

Mobility: Strengthening the Weakest Link in eDiscovery



A guide for IT and legal professionals looking for how to leverage technology to address eDiscovery issues



Executive Summary

The rise of the mobile workforce combined with increasing risks of litigation has created a growing crisis for businesses. As the requirements and complexities of eDiscovery increase, companies are placing new importance on developing their own eDiscovery capabilities. This white paper discusses how mobility trends affect eDiscovery and how businesses can best use technology to simplify it, thus reducing the risks and costs of litigation.

Overview

The rise of the mobile workforce combined with increasing risks of litigation has created a growing crisis for businesses. When faced with a request for eDiscovery, the production of electronically stored information (ESI) in the course of a lawsuit or investigation, legal and IT teams must identify and place holds on responsive files across devices and repositories inside and outside the organization—a costly and time-consuming prospect. Meanwhile, the share of companies facing at least one lawsuit with more than \$20 million at issue reached 34 percent¹.

The share of companies facing at least one lawsuit with more than \$20 million at issue reached 34 percent.



The challenges of eDiscovery are driven in large part by new ways of working. As employees use more devices, messaging systems, cloud-based services and social media, it becomes harder for organizations to keep track of corporate data. When a matter triggers an eDiscovery request, companies often have no choice but to turn to third-party eDiscovery providers, contributing to a sharp rise in costs: companies spending \$1 million or more annually for litigation increased from 53 percent in 2012 to 71 percent in 2013².

As both the requirement for eDiscovery and its complexity increase, companies are placing new importance on developing their own eDiscovery capabilities. In Forrester's Security Survey of Q2 2013, 46 percent of organizations viewed eDiscovery as a "high" or "critical" priority in the coming year, up from 20 percent in 2012. CIOs and general counsels know that technology plays a key role in simplifying and strengthening eDiscovery, but to make informed choices it's essential to first understand the relevant challenges and requirements.

This white paper discusses how mobility trends affect eDiscovery and how businesses can best use technology to simplify it, thus reducing the risks and costs of litigation.

Mobility, social media and cloud services transform business and information governance

Business productivity today is mobile, social and on-demand as people embrace a wide range of devices and services to support their work. Fully three-quarters of the workforce is now mobile and depend on the ability to access, work with and deliver content from anywhere, at any time³. As workers' locations and needs shift over the course of their day, so do the devices they use, from laptops for all-purpose productivity, to tablets for information consumption and light editing, to smartphones for messaging. The average employee now

1. Norton Rose Fulbright, Annual Litigation Trends Survey, 2014.
2. Norton Rose Fulbright, Annual Litigation Trends Survey, 2014.
3. Forrester Research

uses 3.3 connected devices⁴. Often, these include endpoints owned by employees rather than the organization, as people continue to introduce consumer technologies to the workplace—a trend called consumerization.

Consumerization also includes the use of consumer apps and communication channels beyond traditional IT infrastructure, including cloud services, software-as-a-service (SaaS), social media, messaging and productivity tools. Seeking an easy way to sync data across their devices and access files on-the-go, employees frequently use cloud-based file sharing services that are outside IT visibility. A survey conducted by Workshare found that 72 percent of employees use unauthorized free file sharing services for work purposes—rendering large amounts of data and its usage invisible to IT, and creating islands of content that can't be effectively managed or secured⁵.



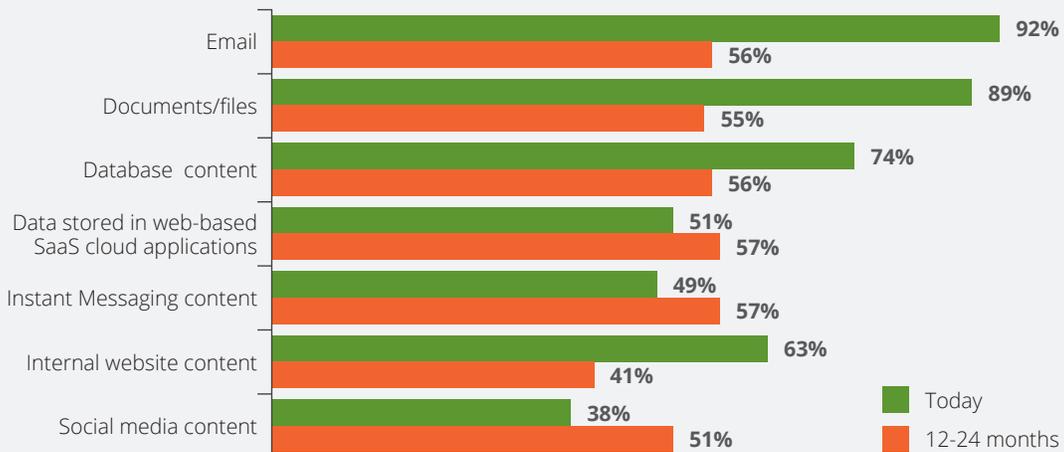
Fully three-quarters of the workforce is mobile. The average employee uses 3.3 connected devices.

According to a Forrester Thought Leadership Paper on governance and eDiscovery, 44 percent of IT and litigation leaders believe that data on user devices is at risk at their organization⁶.

These trends, developing in tandem with expanding requirements for not only eDiscovery, but regulatory compliance as well, are placing pressure on traditional information governance models. It's no longer enough to focus solely on corporate laptops, desktops, phones and servers. IT now faces the challenge of governing data scattered across

Shifting Focus in Data Targets

Thinking about the devices you selected in the previous question, which of the following types of data on these devices are targets for governance at your organization?



Base: 205 IT and litigation professionals at enterprises in US and UK
Source: A commissioned study conducted by Forrester Consulting on behalf of Druva, August 2014

4. Cisco IBSG Horizons
5. Druva 40 Scary Stats presentation
6. Druva-sponsored eDiscovery Thought Leadership paper 2014

Mobility Growing in the Workforce

Which of the following end-user devices are targets for governance at your organization?



Base: 205 IT and litigation professionals at enterprises in US and UK

Source: A commissioned study conducted by Forrester Consulting on behalf of Druva, August 2014

both corporate and employee-owned mobile devices. The rise of mobility is also reshaping the information environment to be governed. To make data available anywhere, on any device, business applications must transmit corporate data over multiple channels and access documents anywhere—data center or cloud—instead of being confined solely to private corporate networks with controlled repositories.

Businesses are also accountable for more types of data, including many beyond the scope of traditional information governance, such as social media, SaaS, file-sharing services, collaboration sites and instant messaging. The Forrester TLP on eDiscovery reports that email, social media and IM content will play a growing role in governance in the coming years.

At a high level, the problem is simple: more and more important company business is being conducted outside the firewall, and litigation best practices call for it to be thoroughly, effectively governed.

Only 51 percent of companies are confident they can preserve data on mobile devices for litigation, regulatory or investigative requirements.



IT organizations struggle to address rising litigation costs

The growing information governance challenge contributes to an ongoing rise in litigation costs, as organizations struggle to apply litigation holds and perform discovery on potentially responsive data spread across an unknown array of devices and repositories. In fact, according to Deloitte, only 51 percent of companies are confident they can preserve data on mobile devices for litigation, regulatory or investigative requirements.

IT typically lacks the resources, staff and skills to address these new requirements, leading to costly outsourcing of eDiscovery



and governance activities. In the Forrester TLP, 48 percent of legal and IT respondents report that understaffing drives them to outsource eDiscovery or governance activities; 35 percent of legal respondents and 33 percent of IT respondents cite a lack of in-house IT skills. Hoping to minimize these costs, some organizations try to repurpose traditional backup solutions as a means of collecting responsive data from endpoints, but this is at best an incomplete strategy that fails to address critical eDiscovery needs such as legal holds and audit trails.

Companies that are unable to perform eDiscovery on mobile devices—or think they can, only to learn that they haven't uncovered the right data or locked it down correctly—can end up in a highly compromised position.

