

Six Trends Affecting eDiscovery in 2024

Understanding the challenges shaping current and future eDiscovery processes.



eBook

eDiscovery Challenges Are Continually Evolving

Plus ça change, plus c'est la même chose. Penned in 1849 by French journalist Jean-Baptiste Alphonse Karr, the phrase translates to “the more it changes, the more it’s the same thing.” While Karr clearly wasn’t referring to electronic discovery — after all, the emergence of electronically stored information (ESI) was more than a century away — his words describe the current state of eDiscovery perfectly. eDiscovery challenges are continually changing and evolving due to several trends, including:

- **Information Volume:** Data volumes have skyrocketed, adding challenges in meeting discovery deadlines and budgets. Meanwhile, the variety of discoverable data types has also increased.
- **Cloud:** The migration to cloud-based solutions accelerated during the pandemic, leading to significantly higher use.
- **Data Protection Challenges:** With data breaches at an [all-time high](#), protecting personal and sensitive data is becoming increasingly difficult. In a [recent global report](#), 65% of respondents reported they’d been hit by a successful attack in the last two years. The stakes are higher than ever with constantly evolving data privacy laws, and the fines for non-compliance are rising in frequency and amount.
- **Technology Evolution:** AI and generative AI have added complexity to the equation. For instance, generative AI shows great promise, but current iterations have yielded concerns about accuracy, privacy, and copyright protection.

“The more it changes, the more it’s the same thing.”
— Jean-Baptiste Alphonse Karr



Challenges like these are shaping current and future eDiscovery processes. We predict six trends will affect eDiscovery this year.



Trend 1: Shift Left

It's time to focus more on the earlier development phases of the Electronic Discovery Reference Model (EDRM) to address data challenges and conduct eDiscovery efficiently and cost-effectively.



Trend 2: Embrace Data Variety

As more data types evolve, you must continually refine workflows to support them.



Trend 3: Integrate to Streamline

Reduce manual processes by integrating with enterprise archival and compliance solutions to preserve and collect ESI.



Trend 4: Focus on Personal Data

Leverage technology to identify and protect personally identifiable information (PII) before and during discovery.



Trend 5: Improve Authentication

With the greater potential of AI to generate false evidence, focusing on metadata will be vital for authentication.



Trend 6: Consider AI (with Caution)

Be proactive, yet cautious, in adopting AI. Focus on reliable use cases with proven benefits.



Trend 1: Shift Left

Data volumes are soaring, and it's a struggle to keep up. The IDC projects that global data volume will exceed **221,000 exabytes by 2026**. When the EDRM was created in 2005, the global data sphere hadn't even reached a zettabyte — but was 100,000 petabytes.

The original EDRM took data from the source and moved through an eight-step workflow: identification, preservation, collection, processing, review, analysis, production, and presentation. The volume of data and variety of ESI sources have since evolved dramatically, forcing eDiscovery earlier in the model. The current EDRM 2.0 has shifted left, placing greater focus on performing early data assessment (EDA) phases at the source for a more targeted collection of potentially responsive ESI (Figure 1).

Conducting EDA earlier leverages technology, including AI and machine learning, to perform advanced filtering, sentiment analysis, and classification tagging. Supporting this level of analysis sooner requires stronger ties between information governance and eDiscovery.

Integrating the left-side phases of the EDRM — information governance, identification, preservation, and collection — has become vitally important to efficient, cost-effective eDiscovery.

You need to analyze data where it lives. Selecting an eDiscovery solution that supports your needs throughout the EDRM, beginning with information governance, is essential.

eDiscovery solutions must include the ability to analyze, classify, and control unstructured data through early data assessment where the data lives across various data sources, using the latest proven AI techniques.

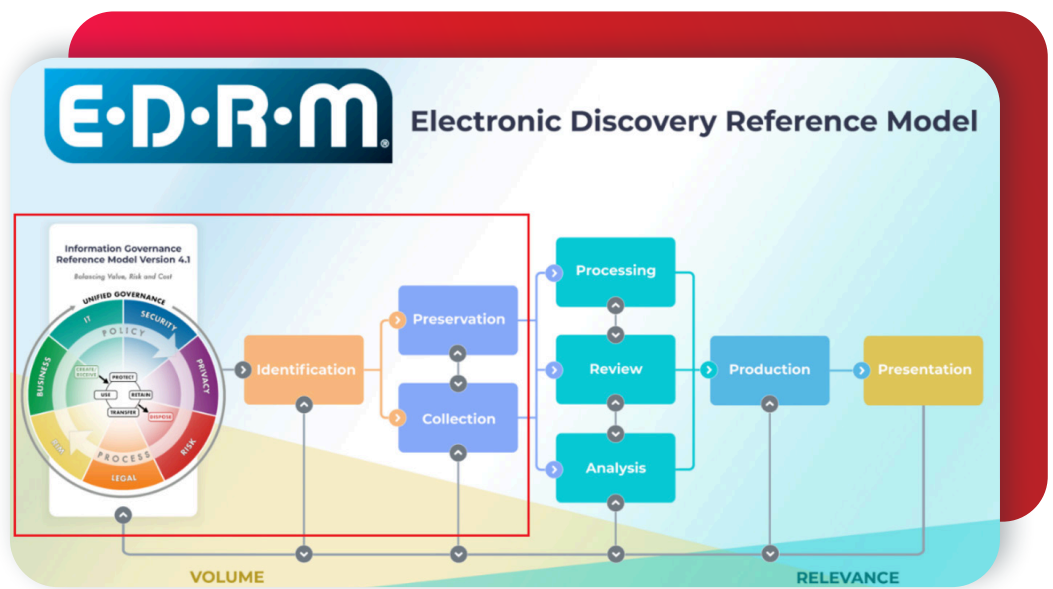


Figure 1: EDRM 2.0 includes a shift left, incorporating early data assessment at the source. (Source: EDRM)



Trend 2: Embrace Data Variety

In a recent [ComplexDiscovery survey](#), respondents identified “increasing data types” as the most significant issue that would affect eDiscovery over the following six months..

This is unsurprising. The 2023 Internet Minute infographic illustrates the volume and variety of data based on what happens in an average minute (Figure 2). It covers everything from 241 million emails sent to nearly 19 million text messages, plus Slack messages, Microsoft Teams chats, and more. Many of these are relevant to eDiscovery requirements.

Some of the data types subject to eDiscovery and compliance today include:

- **Collaboration Platforms:** Not only the most common platforms like Slack, Microsoft Teams, and Zoom, but many others, including Microsoft Teams Channel, Salesforce Chatter, Webex Teams, and Yammer.
- **Document Collaboration:** Cloud-based solutions like Google Drive, Dropbox, and Microsoft OneDrive.
- **Mobile and Text:** Text message data from major telecom providers like AT&T and Verizon, as well as sources such as SMS, WhatsApp, Facebook Messenger, and WeChat, China’s most popular messaging app.
- **Financial Platforms:** These include Bloomberg, Symphony, and Yieldbroker.
- **Other Sources:** Recorded and transcribed meetings, enterprise tools (like ServiceNow), SQL databases, JSON files, and more.

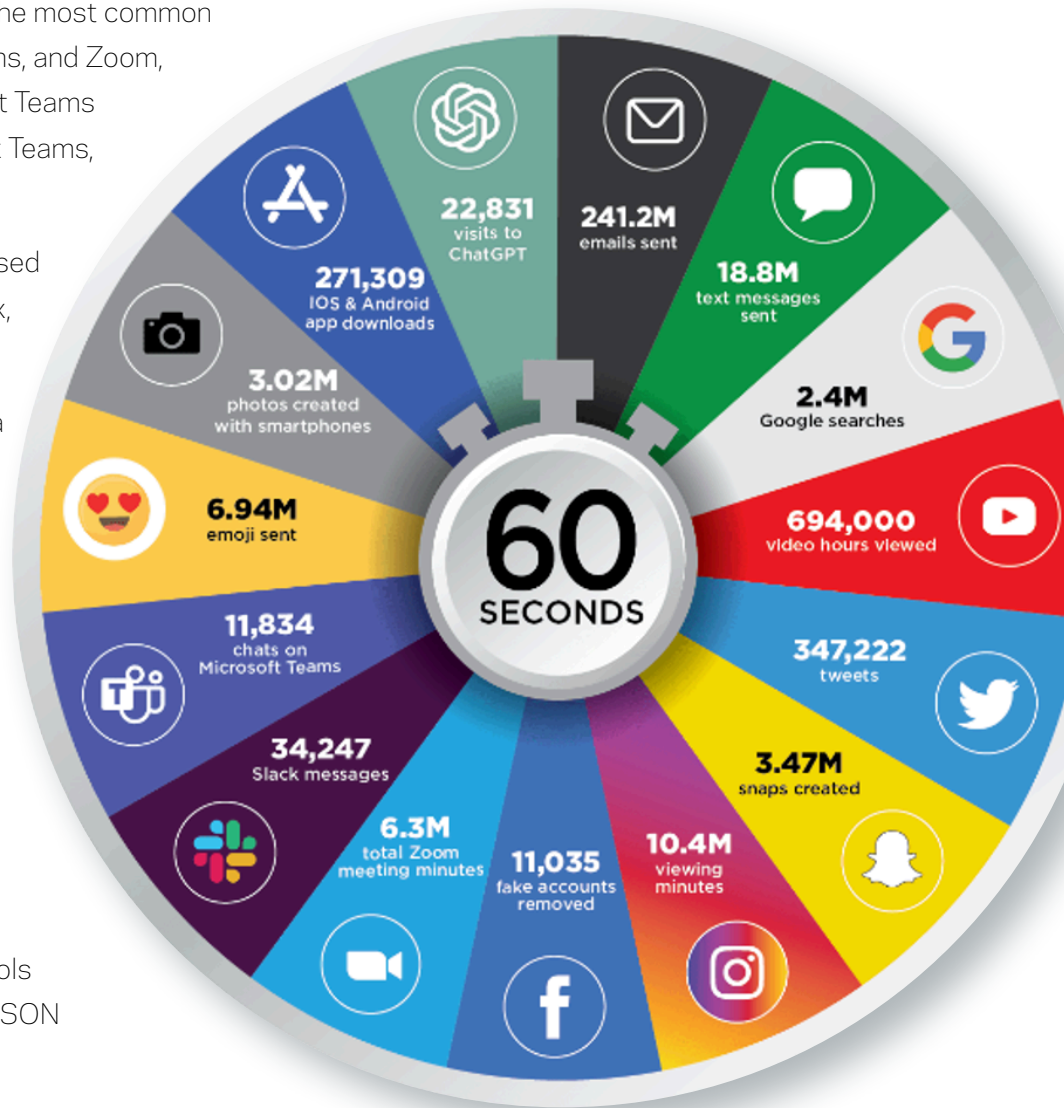


Figure 2: The 2023 Internet Minute infographic shows the variety and volume of data in use. (Source: [eDiscovery Today](#) and [LTMG](#))

If you’re not tracking data sources like these, you could be violating your discovery duties and possibly subjecting yourself to expensive sanctions. Be sure to select an eDiscovery solution that supports the variety of sources required to meet compliance regulations.



Trend 3: Integrate to Streamline

Much of your discoverable ESI likely exists in cloud-based enterprise solutions. Microsoft 365 is an example of this shift. Microsoft has transitioned its widely used Office applications to the cloud, including Word, Excel, PowerPoint, and Outlook. Microsoft offers SharePoint and OneDrive for document management, and Teams for online collaboration and meetings. In addition, Microsoft Purview incorporates data governance and eDiscovery features for software-as-a-service (SaaS) data.

However, Microsoft Purview has several [limitations](#) that can impact your eDiscovery workflows. They include:

- The inability to index more than 2 million characters of any document
- Maximum advanced indexing throughput of 2GB per hour
- Searches take up to 25 minutes for large organizations
- The tendency to throttle the export of data to load-balance environments
- Support for only [63 file types](#)
- Lack of in-place review and analytics

While eDiscovery starts with how you manage and archive for information governance purposes, it's essential to have a comprehensive solution to conduct discovery on ESI in enterprise solutions. In particular, look for [capabilities](#) including:

- **Upstream early data assessment:** Conduct assessment at the source where the data lives.
- **Expansive data capture with full context:** Collect data from a large variety of sources (such as those mentioned in Trend 2) and capture communications while preserving the full context of the conversation.
- **Comprehensive indexing and advanced, iterative searching:** Use advanced indexing technology and powerful search capabilities to deliver results in seconds.
- **Support for collaborative workflows:** Streamline matter management and allow your legal team to work with outside counsel.
- **Self-service capabilities:** Designate internal and external reviewers and administrators to export online search results without disrupting your IT team.

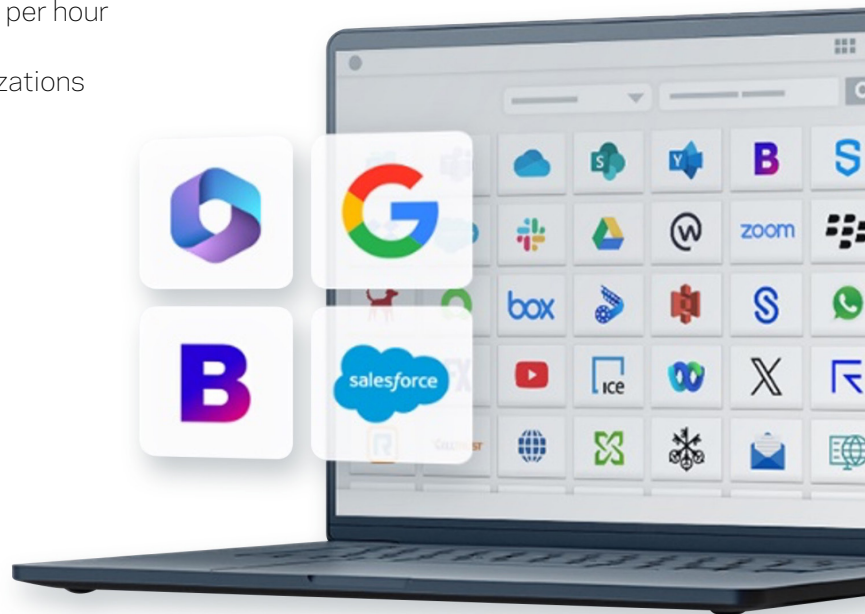


Figure 3: Veritas Alta™ eDiscovery supports more than 120 data sources.



Trend 4: Focus on Personal Data

Protecting personally identifiable information (PII) and protected health information (PHI) has never been more complex. Before 2023, California was the only U.S. state with a comprehensive data privacy law. Initially enacted in 2020, the latest version — the California Privacy Rights Act — went into effect in 2023, as did new laws in Colorado, Connecticut, Utah, and Virginia. Another eight states have passed comprehensive data privacy laws set to go into effect by 2026 (Figure 4). Meanwhile, at least 14 states have active bills. Each law is a bit different, but all have similar components covering consumer rights and the obligations of businesses to protect data.

The stakes have never been higher. Enforcement of the European Union’s General Data Protection Regulation (GDPR) was enacted in July 2018. The cumulative fines totaled less than 300 million euros in the first three years. As of January 2024, cumulative fines had reached 4.4 billion euros from nearly 2,000 fines issued since enforcement began, according to the [GDPR Enforcement Tracker](#).

Maintaining personal data at the level required for compliance requires rigorous [data protection](#) practices. Mechanisms such as role-based access control, multifactor authentication, and military-grade encryption of data in transit and at rest are must-haves to maximize safety of sensitive data and comply with regulations such as [CPRA](#), [FINRA](#), [GDPR](#), [HIPAA](#), [ITAR](#), [MiFID II](#), [PCI](#), [SEC](#), [SOX](#), and others.

