

# [Infographic] eDiscovery Opportunity Costs: What Is the Most Efficient Approach?



[How much does discovery cost?](#) That's a tricky question—and the honest answer is, it depends.

On a national level, the ABA estimates that document review alone accounts for more than [80 percent of total litigation spend](#), or [\\$42.1 billion dollars a year](#), and as data volumes increase, that number is only going to go up.

On a case-by-case basis, eDiscovery costs depend on multiple factors, including the size and type of data, the complexity of review, and, most importantly, the eDiscovery solution employed—that is, whether you review documents manually, use a vendor, do an in-house review using legacy software, such as Relativity, or go with a cloud provider.

So what does this mean for your case? As it turns out, generating an accurate per-case estimate is more complicated than you'd think. Provider type and data size can give you a rough idea of potential monetary spend, but per gigabyte estimates are often inaccurate because they don't account for opportunity costs, like time lost to slow software. In other words, [eDiscovery](#) can cost you more than money. Insecure and slow solutions carry serious risk, including potential security breaches, court sanction, and straight-up loss of sanity.

*Check out our eDiscovery cost infographic below, then read on for startling statistics on the real cost of eDiscovery, as well as tips for protecting your firm and reducing overall spend.*

## Want to see Logikcull in action?

Let us show you how to make Logikcull can help you save thousands in discovery.

Get a demo

## eDiscovery SPEND



**ACTUAL**

VS

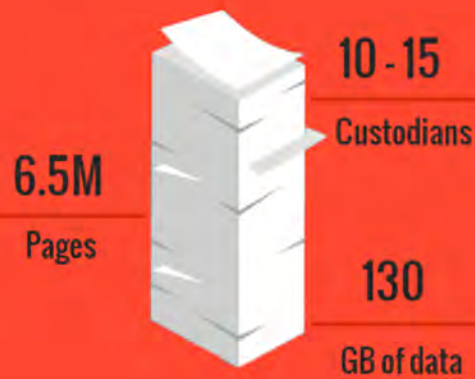
**OPPORTUNITY**

costs



## Data Volume

The average case contains:



This is equivalent to  
100 **TRUCKLOADS** of data.

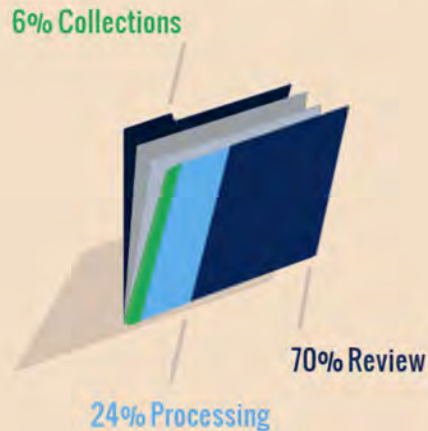


(x100)

And it could cost you.

## Discovery Spend

Where the money goes:

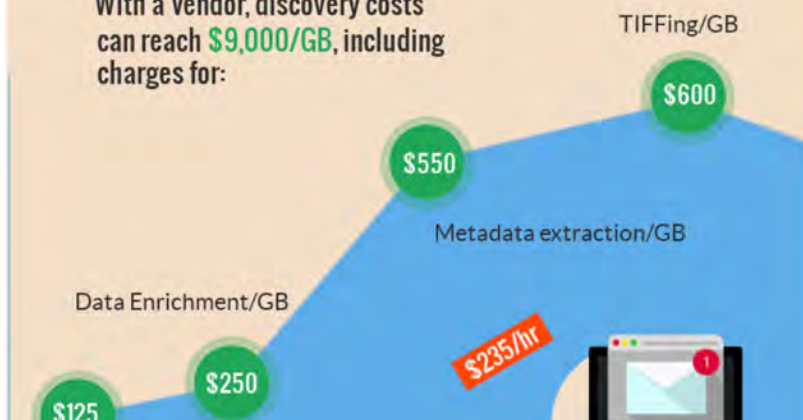


**70%** of discovery costs are tied to the actual review of documents

**35%** of all costs in federal litigation can be attributed to eDiscovery

**\$1M** given average data volumes, per case costs can top \$1M

With a Vendor, discovery costs can reach **\$9,000/GB**, including charges for:

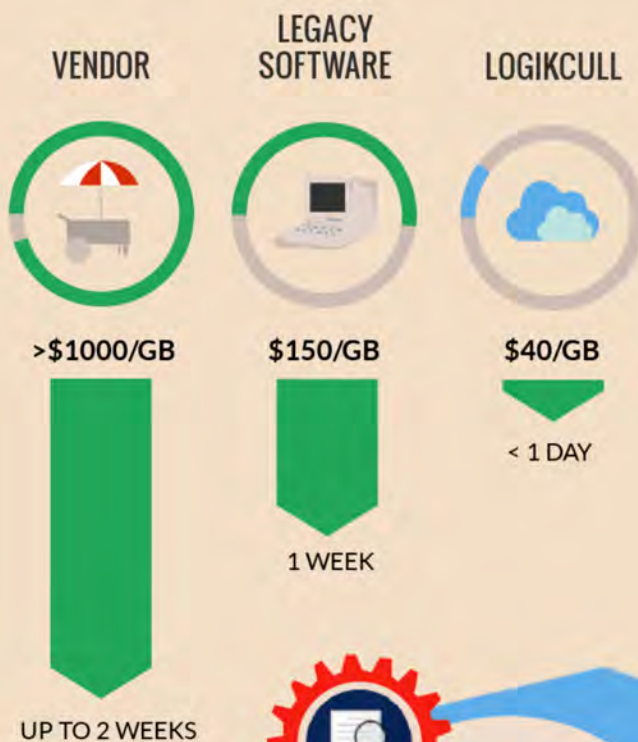


Data ingestion/GB

Some vendors charge \$235/hr  
for project management

## Time Costs

### Time to Review:



### RAM

Vendor speed  
depends  
on local  
RAM

24 HRS

In one 2016 lawsuit  
against United Airlines,  
it took a vendor 24 hours  
to process 3 GB of data

6 HRS

Attorneys spend 6  
hours a day on non-  
billable work, such

## Hidden Costs

1

### Security

Who has your data? When you hand your data over to a third party, like a vendor, you're creating an **open-loop system** — and putting your data at risk.



**\$4.2M**

U.S. companies pay the highest price after an attack: an average of \$4.2M in lost profits

**\$80B**

Data breaches cost the U.S. economy between \$60B and \$100B in 2016

### WHO'S LIABLE?

(Hint: it might you)

Vendors may be contractually required to protect your data, but if a breach occurs, you can still be held liable.

### WHO'S YOUR HVAC VENDOR?



In 2013, Target suffered one of the largest hacks ever, when hackers exploited vulnerabilities in the company's third-party HVAC vendor's system

**Damages:** \$220 Million



In 2017, the same thing happened to Verizon. The company was held liable for ESI leaked by one of their vendors.

**Damages:** 14 million users exposed

## 2 Sanctions

Incompetent or slow discovery  
is grounds for court sanction

### DISCOVERY DEADLINES

When a judge sets a discovery  
deadline, the court may extend  
time if the party failed to act  
because of "excusable neglect"

### BEWARE

Vendors take **60x longer to process data**, and  
waiting on a slow vendor does not count as  
excusable neglect. In **2016**, a federal judge  
called that excuse "lame" and **sanctioned the  
offending attorney**

### TL; DR

Don't be that guy who gets  
tossed for waiting on a vendor



## 3 Sanity

Ever been up at 3am  
trying to complete a  
production? Discovery  
doesn't have to be like that.

eDiscovery is expensive, but it can cost you more than  
money. Long processing times and insecure data storage can  
put your career — and your clients — at risk.

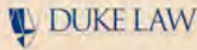
Brought to you by

**logikcull**.com

Statistics from:



ABOVE THE LAW



## The Monetary Costs of eDiscovery Today

On a basic level, the average monetary cost of eDiscovery can be estimated based on data volume. In the U.S., a civil case typically contains around 130 gigabytes, or 6.5 million pages of data, gathered from 10 to 15 custodians—roughly equivalent to the number of pages you would need to fill 100 pickup trucks. In 2012, [a Rand study](#) estimated that each gigabyte costs \$18,000 to produce, with up to 70 percent of costs going to documents, which would put the average case-cost around \$2.3 million.

However, it is important to note that the Rand study drew on data from only 8 large corporations, and discovery costs have generally gone down in the past six years. So, with that in mind, let's cut the average cost in half, to \$9,000 per gigabyte. That still puts per-case cost at around \$1 million, or 16 times the median household income.

*Average per-case eDiscovery cost: \$1 million, or 16x the median household income*

[Another estimate](#), from the of Minnesota Journal Law, Science & Technology, puts that number closer to \$1.3 million, with 94 percent of costs going to document review and processing, and a mere 6% earmarked for collection and production combined. Either way, you'd have to win Family Feud more than 50 times to afford discovery in the average civil case. Of course, most cases aren't average, so those per gigabyte figures are a bit misleading, but they illustrate just how outrageous eDiscovery can become.

*You'd have to win Family Feud more than 50 times to afford discovery in the average civil case.*

And if \$1 million a case seems crazy to you, hold onto your hat. Because that figure fails to capture an entire segment of eDiscovery providers, namely vendors, who can charge much more than that.

## Vendors

With a traditional third-party vendor, eDiscovery costs can easily reach seven or eight digits, especially in data-intensive cases. For example, in one [Apple v. Samsung patent case](#), Samsung paid \$13.1 million to produce 3.6 terabytes (or 3,600 gigabytes) of data. According to court records, that total included hundreds of thousands of dollars in license fees, charged per gigabyte, thousands of dollars in reviewer training, and more than 1,500 individual uploading charges, which range from \$0.20 to \$1,306—but no charges for document review. Assuming that \$13.1 million covered collection, processing, and production, that still leaves 70 percent of costs, or \$30.5 million unaccounted for, bringing the total discovery cost to a whopping \$43.6 million, or **\$12,129 per gigabyte**.

Nickel-and-dime fees, such as upload charges, may seem ridiculous, but according to vendor invoices, they are actually quite common. For example, in [Recognicorp, LLC v. Nintendo Co. LTD and Nintendo of America Inc.](#) (W.D. Wash. 2016), litigants paid an eDiscovery vendor \$150/GB for processing, \$600/GB for TIFFing/Production, \$175/hr "technology fees," and \$235/hr for project management. In another case, [B.L. Mukherjee v. The Children's Mercy Hospital](#), a vendor charged \$90/GB for "pre-processing" and \$80 for a 1TB external hard-drive, which you can pick up at Walmart for half that. In short, litigants are paying through the roof, often for tasks they could easily complete themselves, with the right software.

## In-House or On-Premise Legacy Software

As data volumes continue to increase, firms are looking for ways to cut spending, and shedding vendors is first on the list. For this reason, many law firms opt to bring eDiscovery in-house, purchasing subscriptions to legacy software.

Bringing discovery in house can certainly bring the charges down, but it's still going to cost you. A yearly software subscription runs around \$200,000, plus \$40,000 a year for maintenance, and per gigabyte charges for data uploads and downloads. If you want to host data on-site, you'll need to buy servers and pay a few engineers to maintain those servers, and if you go off-site, you'll need to pay hosting fees. Then, you either have to train your attorneys to use it (which means they have to read [this 151-page user manual](#)), or hire eDiscovery experts to manage your process at \$448/hr. In all, you're looking at around \$2.3 million for the whole system, with a three-year replacement cycle.

Assuming your firm handles more than two cases per year (which I think we can all agree is a safe assumption), that in-house system is looking pretty good, but you also have to account for the significant time and opportunity cost incurred when employees are performing eDiscovery instead of their normal job duties. According to [Clio's 2017 Legal Trends Report](#), attorneys spend up to 6 hours a day on non-billable work, including administrative tasks like document collection and configuring technology. Do you want your most experienced staff converting docs to PDFs, or you do want them strategizing about their case? More on that later.

# Cloud-based eDiscovery With Logikcull

With Logikcull, you can forget about nickel-and-dime or maintenance fees. Instead, you're looking at a flat, per gigabyte price (\$40/GB), which includes uploads, processing (including OCR and PDF splitting), an advanced search platform, and production. Even if your case contains twice the average data volume (or 260GB) you'll have [sliced your total discovery cost by a factor of 10](#).

## Hidden Costs of eDiscovery

Picking the wrong eDiscovery solution can hurt your budget, but it can also cost you in other areas, slowing your case down, exposing you to court sanction, reducing attorney effectiveness, and leaving your data vulnerable to hackers.

Producing data through a vendor can take twice as long as it takes in-house and nearly 60 times longer than it takes with a cloud vendor, due to a number of factors, such as endless back-and-forth emails, limited, 9-to-5 accessibility, long error reports, and straight-up slow processing speeds.

The time it takes a vendor to process your data depends on the bandwidth and RAM of their machines, and even simple snags, such as password protected files, can cause long delays, throwing your case off schedule and putting you at risk for court sanction. For example, in one 2016 lawsuit against United Airlines, a vendor took 24 hours to process a mere 3 gigabytes of data, causing the plaintiff to miss his production deadline—and earn a [verbal shellacking](#) from the presiding judge. Plus, most vendors keep to a strict 9-to-5 schedule, so if there is a problem with your data, it will probably have to wait until morning.

*In one 2016 lawsuit against United Airlines, a vendor took 24 hours to process a mere 3 gigabytes of data, causing the plaintiff to miss his production deadline—and earn a verbal shellacking from the presiding judge.*

Courts have grown increasingly impatient with a [claimed lack of understanding of discovery](#) and turnaround time. Judges know that effective discovery tools exist, and they expect parties to use them. So, slow discovery can certainly get you in trouble, but it can also hit you where it hurts most: slashing billable hours and reducing the amount of time attorneys spend doing their actual job. You can't bill "dealing with vendor error report" back to the client. That means lost income, on top of what you're already paying to outsource or update in-house hardware in the first place, and fewer hours for winning cases, which could hurt your firm in the long run.

*Judges know that effective discovery tools exist, and they expect parties to use them.*

Additionally, when you hand your data over to a third-party, like a vendor, you create an [open-loop system](#), putting your clients' data at risk. While individuals and organizations of any kind can be hacked, law firms and legal vendors are [especially vulnerable](#) because they house large amounts of extremely sensitive data, which turns them into a ["one-stop shop" for cybercriminals](#). Rather than overcome the cyberdefenses of dozens of different businesses, hackers need only break into one, where they can access highly valuable information from a multitude of clients, often for significant gain. In all, data breaches cost the U.S. economy

multitude of clients, often for significant gain. In any, data breaches cost the U.S. economy between \$60 billion and \$100 billion in 2016, and U.S. companies pay the highest price after an attack, an average of \$4.2 million in lost profits.

During discovery, vendors may be contractually required to protect your data, but if a breach of client data occurs, you could be held liable. In 2017, for example, [Verizon was held liable](#) for ESI leaked by one of their vendors, and the same thing happened to [Target back in 2013](#). To avoid this, vet your vendor before signing a contract and make sure to ask about:

- Cloud storage: does access require two-step authentication?
- Remote access: are technical staff working from home? What security configurations are used to secure the connection?
- SOC-II, HIPPA, and GDPR compliance
- Encryption protocols (for data in transit and at rest)
- Any recent leaks within the organization

## Getting the Most from Your eDiscovery Dollar

Actual and hidden costs of eDiscovery make it the most expensive part of modern litigation — but they also make it a great place to cut costs. Knowing the real numbers can help you and your firm stick to the budget and devote less time to doc review and more time to winning cases.

Want to run the numbers? Logikcull's [eDiscovery Cost Calculator](#) helps you predict discovery costs.

### Subscribe to our blog

4,500+ legal professionals love our blog newsletter, where they get the latest tech and discovery news, case law, best practices, and more.



Caselaw — August 28, 2025

### The Growing Importance of Real-Time Data Access in Legal Workflows



Best Practices — August 26, 2025

### The Evolution of Data Subject Access Requests (DSARs) in the Age of AI



Best Practices — August 25, 2025

### Key Features to Look for in an Investigations Software Solution

## Want to see Logikcull in action? Let's chat.

Our team of product specialists will show you how to make Logikcull work for your specific needs and help you save thousands in records requests, subpoenas, and general discovery.

[Get a demo ↗](#)

Join 1,000+ customers using Logikcull to sort and cut the noise for faster, more affordable discovery.

#### Company

[About](#)

#### Use Cases

[Early Case Assessment](#)

#### Learning

[Blog](#)

#### Popular Links

[Get a Demo](#)

[Security](#)

[Pricing](#)

[Reveal](#)

[Onna](#)

[Contact Us](#)

[Litigation/eDiscovery](#)

[Legal Hold](#)

[Legal Holds in Slack 🗨️](#)

[Public Records/FOIA](#)

[Internal Investigations](#)

[3rd Party Subpoenas](#)

[DSARs](#)

[Departed Email Searches](#)

[Data Preservation](#)

[PII Detection & Redaction](#)

[Audio/Video Transcription](#)

[Audio Redaction](#)

[Inside Voices Podcast](#)

[Guides/Whitepapers](#)

[Webinars \(CLE\)](#)

[Industry Reports](#)

[Logikcull Certification](#)

[Case Studies](#)

[What is eDiscovery Software?](#)

[Intro to eDiscovery Basics](#)

[The Ultimate Guide to eDiscovery](#)

[Guide to Slack Investigations](#)

[CLE Webinars](#)

[Logikcull Certification](#)

[Subpoena Response Best Practices](#)

[Legal Hold and Preservation](#)

