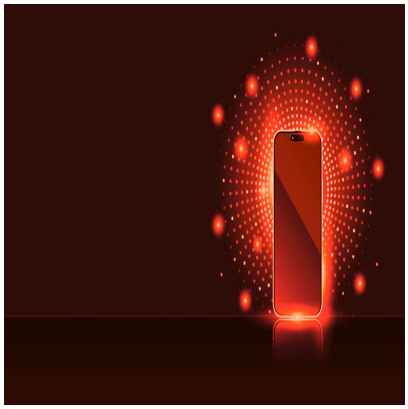

Transforming Mobile Data Collection in eDiscovery Processes

Description

Mobile data is a critical component in today's eDiscovery processes, requiring modern solutions to manage the unique challenges it presents to legal teams. The widespread use of mobile devices and their vast data, ranging from SMS and WhatsApp messages to call logs and app data, presents distinct challenges for legal and forensic teams. As these collections grow in scope and complexity, it becomes imperative to address several key issues that often complicate the process. Two of the most pressing concerns involve the need for physical collection kits and the debate over comprehensive versus targeted data collection strategies. Let's explore these issues and potential solutions to streamline mobile data collections for eDiscovery.

1. **The Necessity (and Drawback) of Physical Collection Kits—**One common practice in mobile forensic collections is deploying physical collection kits, including computers and specialized software, directly to custodians or field agents. While this can be necessary when custodians lack the required hardware, it presents several drawbacks. For instance, shipping computers and equipment to various locations can incur significant costs and logistical complications, especially when dealing with international custodians. Additionally, training non-technical custodians to use the equipment properly can lead to user errors, data corruption, or incomplete collections. This method also introduces the risk of data being altered during the collection process, compromising the defensibility of the data in court.

   A more efficient solution could involve remote, software-based data collection methods that leverage the custodian's existing devices. Legal teams can reduce costs, minimize user error, and expedite the collection process by deploying secure, user-friendly applications that custodians can download and operate from their devices. However, this approach requires careful consideration of security and privacy concerns to ensure the collected data remains intact and unaltered.

2. **Comprehensive Backups vs. Targeted Data Collection—**Another significant challenge in mobile

data collection for eDiscovery involves deciding between comprehensive backups and targeted data collection. Many traditional collection methods require custodians to create complete backups of their devices, including personal photos, contacts, and app data. While comprehensive backups ensure all potentially relevant data is captured, they also bring many privacy issues and may violate regulations such as GDPR. This can feel like an invasion of privacy for custodians, leading to resistance or even non-compliance.

A more effective approach is to focus on targeted collections, capturing only the specific data types relevant to the case—such as SMS messages, WhatsApp chats, or call logs—while excluding irrelevant personal information. This reduces the amount of data legal teams need to sift through, decreasing review times and costs and respecting custodians' privacy. Moreover, targeted collections reduce the risk of inadvertently collecting privileged or sensitive data, making them a more compliant and ethical choice.

3. **Handling Diverse Data Formats and Encryption Challenges—**Mobile devices often store data in various formats and across multiple apps, making it challenging to standardize the collection process. For example, iOS and Android devices have distinct ways of storing and encrypting data. Additionally, apps like WhatsApp, Signal, and Telegram use end-to-end encryption, adding another layer of complexity. When performing a collection, it's not just about gathering data; it's about decrypting, parsing, and presenting that data in a readable and legally defensible format.

   To mitigate these issues, organizations must invest in tools and solutions that support a wide range of data formats and can decrypt and process encrypted data without compromising its integrity. Continuous training for legal and IT teams is also crucial to keep up with the evolving encryption standards and app data structures.

4. **Managing Cloud-Based and Hybrid Data Collections—**Mobile data is not just stored on the device; it often resides in the cloud. Many custodians use cloud services like iCloud, Google Drive, or OneDrive for backups or to store app data on platforms like Dropbox or Box. eDiscovery professionals must consider both on-device and cloud-stored data when preparing ESI protocols, further complicating the collection process.

   The ideal solution is to use software that seamlessly integrates cloud-based collections, ensuring that all potential evidence, whether on the device or in the cloud, is preserved and collected. Additionally, addressing privacy laws that vary across jurisdictions is critical when dealing with cross-border data collection.

As mobile devices become more central to modern eDiscovery, the industry must move away from outdated, cumbersome practices and toward more efficient, secure, and ethical data collection methods. By eliminating the need for physical kits, focusing on targeted data, and investing in advanced tools and training, legal teams can not only streamline the mobile collection process but also ensure that it is defensible, cost-effective, and respectful of privacy. The goal is to create a balanced approach that meets the needs of legal investigations while safeguarding the rights and privacy of custodians—a challenge that requires both innovation and vigilance.

Date
11/02/2024
Date Created
09/20/2024