SUMMER 2024 E-NEWSLETTER

At Digital Mountain, we assist our clients with their electronic discovery, digital forensics, cybersecurity, and data analytics needs. For this E-Newsletter, we discuss the digital forensics implications of ephemeral and encrypted messaging data, the rise of two messaging giants, and noteworthy legal developments.

Ephemeral and Encrypted Messaging Continues to Stump Courts

Ephemeral and encrypted messaging, that class of communications applications that can both delete and scramble messages for security, have been a challenge for courts for a decade now. And while some of these applications have completed their lifecycle and have been removed from the market, others thrive because of the security features they offer. As with many other categories of digital evidence, ephemeral and encrypted messaging continues to stump courts as to just how to deal with what is both here and gone today.

In most situations, ephemeral messages are simply gone by the time digital forensics investigators are engaged to collect device images, and encrypted messages can present problems with scrambled text in the absence of the decryption key. However, from the early days of ephemeral and encrypted messaging applications, parties have been able to avoid sanctions from time to time when they could demonstrate that data custodians were not skirting discovery by erasing messages. While in 2015, *Sec. & Exch. Comm'n v. Huang*, (NO. 15-269, E.D. Pa. Sep. 23, 2015) was news because the SEC was prevented from acquiring encryption keys to decrypt data on company-issued cell phones under a fifth amendment challenge, it's now standard in civil litigation eDiscovery to expect decrypted messaging data in production.

The expectation that encrypted messaging application data will be provided however does not create a carte blanche situation. In *FTC v. Amazon.com, Inc.* (No. 2:23-cv-01495-JHC, W.D. Washington, Doc 223, Filed 05/13/24), Amazon responds to the FTC's request for access to Amazon's preservation instructions to executives, especially as they relate to Signal communications. Amazon refutes the FTC's position by first detailing the efforts previously made to show the FTC the extent to which Amazon executives used Signal, how they used it, and finally, with the argument that the messages were not deleted:

> Plaintiffs ask this Court to speculate that the absence of any such messages means that they disappeared. Yet the equally logical

explanation - made more compelling by the available evidence - is that such messages never existed.

The argument that if you can't see them, there's every chance that they were never there presents an interesting question that may require the technical expertise of a digital forensics professional to review on behalf of the court, but for now, on July 9, 2024, Judge Chun ordered that the FTC may conduct a deposition of Amazon on document preservation, during which the FTC may ask questions regarding preservation instructions.

Finally, we want to share a case where the encrypted messaging app Telegram plays a significant role and may indicate a possible technological advancement for the courts. In, *KOZIAR v. BLAMMO, LTD.,* (No. 23-cv-7870 (JGK), Dist. Court, SD New York 2024), an international cryptocurrency scam case, Judge John Koeltl proposed an order allowing certain defendants to be served via Telegram writing, "Because Telegram is an encrypted, contact based, messaging service, Plaintiffs are authorized to transmit the Summonses and Amended Complaint via Telegram." The defendants in question were apparently foreign nationals or residents of a foreign country for which the Plaintiff had only the Telegram aliases and overseas telephone numbers, presenting a challenge to a physical service of process. Interestingly, this case opens the possibility of digital forensics playing a key role in the verification of process services and preserving the digital evidence by showing documents were sent to verified, operational Telegram accounts. Additionally, proving documents were successfully received when possible, could make or break a case, something that digital forensics professionals will be instrumental in evidencing. In this case, a default judgment was obtained. This innovative use of an encrypted messaging application adds to the courts' arsenal of tools with which to pursue justice and reinforce security. By using digital forensics examiners and innovative data security mechanisms, ephemeral and encrypted messaging stumping the courts may be in the rear view mirror.

Please direct questions and inquiries about electronic discovery, digital forensics, cybersecurity, and data analytics to info@digitalmountain.com.

UPCOMING INDUSTRY EVENTS

ILTACON 2024
Nashville, TN: August 11-15, 2024

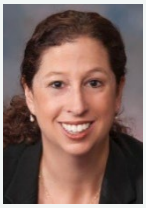
SANS DFIR SUMMIT 2024
Salt Lake City, UT: August 22-23, 2024

THE SEDONA CONFERENCE WORKING GROUP 12 ANNUAL MEETING
Phoenix, AR: September 9-10, 2024

TECHNO SECURITY & DIGITAL FORENSICS CONFERENCE WEST
Pasadena, CA: September 16-18, 2024

MASTERS CONFERENCE SEPTEMBER 2024
Seattle, WA: September 18, 2024

Click here to see more upcoming events and links.



Digital Mountain, Inc. Founder and CEO, Julie Lewis, will be presenting at various upcoming industry events. Please send requests for speaker or panel participation for her to marketing@digitalmountain.com.

DIGITAL MOUNTAIN, INC.
4633 Old Ironsides Drive, Suite 401
Santa Clara, CA 95054
866.DIG.DOCS

www.digitalmountain.com

Contact us today!

FOLLOW US AT: