LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com

THURSDAY, MAY 13, 2021

PERSPECTIVE

The disappearing act: using ephemeral social media in litigation

By Daniel Garrie
and Gail Andler

Disappearing and self-destructive messages were a considered a "thing of the future" not too long ago. With technological advancements and the development of new messaging platforms, however, this is now quite a common function. In fact, today ephemeral messaging, a form of communication that lasts a short period of time before disappearing, can be found on various social media platforms. Snapchat, for example, allows users to transmit pictures, videos and messages, for a chosen amount of time (e.g., three seconds), to other users. Once the recipient opens the "snap," it will automatically self-destruct after the chosen amount of time passes. This technology was embraced by pre-teens and teenagers who could prevent snooping parents from reading their messages. In very short order, lawyers turned their attention to how ephemeral messages could be preserved and authenticated for purposes of litigation

While ephemeral messaging applications and platforms such as Snapchat are used for communicating information that someone wishes to preserve to withstand potential questions about their authenticity, it raises challenges. So, when you or client receive a snapchat or other message from a disappearing messaging tool, how do you preserve that message?

Screenshots may seem like the obvious answer, but in reality, how reliable is a screenshot? A quick Google search for "fake a screenshot," will reveal that tutorials and/ or actual screenshot generators abound which allow users to fake text message conversations. On the website "iphonefaketext.com," for example, it is possible to enter various data values, such as contact name, carrier, message content, and even signal strength. Entering enough detail into this type of fake message generator can result in a very convincing faux screenshot of a conversation.

Importantly though, faked screenshots can be detected. Like other malicious mimicry forms, such as phishing emails, faux screenshots are not always detailed with precision to look like an actual conversation. Common errors which may be detected include the date being formatted incorrectly, the carrier's name not being properly capitalized (AT&T as opposed to at&t), text bubbles being the wrong color, the battery icon being placed in the wrong corner of the screen, and so on. In addition, these telltale signs are routinely expanded to include enhanced reviews looking for artifacts such as misspellings, font size and footnote placement. Investigators are constantly on the lookout for these mistakes.

While relying on physical access and visual inspection of screenshots is one path to authentication, it is not the only one. The other option is to take a screenshot of the message and email that very message to your email account. It is important that you preserve both the email and the attached screenshot — do not open either. Because it is less likely that someone would create a fake image and attach it to an email message as a back-up, if you take the screenshot and send the email within a minute or two of capturing the screenshot on the phone (assuming all clocks on all of your devices are in sync), it helps to support the authenticity of the screenshot. In addition, the metadata for the screenshot image for some devices has both a timestamp and additional indicia that indicates the snapshot was taken from a device at a particular time and location. This information, along with the timing of the email, offers substantial circumstantial evidence that the screenshot is what it purports to be.

Consider this scenario: an employee was harassed at work by an intoxicated manager at a company event. After sobering up, the manager feels bad and sends the employee an apology message via Snapchat. The employee uses a screenshot of that apology message in her complaint against the manager. The manager, however, claims that the screenshot is faked, and that the employee likely created it herself. Here, visual inspection could potentially indicate whether or not the screenshot is real or faked, however, if the employee had sent the screenshot to herself in an email to support the timing of the conversation, her argument would be stronger. Looking into the metadata of the screenshot would then further bolster the authenticity of the screenshot.

While screenshots alone can be quite helpful in preserving ephemeral communications, the ease with which such screenshots can be manipulated and faked, requires individuals to carefully consider additional measures to support the authenticity of what is being captured. Immediately sending the screenshot in an email to oneself and analyzing the metadata of the captured image are two options that can help create a much stronger circumstantial argument for any potential challenges that may be brought regarding the authenticity of the image. ■

The authors gratefully acknowledge the contributions of Shradha Patel, an Associate of Law & Forensics LLC, to this article. The content is intended for general informational purposes only and should not be construed as legal advice. If you require legal or professional advice, please contact an attorney.

Daniel B. Garrie *is the co-founder of Law & Forensics, a global forensic, e-discovery and cybersecurity engineering firm. He is also a neutral, discovery referee, arbitrator, technical special master and forensic neutral with JAMS.*

Gail A. Andler joined JAMS as a fulltime neutral after more than 21 years on the Orange County Superior Court where she served from 2007-2017 on the Complex Civil Litigation Panel.