US State Privacy Legislation Tracker 2024



Comprehensive Consumer Privacy Bills

| State | Legislative process | Statute/bill | Common name | Consumer rights | | | | | Business obligations | | | | | | |
|-----------------------|---------------------|--------------|---|-----------------|------------------|-----------------|--|----------------------|---------------------------|---|---|-------------------------|----------------------------------|---------------------------------|------------------|
| | | | | Right to access | Right to correct | Right to delete | Right to opt out of certain processing | Right to portability | Right to opt out of sales | Right to opt in for sensitive data processing | Right against automated decision-making | Private right of action | Opt-in default (requirement age) | Notice/transparency requirement | Risk assessments |
| LAWS SIGNED (TO DATE) | | | | | | | | | | | | | | | |
| California | | CCPA | California Consumer Privacy Act (2018; effective 1 Jan. 2020) | X | X | X | X | X | L | 18 | X | X | X | X | |
| | | CPRA | California Privacy Rights Act (2020; fully operative 1 Jan. 2023) | X | X | X | S | X | X | X | L | 18 | X | X | X |
| Colorado | | SB 190 | Colorado Privacy Act (2021; effective 1 July 2023) | X | X | X | P | X | X | X | X | 5/13 | X | X | X |
| Connecticut | | SB 6 | Connecticut Data Privacy Act (2022; effective 1 July 2023) | X | X | X | P | X | X | X | X | 5/13 | X | X | X |
| Delaware | | HB 154 | Delaware Personal Data Privacy Act (2023; effective 1 Jan. 2025) | X | X | X | P | X | X | X | X | 17 | X | X | X |
| Indiana | | SB 5 | Indiana Consumer Data Protection Act (2023; effective 1 Jan. 2026) | X | X | X | P | X | X | X | X | 5/13 | X | X | X |
| Iowa | | SF 262 | Iowa Consumer Data Protection Act (2023; effective 1 Jan. 2025) | X | X | X | X | X | X | X | X | 5/13 | X | X | X |
| Montana | | SB 384 | Montana Consumer Data Privacy Act (2023; effective 1 Oct. 2024) | X | X | X | P | X | X | X | X | 5/13 | X | X | X |
| New Jersey | | SB 332 | (2024; effective 15 Jan. 2025) | X | X | X | P | X | X | X | X | 5/13 | X | X | X |
| Oregon | | SB 619 | Oregon Consumer Privacy Act (2023; effective 1 July 2024) | X | X | X | P | X | X | X | X | 5/13 | X | X | X |
| Tennessee | | HB 1181 | Tennessee Information Protection Act (2023; effective 1 July 2025) | X | X | X | P | X | X | X | X | 5/13 | X | X | X |
| Texas | | HB 4 | Texas Data Privacy and Security Act (2023; effective 1 July 2024) | X | X | X | P | X | X | X | X | 5/13 | X | X | X |
| Utah | | SB 227 | Utah Consumer Privacy Act (2022; effective 31 Dec. 2023) | X | X | X | P | X | X | X | X | 13 | X | X | X |
| Virginia | | SB 1392 | Virginia Consumer Data Protection Act (2021; effective 1 Jan. 2023) | X | X | X | P | X | X | X | X | 5/13 | X | X | X |

Figure 4: 2024 U.S. State Privacy Legislation Tracker (Source: [International Association of Privacy Professionals](#))

You can't protect what you can't find. Creating customizable auto-classification rules to identify personal data, such as PII or PHI, is crucial to locating where you store such data.



Trend 5: Improve Authentication

Metadata has always been necessary in eDiscovery. In addition to enriching the information available, it enhances the efficiency and accuracy of the process. Metadata provides several key benefits, including:

- **Context:** Metadata might show when a document was created, by whom, who had access, and how often it was edited or viewed. This information can provide insights into its significance or relevance.
- **Search and Organization:** Efficient and targeted searches help legal teams quickly locate relevant documents among potentially millions of files.
- **Timeline Analysis:** You can use data, such as sent and received dates, to construct event timelines, which can be vital in understanding the sequence of events in a case.
- **Deduplication:** Redundant data can increase costs and review time. Hash values can help identify and remove duplicates, ensuring that legal teams don't review the same document multiple times.
- **Chain of Custody:** Custody data can demonstrate that electronic evidence has been handled properly and has not been altered.
- **Linking:** Some metadata, such as email thread fields, can show relationships between files or communications.
- **Assist in Privileged Review:** Email metadata identifying senders and recipients can help legal teams locate potentially privileged communications that might be exempt from production.

One of the most significant benefits of metadata is how you can use it to confirm the authenticity and integrity of a document or file. One of the downsides to the emergence of generative AI is that it has enhanced the ability to create convincing deepfakes of images, audio, or video evidence. As a result, the ability to authenticate your evidence has become more critical.

