PERSPECTIVES

NAVIGATING CLOUD FORENSICS IN COMPLEX INVESTIGATIONS

Our perspectives feature the viewpoints of our subject matter experts on current topics and emerging trends.

Introduction: Understanding Cloud Data in the Modern Digital Landscape

In today's hyper-connected digital world, we interact with vast amounts of data, much of which isn't stored locally on our devices but instead resides on remote servers accessed via the internet. This infrastructure is commonly referred to as the "Cloud."

The shift toward cloud-based platforms began around the mid-2010s with the rise of services like Microsoft Office 365 and Slack. However, the COVID-19 pandemic accelerated this transition, as organizations urgently sought secure, remote collaboration tools. Cloud platforms house a vast trove of data that often goes unnoticed when we think in traditional terms of data storage. From file sharing and document collaboration to real-time messaging and virtual meetings, cloud platforms have become essential to both professional and personal worlds.

Key Cloud Data Issues and Challenges

With the widespread adoption of cloud services comes a new set of challenges, especially when it comes to data management, legal compliance, data preservation, and forensic investigations. Key concerns include:

» Data fragmentation across multiple providers
» Legal complexities in cross-border / jurisdiction data access
» Data identification and preservation for legal or investigative purposes
» Practical uses of Cloud Data and Digital Forensics

While everyday users may not need to consider these issues, professionals involved in legal, compliance, or investigative roles must be equipped to navigate them. In this article, we will explore each of these four challenges as well as how cloud data and digital forensics work together in modern investigations.

Data fragmentation across multiple providers

Organizations often use a mix of cloud platforms to streamline operations and enhance security. Common providers include Microsoft Office 365, Google Workspace, Slack, AWS, Box, and Zoom. Each platform stores and exports data differently, ranging from emails and documents to chat logs and transactional data.

This fragmentation means data is dispersed across various systems and formats, complicating efforts to collect and analyze it cohesively. For example, exports from Google Workspace and Microsoft Office 365 may differ significantly in structure and usability. Understanding each platform's data capabilities and data policies is crucial for effective forensic collection and analysis. By gaining insight into how each platform creates, stores, and maintains data, we can harmonize disparate information, transforming large, fragmented data into a dataset that is unified. This harmonization is key to making data review more efficient and meaningful.

Legal complexities in cross-border / jurisdiction data access

As mentioned above, cloud data is stored on remote servers and can be accessed via the internet. These servers may be located in different countries, each governed by its own data protection laws. When data is needed for an investigation, accessing it across jurisdictions can raise legal challenges.

We need to be mindful that there is no universal legal framework that covers all cross-border data access. Consulting legal experts is strongly recommended to avoid potential violations of international data protection laws. A few key regulations with stringent policies to be aware of include:

» **General Data Protection Regulation (GDPR)** – European Union
» **Digital Charter Implementation Act** – Canada
» **Personal Information Protection Law (PIPL)** – China

Even if data can be remotely accessed or exported, understanding where it resides and the applicable legal boundaries is important.

Data identification and preservation for legal or investigative purposes

Depending on the cloud platform, identifying and exporting data for investigations can range from straightforward to complex. Many platforms offer built-in export tools, but these may not always preserve critical metadata, contextual logs, or provide the necessary level of detail required in an investigation.

In such cases, advanced forensic tools may be required to ensure data integrity and completeness. It's also important to consider how the data will be used downstream, for example, whether it needs to be compatible with eDiscovery platforms or other analytical tools.

Practical uses of Cloud Data and Digital Forensics

Cloud data and digital forensics go hand-in-hand with modern investigations. In short, a lot of information can be retrieved from cloud platforms, and how it's used depends on the issue. Here are a few examples of how cloud data and digital forensics can be used today:

1. Government Regulatory Inquiries: Often times corporations may be required to produce documents in response to a government investigation. Cloud platforms can expedite this process by enabling quick identification and export of relevant data such as emails, shared folders, and chat records.

2. Workplace Misconduct Investigations: In cases of suspected employee misconduct, such as the misappropriation of trade secrets, cloud audit / user logs can reveal user activities, including login times, IP addresses, email communications, and document access or sharing. These logs help reconstruct timelines and uncover potential violations. Additionally, if a user has sent trade secrets to an external email address, those messages can be discoverable through the cloud platform.

3. Business Email Compromise (BEC) / Unauthorized Access: For cybersecurity incidents like BEC or unauthorized access, audit / user logs are invaluable. They can show how a bad actor gained entry, what actions were taken, and whether access was extended to other cloud environments. This information is critical or containment and remediation.

Conclusion

In a nutshell, navigating cloud forensics requires a deep understanding of how modern cloud platforms store, manage, and protect data. With data often being fragmented across multiple providers and jurisdictions, leaders in this space must be mindful of technical, legal, and procedural challenges. Success in cloud forensics relies

on preserving critical evidence, normalizing disparate data, and ensuring compliance with local regulations and laws. As cloud services continue to evolve, so too must our strategies and tools used to investigate and secure digital evidence.

Acknowledgements

We would like to thank our colleague, Richard Chung, for providing insight and expertise that greatly assisted this research.

Richard Chung is a Managing Director providing Digital Investigations & Discovery services within J.S. Held's Global Investigations practice. Based in New York, he has more than 18 years of experience in technology consulting. His expertise is in digital forensics and e-discovery, in connection with all aspects of investigations, litigation, and antitrust and merger matters. Richard has worked across a wide variety of industries, including financial services, pharmaceutical, healthcare, construction, energy, and technology. His extensive experience and decisive expertise make him a trusted advisor on a variety of technology consulting engagements involving data preservation, data analysis, document review, and document production.

Richard can be reached at
richard.chung@jsheld.com or +1 347 786 8958.