Below are three real-world examples of how a lack of effective eDiscovery capabilities led to negative financial consequences in court:

- In *Small v. University Medical Center of Southern Nevada*, a court-appointed eDiscovery special master recommended that the court enter an order of default judgment (among other sanctions) in favor of over 600 named plaintiffs in a wage and hour class action. The special master was especially critical of the defendant's failure to preserve text messages and other mobile device data both on company-issued BlackBerry devices and from personal smart phones that employees used under a BYOD policy⁷.
- In *Regas Christou v. Beatport*, the defendant was sanctioned for taking "no steps to preserve text messages." While finding the spoliation to be the likely result of negligence rather than intent, the court observed that "Those text messages, few as they might have been, should have been preserved and either provided to the plaintiff or potentially made the subject of further proceedings before the court."⁸
- In a matter involving Pradaxa Products liability litigation, a U.S. District Court judge imposed nearly \$1 million in

punitive damages on Boehringer Ingelheim International GmbH and Boehringer Ingelheim Pharmaceuticals, Inc. The judge showed no sympathy for the defendants' arguments that their ignorance of the business-related texts on employees' smartphones was not their fault, or that the expectation to preserve and produce text messages was "too burdensome."⁹

As a practical matter, it's not unusual for a company to choose to settle a lawsuit just to avoid the uncertainty and risk of eDiscovery in a complex and opaque information environment. In fact, a litigant may specifically design discovery requests to target likely gaps in a company's information governance capabilities. In either scenario, the lack of effective eDiscovery capabilities can lead to direct financial consequences.



Only 22 percent of IT and litigation leaders think they have the right technology in place to enforce and execute governance policies on user devices.

CIOs wake up to the gap between IT and legal

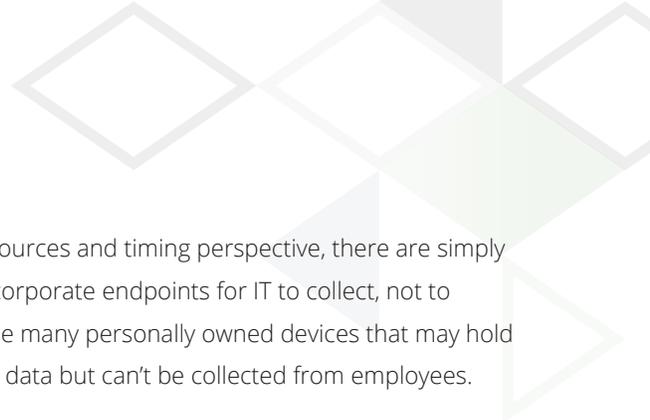
Only 22 percent of IT and litigation leaders think they have the right technology in place to enforce and execute governance policies on user devices¹⁰. Seeking to gain control over the issue, some companies reflexively try to restrict the information environment, applying measures such as preventing access to IT services beyond the firewall and revoking access to email and other corporate services on devices that also contain personal applications. This approach is ineffective at best and can often be counterproductive.

7. <http://www.recomind.com/blog/2014/09/11/breaking-news-mobile-device-preservation-failures-lead-doomsday-ediscovery-sanctions>

8. <http://www.exterro.com/e-discovery-beat/2013/02/21/text-messages-must-be-accounted-for-in-e-discovery/>

9. wjta.wordpress.com/2014/02/13/costly-penalties-imposed-for-pharma-companys-failure-to-comply-with-e-discovery-requests/

10. Druva-sponsored eDiscovery Thought Leadership paper 2014



Unable to meet their needs through IT-sanctioned systems, employees are likely to switch to less secure workarounds such as emailing files to their personal accounts or using consumer file-sharing services, creating even wider security gaps and making governance even more elusive. Instead, organizations need a better approach to information governance—one that enables effective eDiscovery and gives legal and IT teams what they need in order to respond to lawsuits and regulatory orders without disrupting the flow of business.

More effective eDiscovery is becoming a top priority for CIOs and IT decision-makers, with special focus on technologies which discover content from user devices and enforce policies on those devices - whether owned by the business or the employee. Seeking to curb costs and increase control, many companies are moving from outsourcing providers to an in-house strategy for identifying, preserving, collecting and processing eDiscovery data. Forrester reports that 85 percent of organizations expect to rely on technology for eDiscovery in the next two years, a 34 percent increase from today and a 61 percent increase from two years ago¹¹. This broad adoption is driving double-digit revenue growth in the market for enterprise eDiscovery software, from \$1.8 billion in 2014 to \$3.1 billion in 2018¹².

