FALL 2021 E-NEWSLETTER

At Digital Mountain, we assist our clients with their electronic discovery, computer forensics, cybersecurity, and data analytics needs. For this E-Newsletter, we discuss the growing business messaging application market, eDiscovery nuances and relevant court cases.

Scary Tactics Disturb Courts in eDiscovery of Business Messaging App Data

Horror stories aren't limited to books and movies. Judges and magistrates see their share of tricks and frights in the courtroom. When it comes to the eDiscovery of data from business messaging apps, we're starting to see the scary lengths to which some will go to avoid responding. All Halloween kidding aside, the massive amount of data associated with business messaging apps these days has given rise to disagreements about how that data should be handled from an eDiscovery perspective. For guidance, we look at how courts recently responded to some dramatic issues involving eDiscovery of business messaging apps.

Time is Money but Not That Much

Courts take the six elements of proportionality (relevance, stakes, access, resources, determinative import, and likely influence) outlined in state and federal rules very seriously; however, judges and magistrates also realize that not every estimate of the time and cost required to produce the requested information is realistic or indisputable. In *Benebone LLC v Pet Qwerks Inc.*, No. 8:20-cv-00850, 2021 WL 831025 (C.D. Cal. Feb. 18, 2021), the court determined the plaintiff's estimate that producing 30,000 Slack messages would cost upwards of $110,000 to potentially $225,000 was grossly inflated, especially in light of an expert-witness produced estimate of $22,000, using appropriate eDiscovery tools. In addition to highlighting the cost-benefit of using professional eDiscovery services, the ruling also cautions litigators to assess carefully before presenting the court with exorbitant costs as a reason not to comply with a discovery request.

Preservation is Still Required

While courts are not capitulating to the "it's too much" argument, they're also not giving credence to defenses that amount to lax data preservation practices. When the defendant in *WeRide Corp. v. Kun Huang*, No. 5:18-cv-07233, 2020 WL 1967209 (N.D. Cal. Apr. 24, 2020) dumped email accounts, replaced devices, deleted data including source code and email messages, as well as advised the use of an ephemeral messaging application for business use, the court resorted to no less than terminating sanctions in response to the "staggering" loss of evidence. Trying to hide and destroy data to keep it out of the courts almost never pays off and often results in negatively impacting a case and potential sanctions.

Equally dramatic was the near incredulous mishandling of eDiscovery in *DR Distributors, LLC v. 21 Century Smoking, Inc.*, No. 12-CV-50324, 2021 WL 185082 (N.D. Ill. Jan. 19, 2021), wherein the defendant's counsel, after not following the most basic steps to preserve data, allowed the defendant to conduct the eDiscovery tasks for emails and chat messages, which, not surprisingly, resulted in the loss of data and a very untimely three years to produce a deficient response. The court conveyed its disappointment in no uncertain terms by categorizing counsel's behavior as a "race to the bottom of technical ignorance," and including continuing education on eDiscovery as part of the sanctions. Hopefully, one lesson counsel will learn attending those CLE courses is that eDiscovery is best practiced by those with the proper experience and credentials, and not by those with a vested interest in seeing data disappear.

Not all attempts to thwart discovery end with terminating sanctions or orders to attend continuing education programs. Some attempts, like those made by the defendants in *FTC. v. Noland*, No. CV-20-00047-PHX-DWL, 2021 WL 3857413 (D. Ariz. Aug. 30, 2021), end with a determination that "general adverse inference" instructions are an adequate consequence. In this case, the court determined that all missing communications from the defendants' emails and chat records and from devices used were to be interpreted as inculpatory, in light of the deliberate efforts taken to make those communications disappear. Defendants had, after realizing they were under investigation by the FTC, employed the ephemeral messaging app Signal, encouraged employees to migrate to Signal as well as the secure email app ProtonMail. They also refused to preserve data, withheld data and devices, and when devices were finally turned over, the Signal app had been deleted. Even without the adverse inference instructions, the behavior certainly runs contrary to expected, cooperative behavior in response to a litigation hold.

While the court system does observe holidays, Halloween is not one of them. When it comes to eDiscovery of business messaging apps, the rules are no different than any other electronically stored data – the process is still governed by federal, state, and local court rules and regulations, and upholding professional conduct and services is important. Trickery, while fun to engage in with costumed kids seeking treats, does not go over well in the courtroom. Treat yourself to the fastest, easiest, and most professional eDiscovery services to keep your case on the proper course.

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

UPCOMING INDUSTRY EVENTS

TECHNO SECURITY & DIGITAL FORENSICS CONFERENCE
San Diego, CA: October 25-27, 2021

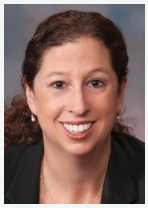
SEDONA CONFERENCE WORKING GROUP 11 MIDYEAR MEETING 2021
Houston, TX: October 28-29, 2021

INTERNET OF THINGS WORLD
Santa Clara, CA: November 2-4, 2021

ISSA SHOW 2021
Las Vegas, NV: November 15-18, 2021

OPENTEXT WORLD 2021
Virtual: November 16-18, 2021

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: