



DISCOVER EDISCOVERY
WHITEPAPER

DISCOVER EDISCOVERY

WHAT IS EDISCOVERY AND HOW DID WE GET WHERE WE ARE RIGHT NOW

Mention eDiscovery in a crowd. (We dare you.) You'll hear loud groans. People will raise their arms defensively and back away, shaking their heads no. Some will turn their backs completely.

They want no part of eDiscovery, thank you very much.

eDiscovery has a bad reputation. Litigators, general counsels, legal support staff, IT professionals, and information management specialists each approach eDiscovery from varying angles. Yet, they are united in a singular view: eDiscovery sucks.

It's bad reputation is duly deserved. eDiscovery arrives with all the subtlety of a tornado, demanding immediate attention and sucking up time, money and manpower in a deluge of dull, repetitive tasks and tedious processes. As if that's not enough, eDiscovery can leave behind severe and crippling damages if it's not completed absolutely thoroughly and accurately.

Definitely not a crowd pleaser.

Which is tragic, really, because technology has finally advanced far enough to relegate eDiscovery's bad reputation to the past. Today's eDiscovery is much easier, more efficient, and completely reliable. For example, Technology Assisted Review (TAR), which felt like a crowning achievement when it came out, is now merely one of several even more sophisticated capabilities.

DEFINITELY NOT A CROWD PLEASER

THE ROOT OF ALL ~~EVIL~~ EDISCOVERY

eDiscovery is a direct result of developing strategies to deal with the ever-increasing types and amounts of electronically stored information (ESI) generated by businesses, people, and devices in our hyperconnected online world.

Lawyers used to say, “If it’s not on paper, it doesn’t exist.” Businesses ran on promises committed to paper: the contracts, leases, agreements, letters, memoranda, and notes filed away in drawers, alphabetically, in carefully labeled files. If you questioned whether a thing was supposed to happen or did happen, the answer was right there, indelibly typed on paper. Debate over.

Now, digital communications and transactions result in scattered bits and links of ESI, not paper trails.

An entire Internet of Things is entwined in our daily lives. Social media are our coffee shops. “Online” meets our daily personal and business needs for everything from communication to shopping to scheduling appointments and travel plans to banking, filing taxes, and everything in between.

Along with it all? Massive amounts of new data generated constantly. Every single minute. Of every single day.

Even a lunchtime walk generates mobile GPS data. Facebook, Amazon, Google, and Verizon can know more about a person than their spouse. A dispersed, mobile workforce relies heavily on online social collaboration tools.

We’re far, far beyond the days when reaching inside an organized file cabinet was the height of fast, effective data retrieval.

EDISCOVERY GET ITS START

Lawyers and courts were the first forced to address the need to manage the daily data deluges. Legal actions floundered when substantial amounts of critical information remained undiscoverable simply because it was digital. The result was an unacceptable barrier to justice.

In 2006, “eDiscovery” became a definable process under the U.S. Federal Rules of Civil Procedure (FRCP) (Amended in 2015.) The FRCP set forth guidelines for the discoverability of ESI and laid out expectations for managing fair requests for information and functional exchanges of ESI.

The FRCP provided the rules of the game. But someone still needed to create a playing field.

Enter the [Electronic Discovery Reference Model](#) (EDRM), which offers standards, guidelines and practical resources for managing processes involved in eDiscovery including:

IDENTIFICATION: Locating potential sources of ESI and determining its scope, breadth and depth.

PRESERVATION: Protecting ESI against inappropriate alteration or destruction.

COLLECTION: Gathering varying types of ESI from multiple sources.

EDISCOVERY GET ITS START

PROCESSING:

Reducing the volume of ESI and converting data to forms more suitable for review and analysis.

REVIEW:

Evaluating ESI for relevance and privilege.

ANALYSIS:

Evaluating ESI for content and context, including key patterns, topics, people and discussions.

PRODUCTION:

Delivering ESI to others in appropriate forms using appropriate delivery mechanisms.

TODAY, EDISCOVERY HAS EVOLVED INTO
A **\$9 BILLION DOLLAR** INDUSTRY THAT'S EXPECTED
TO DOUBLE IN SIZE TO OVER **\$18 BILLION** BY 2022.

Legal technology vendors offer eDiscovery software as an end-to-end solution that many organizations are using in-house, either through a one-time cost or, more commonly now, as a scalable, cloud-based subscription service.

OUR RELATIONSHIP WITH DATA: “IT’S COMPLICATED”

Together, we create [2.5 quintillion bytes](#) of data every day. And, if the varying versions and formats of duplicate documents found across every corporate network in existence are any indicator, we’re storing every last bit of it.

The problem is, nobody is really sure how to get to it all.

For a long time, the “e” in eDiscovery meant legal technology focused on handling emails and documents stored on file-sharing platforms. Videos and audio recordings were set aside as exceptions or tagged for time-consuming manual review. As the internet infiltrated our lives, new data created by online activities, cell phones, social media, wearable tech, connected devices, and so on joined them.

Now, this collection of what used to be outliers has grown to massive proportions that can no longer be ignored or dealt with manually.

And, it’s more than just the new data gunking up the works. Accessing ESI gets even more complicated as older word processing programs are retired. Old file formats and “legacy” data after mergers or acquisitions become difficult or even impossible to access.

OUR RELATIONSHIP WITH DATA: “IT’S COMPLICATED”

“Keep it just in case” is the mantra of data hoarders everywhere. With scandals such as Enron seared in their memories, many executives won’t risk losing information that may be relevant to important matters in the future. Employees and IT staff do not want to be blamed for deleting critical information, either. Pushing companies into still more over-retention activities are issues such as:

LACK OF DIRECTION **OR** POLICY

Organizations may lack company-wide document and data retention policies. Some also lack document and information management systems or use inadequate, antiquated software. The end result is that employees “manage” their own documents and files, yet no one actually takes any real responsibility for them.

STAFF TURNOVER **AND** LACK OF MANPOWER

Mergers, layoffs, and the normal job cycle of people leaving positions also result in mountains of ESI no one is really sure about. Corporations face more regulation and compliance demands than ever before, but now work with smaller IT staffs to manage their data.

**“KEEP IT JUST IN CASE” IS THE MANTRA
OF DATA HOARDERS EVERYWHERE**

EVERYONE WANTS A LOOK INSIDE

Perhaps ironically, the more massive and unwieldy a corporation's accumulated data grows, the more people become interested in seeing every last bit of it.

Consumers expect companies to show they conduct business ethically across the globe. As more massive data breaches top the news cycle, consumers also demand proof that businesses can protect their private information.

Responsible businesses strive to create more transparency into internal behaviors to build goodwill, public trust, and employee loyalty. Yet, producing that information is a delicate process. The public can all too easily make inaccurate inferences from troves of disorganized information.

Of course, government and regulatory agencies do not wait to see what information companies willingly produce. Organizations must continually prove their compliance with a vast assortment of old, new, and revised regulations.

THE MORE MASSIVE A CORPORATION'S ACCUMULATED DATA GROWS, THE MORE PEOPLE BECOME INTERESTED IN SEEING EVERY LAST BIT OF IT.

REGULATIONS INTENSIFY ALREADY MOUNTING PRESSURES

Pressures mount from all sides. In addition to consumers and clients, others who insist on peering inside companies include:



A combination of federal, state and local governments



Multiple regulatory agencies, licensing bodies, and other administrative institutions.



Courts, plaintiffs, and third parties involved in litigation, IP disputes, mergers, acquisitions, and so on.

Demands from multiple regulatory agencies across various jurisdictions can vary widely and may even conflict, particularly as regulations increase in number, scope, and complexity. New and increasingly complex privacy regulations such as the European General Data Protection Regulation (GDPR) saddle corporations with heavy responsibilities to cleanse data before it is disclosed to third parties. Data protection rules require constant action to assess archived ESI and disclosures for compliance.

REGULATIONS INTENSIFY ALREADY MOUNTING PRESSURES

Companies that release confidential or protected information to third parties - even inadvertently - can expect serious fines and potential public backlash.

California just passed one of the toughest data privacy laws in the U.S. The California Consumer Privacy Act gives consumers the right to request that a business to disclose the categories and specific pieces of personal information it collects about them. Companies also need to indicate the categories of sources from which that information is collected, the business purposes for collecting or selling the information, and possible third parties with which the information is shared.

In early 2018, the U.S. Department of Labor (DOL) issued a rule increasing [ERISA's non-compliance penalties](#). Ignoring a DOL request for plan information will cost employers \$156 per day per document request. They'll pay \$1,693 per day for issuing automatic contribution notices before the plan year starts. Errors in issuing timely blackout notices and maintaining predecessor employer records will cost them, too. Employers can be charged over half a million dollars for impermissible use of participant genetic information even when the violation is unintentional.

In addition to the GDPR, the UK also put in place the [Data Protection Act of 2018](#). Failure to comply incurs a fixed penalty of £4,000 for large organizations. Aggravating factors can increase the penalty to a maximum of £4,350. Penalties under the Data Protection Act **are in addition to** the GDPR penalties of up to £17 million (€20 million), or 4% of an organization's annual global turnover.

REGULATIONS INTENSIFY ALREADY MOUNTING PRESSURES

The consequences of a misstep are dire. Mistakes are instantly public. Leaked or hacked data or the inability to comply with regulations can send a corporation's reputation and finances tumbling.

When an incident occurs, corporations need to form an immediate response. Yet, the core issue that created the problem remains: Executives are still unable to timely or thoroughly access critical ESI.

Corporate stakeholders lose patience, consumers lose trust, and the company faces a long road ahead trying to recoup lost profits and prestige.

**THE CONSEQUENCES OF A MISSTEP
ARE DIRE. MISTAKES ARE
INSTANTLY PUBLIC.**

EDISCOVERY SAVES THE DAY

The most effective way to manage problems caused by technology is by turning to better technology. Advanced search capabilities, data analytics, and machine learning techniques give today's eDiscovery platforms what yesteryear's systems never had: The power to preserve, identify, collect, process, review, analyze and produce enormous amounts of data and the flexibility to adapt to new data types as they emerge.

TODAY'S ADVANCED EDISCOVERY CAN:

- Identify and collect relevant information from various sources using advanced search capabilities
 - Consolidate multiple, varying file types onto a single review platform
 - Eliminate duplicate copies, handle various document versions, and perform email threading
 - Meet privacy demands with automated redaction of private data and anonymization of protected names
 - Simplify production by providing access to all files types from a single source
 - **MUCH MORE!**
-

EDISCOVERY TAKES OFF

Clever professionals recognize the potential for applying eDiscovery processes in other areas of business. The EDRM model has been co-opted to meet information governance needs and reduce privacy and security risks. eDiscovery is a versatile and powerful tool that aids businesses in:

- I. Litigation & arbitration (cross-border and internationally)
- II. Responding to regulatory requests
- III. Conducting internal investigations
- IV. Vendor due diligence and building virtual data rooms

I. LITIGATION

Accurately predicting the time and financial resources needed, when, or for how long requires taming unruly amounts of ESI. Properly implementing and managing legal holds and conducting early case assessments are particularly helpful when meeting challenges involving:

- HR and employee concerns
 - Intellectual property claims; patent and trademark disputes
 - Class actions, mass torts, and product liability claims
 - Commercial disputes
 - Shareholder disputes
-

EDISCOVERY TAKES OFF

I. ARBITRATION

Search protocols that are neither under- nor over-inclusive helps parties who resolve disputes by arbitration avoid the excessive costs and time involved in performing the type of in-depth eDiscovery required in litigation. Production must be swift, yet secure while privacy issues are addressed.

II. RESPONDING TO REGULATORY REQUESTS

Responses to regulatory requests are supported by identifying, collecting, reviewing and producing relevant ESI - the very heart of eDiscovery. These aid corporations in complying with regulations related to:

- Unfair Competition and Antitrust investigations
- Financial reporting
- Environmental restrictions
- Food and consumer goods guidelines
- Healthcare mandates
- Privacy concerns and data protection rules
- External bribery and fraud investigations

III. INTERNAL INVESTIGATIONS

The accuracy of internal investigations rely on a company's ability to fully access its data. Corporations with global operations benefit from the ability to collect, consolidate, organize, and prioritize enormous amounts of data. Companies of every size use eDiscovery to assist with internal investigations such as fraud detection and financial audits.

EDISCOVERY TAKES OFF

IV. VENDOR DUE DELIGENCE AND VIRTUAL DATA ROOM PREPARATION

Managing a venture capital or private equity deal and activities such as refinancing and fundraising are heavily regulated and need extensive documentation. Due diligence related to mergers and acquisitions requires that an organization builds a Virtual Data Room (VDR) to organize and ease buying and selling processes.

eDiscovery technology automatically detects red-flag issues in the due diligence process. Sellers can find and fix potential problems early by reviewing the VDR before any information is disclosed to third parties. Auto-redaction protects sensitive and confidential information while it is gradually disclosed to potential buyers in a secure, controlled environment.

Blacklining also protects corporate intellectual property. Manually detecting and redacting information about proprietary technologies and other sensitive commercial information is exactly the type of time-consuming and dull work that makes people flee from the room when you mention eDiscovery. Its tedium also makes it exceptionally prone to human error, which is avoided when using technology.

During cross-border or large mergers and acquisitions, eDiscovery technology can be helpful in conducting a proactive FCPA investigation to avoid future liabilities or to respond to second requests from regulatory agencies such as the Federal Trade Commission and the European Commission Directorate-General Competition.

EDISCOVERY TAKES OFF

The road to today's advanced eDiscovery software emerged from a path beaten during two decades of legal technology advancements. Antiquated eDiscovery software was reactionary, always playing catch-up on a road continually repaved to cover potholes created by new technologies.

Advanced eDiscovery technology looks to the road ahead, completely adaptable to covering new potholes that pop up as advanced data analytics inform our decisions, AI teaches computers what to look for, and blockchain, robotics, the Internet of Things and other innovations make their way across the globe.

Modern eDiscovery informs and educates decision makers by providing intelligent insights and actionable answers that are far more helpful than the simple search results provided by yesteryear's technology.

We confess to being oddballs who feel eDiscovery is worth celebrating every day. While we may be a little over-enthusiastic, we feel we have, without a doubt, arrived at a time when eDiscovery can be happily discussed in polite society without the crowd making a beeline for the door.

In fact, every year more organizations are bringing eDiscovery processes in-house to save time and money. But that's another story, which you can read all about in the whitepaper "Bringing eDiscovery In House." You may also be interested in the whitepaper "The hidden costs of eDiscovery," in which we investigate the question "Why is eDiscovery so expensive (and does it has to be)?"