From reactive to proactive eDiscovery: Including endpoints in your data collection strategy

A better approach to eDiscovery must be informed by an understanding of the shortcomings of current approaches. In too many organizations, digital data is collected in the same way that paper data has been: manually. IT either asks people to send their laptops to a central location or sends a team into the field to collect devices or data from employees. The problems with this method are numerous:

- From a resources and timing perspective, there are simply too many corporate endpoints for IT to collect, not to mention the many personally owned devices that may hold responsive data but can't be collected from employees.
- There are too many repositories to search manually, including email, enterprise content management (ECM) systems, databases and SaaS repositories. The stores to be searched include not only on-premise corporate systems, but also cloud-based and third-party services with varying levels of accessibility.
- As the manual search is being conducted, IT has no way to ensure the integrity of the data being collected.
- Users whose devices have been collected face potentially protracted downtime without access to their usual tools and business information, increasing overall litigation costs.



Traditional eDiscovery methods are also undermined by a more fundamental flaw: reactivity. Each process begins from scratch as the company learns about the litigation, the general counsel informs IT of the relevant custodians, IT pulls together an eDiscovery team, and data is collected and stored. This amounts to reinventing the wheel each time, instead of ensuring that the company is well prepared for litigation even before it arises and is positioned to respond to eDiscovery requests in a rapid and repeatable way.

11. Druva-sponsored eDiscovery Thought Leadership paper 2014
12. Gartner, Magic Quadrant for eDiscovery Software, 2014.

Instead, IT needs to take a proactive approach to eDiscovery, implementing a way to discover and collect data on mobile endpoints in advance so that when a matter arises, the company is ready to comply with eDiscovery requests without the manual work, disruption and unpredictability of traditional methods. This approach should include:

- Centralized governance processes designed to reduce complexity and increase visibility and control over today's decentralized information environment. Centralization is critical to reduce the need to collect dispersed endpoints or to venture into the field to identify data device-by-device.
- Data visibility and audit trails to demonstrate a clear, unbroken chain of custody for responsive data, including all the touch points involved in the discovery process.
- A non-intrusive way to collect data from endpoints without disrupting user productivity unnecessarily.
- The ability to place legal holds on data of all types, wherever it may reside—including on personally owned devices and third-party repositories.
- Integration with downstream eDiscovery solutions for review and analysis to streamline the handoff between systems, reducing manual intervention and lessening the chance of data being compromised.



Conclusion: the benefits of better eDiscovery

A proactive approach to eDiscovery data collection reduces both litigation risk and cost.

- A complete in-house data collection capability eliminates the need to outsource and pay high third-party fees.
- Not having to set up as much intermediary storage or a separate collection server for mobile devices reduces cost.
- IT spends less time and money on data management and can recover files far more quickly.
- By spending less time collecting data, IT and legal can devote more time to analysis to ensure that the dataset is correct and complete.

Traditional approaches to eDiscovery are increasingly inadequate in the face of workforce mobility and an increasingly dispersed and complex information environment. As litigation costs rise, companies need a way to ensure complete and effective eDiscovery while reducing their reliance on expensive outsourcing. To avoid costly errors and to control internal costs, the approach must be both proactive and comprehensive, centralizing all data—including on corporate and employee-owned devices—before litigation arises so that it can be discovered quickly and managed as needed. With the right technologies in place, the company can achieve more effective governance across corporate information no matter where it resides—to support both eDiscovery and regulatory compliance for even greater return on investment. IT spends less time on manual data management and collection, users face less disruption from data collection processes, and the business reduces the cost and risk of litigation.

About Druva

Druva is the pioneer and market leader in data protection and governance at the edge of the enterprise, bringing visibility and control to business information in the era of the mobile workforce and consumerization of IT. Druva's solutions for managing data outside the corporate firewall reduce the loss of corporate information assets and address organizations' compliance, governance, forensics and eDiscovery needs. Headquartered in Silicon Valley with offices worldwide, Druva is privately held and is backed by Nexus Venture Partners, Sequoia Capital and Tenaya Capital. For more information, visit www.druva.com and connect at www.druva.com/blog.

More Resources

To learn more about tools and best practices for eDiscovery, please refer to the following:



[A Forrester Thought Leadership Paper: Governance Takes A Central Role As Enterprises shift to mobile](#)



[Overview of eDiscovery readiness](#)



[Endpoint Data Protection for HIPAA-Regulated Organizations](#)

For more resources, visit druva.com/resources.



Druva, Inc.
Americas: +1 888-248-4976
Europe: +44.(0)20.3150.1722
APJ: +919886120215
sales@druva.com
www.druva.com