FALL 2020 E-NEWSLETTER

At Digital Mountain we assist our clients with their computer forensics, e-discovery, cybersecurity and data analytics needs. For this E-Newsletter, we focus on ephemeral communications and the affect of disappearing messages on discovery cases.

Ephemeral Messaging App Use Raises Questions of Intent

Ephemeral messaging app developers are experts at touting the benefits of disappearing communications: automated data elimination keeps devices "cleaner"; hackers and cyber-spies are thwarted from stealing information; lost devices don't raise panic-inducing alarms because ephemeral apps can often be set to overwrite or wipe unseen data after a certain amount of time; and finally, if used as part of a regular, legitimate, and well-implemented policy, data destruction can provide beneficial legal protections. But for every cost, privacy, and legal benefit, there is an equal argument against ephemeral messaging that centers on the intention of the user relying on the app to erase data that could be used to establish some wrongdoing. So, while the courts and various government agencies aren't engaging blanket prohibitions of ephemeral messaging app use, they are looking at the implementations to judge the intentions of users when making determinations. There are two cases in particular that demonstrate the need to follow best practices, and the law, when using ephemeral messaging.

***Waymo LLC v. Uber Tech., Inc.*, No. C 17-00939 WHA, 2018 WL 646701**

This case centers upon Waymo's claim that Uber stole intellectual property by hiring a Waymo executive who, in anticipation of his changing employment, downloaded design material belonging to Waymo. While the case ultimately settled out of court, the question of ephemeral messaging use arose when Waymo alleged that Uber used an ephemeral messaging app to destroy discoverable communications *while subject to a litigation hold*. The court allowed for Waymo to present the evidence that Uber had, in fact, used the app to make relevant information disappear, but also allowed Uber to present evidence that the company used the app as part of a legitimate business practice. The result: Waymo was allowed to claim that their case was undermined by Uber's erasing potentially harmful information, and Uber was able to claim they didn't mean to do it. Perhaps most vexingly, the court left the issue of ephemeral messaging there without directly addressing the question of what responsibility a corporation takes on when using ephemeral messaging apps.

What might appear to be fence-sitting by the court in Waymo, may just be highlighting an area of the Federal Rules of Civil Procedure ("FRCP") that was significantly reinterpreted in 2015, Rule 37(e). In 2015, the rule was re-examined and among other notes, the following was added:

> The rule applies only if the information was lost because the party failed to take reasonable steps to preserve the information…**As under the current rule, the routine, good-faith operation of an electronic information system would be a relevant factor for the court to consider in evaluating whether a party failed to take reasonable steps to preserve lost information, although the prospect of litigation may call for reasonable steps to preserve information by intervening in that routine operation.** This rule recognizes that "reasonable steps" to preserve suffice; it does not call for perfection…(https://www.law.cornell.edu/rules/frcp/rule_37, emphasis added).

Connecting the dots from the 2015 Rule 37 (e) note back to Waymo v. Uber, the court's position may be the logical outcome of Uber's defense to the allegation that they intentionally destroyed the evidence. The "routine, good-faith operation of [the] electronic information system," in this case the ephemeral messaging app, is that the data is routinely destroyed as part of its good-faith operation. The court's nod to the possibility that Uber's defense was the legal equivalent of a disingenuous shrug is the modified adverse inference that the missing evidence, while it cannot conclusively be determined to have been prejudicial against Uber, certainly created gaps in the case that Waymo was creating.

***WeRide Corp. v. Kun Huang*, 379 F. Supp. 3d 834 - Dist. Court, ND California 2019**

While *Waymo v. Uber* provides support for the idea that ephemeral apps may provide some legal defense to Rule 37(e) and an adverse inference, *WeRide v. Kun Huang* shows just how seriously courts take litigation holds. In *WeRide v. Kun Huang*, the defendant was also alleged to have pilfered intellectual property via the plaintiff's former employees and devices. The court issued terminating sanctions against defendants for their destruction of email, source code, and communications transmitted using the ephemeral messaging app DingTalk. The court interpreted that the defendants' behavior clearly demonstrated an attempt to thwart a litigation hold by, among other actions, moving communications to DingTalk after the hold was put in place. In light of the severity of the sanctions, there's no question that the court was adamant that a litigation hold, Rule 37(e), and the use of an ephemeral messaging app were not subject to interpretation – preserve the data or else.

In cases that hinge on the courts determining the intent of an ephemeral messaging app user, policies and procedures that appear suddenly and in close proximity to a litigation hold are likely to be read as intentionally flagrant destruction, while the benefit of the doubt may be afforded to users and organizations that can clearly demonstrate a regular and thoughtfully established pattern of use. Courts may not rapidly embrace the cutting edge of technology, but they are practiced at discerning intent which can be a gray area when it comes to usage of ephemeral apps. The best approach may still be the most virtuous approach when it comes to ephemeral messaging apps: keep your intentions and your data – on the right side of the law.

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

UPCOMING INDUSTRY EVENTS

THE SEDONA CONFERENCE WORKING GROUP 1 ANNUAL MEETING 2020, VIRTUAL
October 28-29, 2020

DATA CONNECTORS GREAT LAKES VIRTUAL CYBERSECURITY SUMMIT
November 5, 2020

FORENSICS@NIST 2020, VIRTUAL
November 5-6, 2020

THE SEDONA CONFERENCE WORKING GROUP 12 ANNUAL MEETING, VIRTUAL
November 9, 2020

OPENTEXT ENFUSE ON AIR 2020, VIRTUAL
November 10, 2020 - December 1, 2020

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. In the short term, she is available for webinars and remote e-conferences.

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: