instance, before reviewing this Book of Jargon, you may have searched, “What is eDiscovery?”

Near-Duplicates: ESI Files that are so similar to one another, they are almost duplicates. Near-Duplicates can be identified by a Vendor; this can substantially reduce the resources needed for review by eliminating the need to review multiple copies of nearly identical documents.

Non-Inclusive Email: an Email that is wholly contained in another Email, adds no new participants or Attachments, and could be excluded from a Threading review. Excluding Non-Inclusive Email from a review may create efficiencies and save time in document review.

In contrast, see Inclusive Email.

Optical Character Recognition (OCR): the process of scanning or capturing text from an image so that it can be later searched as text. It is often helpful to OCR hard-copy documents that are scanned and saved as PDFs, and most Vendors will ensure that materials processed and loaded to a Review Platform are automatically OCR'd. Oh, see R? Yes, if it's OCR'd.

Parent: the main document in a Family (typically a cover email). Children are attached to Parents to comprise a single Document Family.

Personally Identifiable Information (PII): any information associated with an individual that would allow the individual to be identified.

Examples include a person's name, Social Security number, address, date of birth, physical characteristics, etc. Treatment of PII is subject to jurisdiction-specific rules; document reviewers and litigation teams should fully understand those rules at the outset of a matter. Litigation teams should also consider whether PII should be produced to other parties, and take care before filing PII in any public filings.

Platform (or Review Platform or Review Software): a system built to store and present ESI to attorneys for review, Coding, and Production. The selection of a Platform may depend on the type of litigation and a review team's needs. Teams may consider a Platform's cost and analytical capabilities before selecting one to host a document review.

"Possession, Custody, or Control": as specified under FRCP 34, parties may request Production of ESI within the other party's "Possession, Custody, or Control" during Discovery; the test to determine whether ESI is within a party's "Possession, Custody, or Control" varies by jurisdiction. Some jurisdictions apply the "legal right" test (i.e., whether the party has a legal right to the data, regardless of whether it physically has the data), while others apply the "practical ability" test (i.e., whether the party has the practical ability to obtain the data).

Predictive Coding: the automation of ESI Coding. Typically, a human document reviewer codes an example set of ESI for relevance. Predictive Coding then analyzes the codes applied and "predictively codes" the remaining ESI population.

See also AI and TAR.

Preservation: the process of ensuring that all potentially relevant ESI is protected from deletion or destruction. The duty to preserve, created by common law, attaches when there is a Reasonable Anticipation of Litigation. Failing to take steps to preserve relevant ESI may lead to serious consequences, including Sanctions. When implementing Preservation measures, parties should actively involve all relevant stakeholders, including IT personnel, and document steps taken to ensure that a defensible Preservation plan is in place. If you want to preserve your job, preserve your docs.

Privilege (Attorney-Client): a legally recognized protection afforded to communications between lawyers and clients. Privilege protects communications made in confidence (for the purpose of discussing legal advice) from disclosure during Discovery. The main goal of Privilege is to allow for open and honest communications between lawyers and clients.

Privilege Log: a list of documents that a party has withheld from producing in a litigation or investigation on the legal basis that it is

protected from disclosure. The most common privileges a party applies are attorney-client Privilege and work-product protection. A party submitting a Privilege Log must provide enough information for the requesting party to evaluate the sufficiency of a privilege claim. Privilege Logs frequently become a source of contention in litigation.

Processing: the process of converting ESI into a format for review on a document Platform.

Production: the process by which a party delivers relevant ESI to a requesting party, typically after screening the ESI for relevance and privilege. By managing your review timelines effectively, you can help your Production be less of a “Production.”

Production Format (or Production Specifications / Specs): the specifications by which ESI is organized prior to delivery to a party. The Production Format details the data to be exchanged, the format of the data, and the method of delivery to dictate how ESI is processed and/or produced. Typically, parties will agree to a Production Format prior to Production.

Protected Health Information (PHI): information regarding a person's physical or mental health. PHI is subject to various US and cross-border Data Privacy laws.

Protective Order (or Confidentiality Order): a court order governing the use of ESI or testimony produced during Discovery. One objective of Protective Orders is to set rules for maintaining the confidentiality of certain categories of ESI or testimony. Parties may enter into a stipulated Protective Order prior to exchanging Discovery. Under Rule 26, a party may move a court for a Protective Order to seek to limit the scope of Discovery or otherwise protect a party from “annoyance, embarrassment, oppression, or undue burden or expense” in the Discovery process.

PST: a File containing archived Microsoft Outlook Emails.

Quick Peek: the process by which ESI and documents are produced to another party or entity without having been reviewed for content or Privilege first. Quick Peeks are most often used in matters involving a large volume of ESI that needs to be produced in a short time frame. Parties should document the process and expectations of the arrangement prior to entering into any type of Quick Peek agreement, including with respect to Preservation and non-waiver of applicable Privileges and protections.

Reasonable Anticipation of Litigation: when an organization or entity becomes aware of a believable threat of litigation or considers

and/or takes steps to initiate litigation. Once this occurs, the organization must implement steps to ensure Preservation of potentially relevant ESI, typically through a Litigation Hold. Failure to do so may leave the party exposed to risk of Spoliation.

