

Top eDiscovery Sources for Locating Vital Employee Content in the Cloud

Description

Originally published in February of 2023. Updated on April 11, 2024.

As companies continue to embrace cloud technology in the workplace, understanding where important employee content is stored in the cloud has become crucial. In a legal dispute, eDiscoveryâ??the process of locating and producing relevant dataâ??is critical. This post discusses the top eDiscovery sources for locating vital employee content in the cloud, incorporating recent developments and tools.

- **Email accounts:** Email remains a critical source of evidence in eDiscovery. Employeesâ?? email accounts may hold crucial information relevant to a case, including communications with colleagues, clients, or customers and attachments like documents, images, or audio recordings. Tools like Pinpoint Harvester are essential for collecting data from email accounts, and they can search through various email formats to extract pertinent messages and attachments based on specific criteria.
- **Cloud storage platforms:** Cloud storage platforms such as Dropbox, Google Drive, Box, and OneDrive are indispensable for storing essential files and documents. These platforms can contain documents, spreadsheets, presentations, and more. eDiscovery collection tools like Pinpoint Cloud Collector, SharePoint Collector, and CrossCopy Enterprise are designed to collect data from these sources securely and defensibly.
- **Social media accounts:** With the rise of social media platforms like Facebook, Instagram, and X (formerly Twitter), these accounts can contain case-relevant information, including public and private communications. Newer platforms and features like Stories and Reels may also hold ephemeral but relevant content that requires specialized collection tools and strategies.
- **Collaboration tools:** Collaboration tools, including Slack, Microsoft Teams, and newer entrants like Discord, have become central to employee communication and potentially contain vital information related to a case. These platforms may house shared files, images, audio recordings, and even code snippets or project management boards, necessitating comprehensive eDiscovery collection approaches.

- **Company-specific systems:** Beyond generic platforms, companies often use custom systems like customer relationship management (CRM) systems, human resources management systems (HRMS), and enterprise resource planning (ERP) systems. These systems can store vast data, including customer interactions, employee records, financial transactions, and operational data.
- **Emerging sources:** With technological advancements, new data sources are becoming increasingly relevant for eDiscovery. These include:
    - Internet of Things (IoT) devices: Smart devices in the workplace can generate data relevant to investigations or disputes, such as access logs or sensor data.
    - Cryptocurrency transactions: For companies engaged in or accepting cryptocurrencies, transaction ledgers may become pertinent in financial disputes or investigations.
    - End-to-end encrypted messaging apps: Apps like Signal and WhatsApp offer end-to-end encryption, presenting unique challenges for data collection and requiring specialized eDiscovery approaches.
- **Mobile Device Collections:** In todayâ??s digital age, mobile devices are treasure troves of information that can prove invaluable during eDiscovery and Digital Forensics. As smartphones have become ubiquitous in personal and professional spheres, the data stored on these devices, including Android and iOS systems, encompasses various formats and sources.

Valuable eDiscovery and Digital Forensics mobile device sources include messaging apps such as WhatsApp, Signal, Viber, Line, and WeChat, which have become primary communication channels. These apps can contain messages, shared files, images, and even voice notes, all of which may be pertinent to a case. Call logs, images, videos, application-specific data, and location data can also play a critical role.

Companies must maintain an up-to-date understanding of their data landscape and implement data retention policies and procedures to ensure that essential data is preserved and accessible. Proactively addressing the legal implications of cloud-based data storage can minimize legal dispute risks and prepare companies to swiftly locate and produce relevant employee content for eDiscovery requests.

With the evolving use of cloud technology, mobile devices, and digital communication platforms in the workplace, companies must stay informed about where their data is stored and how it can be accessed in case of a legal dispute. By considering the expanded range of eDiscovery sources discussed in this blog post, companies can enhance their preparedness for any legal challenges.

Date
11/25/2026
Date Created
02/10/2023