Complete and accurate metadata — including the full conversational context of messages — is a significant factor in ensuring proper evidence authentication, making it more important to your discovery workflows.

*Capture data defensively.
Preserving metadata
in place at the data
source maintains chain
of custody and positions
your team to respond to
authenticity challenges.*



Trend 6: Consider AI (with Caution)

Following the introduction of ChatGPT in late 2022, generative AI reached global phenomenon status in 2023. And it has shown exceptional abilities. GPT-4, introduced in March 2023, not only [passed the exam](#) to obtain a license to practice law as an attorney, it scored in the 90th percentile. It can [suggest a meal](#) based on what it “sees” in a picture of a refrigerator’s interior. And it can [write code](#) in popular programming languages. You can use it to generate sophisticated images in seconds based on a simple prompt (Figure 5).

Generative AI has the potential to provide significant benefits — as well as create substantial problems. In 2023, a lawyer [submitted a filing](#) generated by ChatGPT that included at least six “bogus judicial decisions with bogus quotes and bogus internal citations.” These were so-called *hallucinations*, in which the AI model presented information it generated as fact. Add to that concerns about [copyright issues](#), [defamation claims](#), data protection, and using the technology to [launch cyberattacks](#).

It’s still unknown whether the benefits of generative AI outweigh the risks. However, there are proven use cases of how AI technology can streamline eDiscovery workflows, specifically [sentiment analysis and classification](#).

In sentiment analysis, you can use natural language processing to identify attitude, sentiment, or emotion. In eDiscovery, you can use this information to:

- Prioritize documents that are more likely to be relevant.
- Identify patterns in communication that may be relevant to a case.
- Flag content with strong negative sentiment for further review.

Automated classification uses advanced algorithms and machine learning models to organize information in predefined classes or categories. Example applications include using it to:

- Identify PII, PHI, or other sensitive data.
- Identify and remediate redundant, obsolete, or trivial (ROT) data.
- Detect foreign languages.

Until the benefits of generative AI technology have been reliably demonstrated, it’s best to focus on use cases that have consistently proven benefits in streamlining discovery workflows.



Figure 5: An image we generated by DALL-E 3 using the prompt “technology trends 2024.” (Source: [Microsoft](#))

How to Prepare

As a leader in multicloud data management, Veritas is focused on ensuring your data's protection, recoverability, and compliance. When it comes to eDiscovery, [Veritas Alta™ eDiscovery](#) provides a cloud-based, end-to-end solution that enables you to collect, review, and produce electronically stored information for your legal and investigation needs. Veritas Alta eDiscovery offers a complete solution, including:

- Defensible collection of your organization's relevant content sources
- Purpose-built review of all types of data
- Efficient production of your relevant documents

Use it to support cross-functional collaboration on matters and investigations so that your internal and external legal teams, IT, human resources, and other organizational stakeholders can work together more efficiently. Give your teams the tools to quickly locate their intended dataset, including real-time iterative search capabilities, built-in collaborative eDiscovery workflow, and flexible SaaS export options.

What's Next?

Our society and business world are continually changing, affecting how you conduct eDiscovery today and in the future. It's vital to be proactive, addressing trends in eDiscovery as they evolve. Start with implementing the right technology solutions. Look for eDiscovery solutions that:

- Span the entire EDRM life cycle, including information governance
- Comprehensively support a broad range of file types
- Provide seamless integration with cloud-based enterprise solutions
- Automate the identification of personally identifiable information (PII) and provide industry-standard data protection mechanisms
- Preserve complete and accurate metadata, including the full conversational context of messages
- Support AI use cases that have proven to provide benefits

One thing is certain: Change is inevitable. Organizations that embrace change are more likely to conduct eDiscovery efficiently and cost-effectively in 2024 and beyond.

About Veritas

Veritas Technologies is the leader in secure multi-cloud data management. Over 80,000 customers—including 91% of the Fortune 100—rely on Veritas to help ensure the protection, recoverability and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor is able to match the ability of Veritas to execute, with support for 800+ data sources, 100+ operating systems and 1,400+ storage targets through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. Learn more at www.veritas.com. Follow us on X at [@veritastechllc](https://twitter.com/veritastechllc).

VERITAS™

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact
information visit:
veritas.com/company/contact