Redact / Redaction: removing or blocking part of a document to prevent its content from being viewed by others. Information is typically Redacted due to Privilege, Confidentiality, or privacy concerns. Redaction is helpful to guard secrets, such as [REDACTED].

Review Protocol: a set of guidelines established at the start of a document review that provide parameters for reviewers in executing the review. Review Protocols typically provide the background of a matter and instructions and guidance for reviewing/Coding documents, including for relevance, Privilege, and issues of note.

Rule 26: an FRCP rule that establishes ESI Discovery parameters for parties, including relevance and scope of Discovery, initial disclosures, Protective Orders, Discovery planning, and signing of Discovery requests. Rule 26 is rule No. 1 in eDiscovery.

Rule Amendments: changes to the FRCP, including the provisions that govern Discovery. The most recent amendments to the FRCP included changes to the scope of Discovery under Rule 26 (“relevance and proportionality”), standards for objections under FRCP 34 (no more boilerplate objections!), and Sanctions under FRCP 37(e) (failing to preserve ESI can land you in hot water). Parties should avoid having to amend their Discovery requests by reading the Rule Amendments first.

Sampling: reviewing a subset of data (either random or targeted) to get a sense of what may be in a larger population of the same data. Also a favorite pastime of grocery shoppers.

Sanctions: penalties a court may impose against a party that has committed wrongdoing during a litigation. FRCP 37 provides parameters for courts to impose Sanctions for various Discovery violations. FRCP 11 provides parameters for courts to impose Sanctions for pursuing frivolous or harassing lawsuits. Basically, Sanctions are what keep attorneys awake at night.

Search Term: a word or series of words or phrases used to identify or find information. Search Terms are often negotiated between parties.

Sedona Conference: a nonpartisan research institute dedicated to advancing law and policy in several legal fields, including eDiscovery. Sedona Conference periodically publishes commentary on various aspects of eDiscovery law and practice.

Seed Set: the initial set of documents or ESI used to train a TAR system.

SFTP (or FTP): acronym for Secure File Transfer Protocol, which provides secure methods of electronically transferring Files from one entity to another. Productions now often occur through SFTP rather than transmission of DVDs or hard-copy materials given the benefits of instantaneous transmission and download.

Slip Sheet: a placeholder for a document that is not produced. Typically, a Slip Sheet identifies the reason that the document is not within the Production (e.g., “withheld as Privileged”).

SMS: acronym for Short Message Service, an application used to send Text Messages to mobile devices. SMS killed the beeper, voicemail, and most other forms of interpersonal communication.

Spoliation: the destruction of relevant ESI, including its Metadata. Depending on the type of Spoliation that occurred (inadvertent or deliberate), a court may apply Sanctions against a party that lost the data.

Structured Data: data stored in a database instead of a document format. Structured Data is often produced by running reports or queries.

In contrast, see Unstructured Data.

Tagging: the act of classifying documents in Review Software as responsive, not relevant, Privileged, interesting, etc. In the olden days, lawyers physically applied tags to paper documents one by one. They also had to walk three hours uphill in the snow to work each day, both ways.

Targeted Collection: ESI collected in a manner that focuses on relevant materials and avoids over-collection. A Targeted Collection may involve applying Search Terms to a population of documents before collection and/or targeting a specific File path, Data Source, Custodian, or time period.

Technology-Assisted Review (TAR): a process by which ESI is organized or reviewed using a computer system. TAR can, for instance, help organize a Document Population by responsiveness, or by documents most likely to contain Privileged information.

Text Message: a communication sent via a cellular network, typically between cell phones, and routed using a cell phone number. Text Messages and their Metadata may be retained for several days or months.

TIFF: acronym for Tagged Image File Format, a commonly used Production Format in eDiscovery that stores bitmapped images. TIFF images are generally identified by a .TIF extension and may have black and white, gray, or color images. Parties hope their eDiscovery Vendor will generate TIFFs in a jiff.

Unstructured Data: data and/or documents not stored or organized in a database or other document management system. Unstructured Data may include loose Files stored on a hard drive or network folder.

In contrast, see Structured Data.

Vendor: a third-party legal service provider that typically aids in the collection, Processing, and Production of ESI during a litigation or investigation.

Workplace Collaboration Tools: software or platforms typically used by organizations that allow individuals to share information and communicate with one another across departments.

Work Product Protection: a protection that prevents disclosure to an adversary of materials prepared by an attorney or at an attorney's direction in connection with or in anticipation of litigation.

Austin
Beijing
Boston
Brussels
Century City
Chicago
Dubai
Düsseldorf
Frankfurt
Hamburg
Hong Kong
Houston
London
Los Angeles
Madrid
Milan
Munich
New York
Orange County
Paris
Riyadh*
San Diego
San Francisco
Seoul
Shanghai
Silicon Valley
Singapore
Tel Aviv
Tokyo
Washington, D.C.

LW.com

* In cooperation with the Law Firm of
Salman M. Al-Sudairi LLC