

EPHEMERAL MESSAGING AND THE DUTY TO PRESERVE

Short, often informal messages have become an increasingly prevalent form of business communication. Whether by sending a simple text message or using a communication application like WhatsApp, Slack, or MS Teams, employees conduct more business in less formal ways than ever before. This article will discuss the rise of ephemeral messaging platform use, a case where the technology was misused that resulted in sanctions, and ways in which practitioners can avoid sanctions themselves.

Ephemeral Messaging Explained

Ephemeral (or disappearing) messaging applications enable users to automatically delete messages after they are received. These platforms not only delete messages and related metadata from all devices and servers, but many also apply end-to-end (E2E) encryption to messages sent within them. This means that nobody, *including forensics professionals and the platform itself*, can read these messages besides the sender or recipient.

While there may be substantial business benefits to the use of ephemeral messaging applications, the medium also raises significant e-discovery challenges. Courts have begun to grapple with the discovery implications of ephemeral messaging, as evidenced by a 2019 decision out of the Western District of Arkansas, *Herzig v. Arkansas Foundation for Medical Care, Inc.*

Herzig v. Ark. Found. For Med Care, 2019 WL 287106

Herzig v. Ark. Found. For Med Care was a wrongful termination matter. After making an initial production of text messages, Plaintiffs installed Signal—an E2E encrypted messaging app—on their mobile devices. They configured the app to delete all messages after the recipient reads the message. Plaintiffs made this change after they were well aware of their duty to preserve documents, and only disclosed it to the Court and Defendants toward the end of discovery. The initial production showed that Plaintiffs had numerous communications with one another and with Defendant employees, but only produced some of those messages. Following Defendants' successful motion to compel, Plaintiffs produced several more communications, but, suspiciously, the dates of communications ended the day one of the Plaintiffs downloaded Signal.

Plaintiffs argued that their duty to preserve did not allow Defendants to see all of their communications, only responsive communications, and that the Defendants had not shown that the communications that disappeared were responsive or that their destruction was in bad faith. The Court disagreed, finding that Plaintiffs used Signal to intentionally and in bad faith destroy and withhold ongoing communications about the litigation.

The Court inferred that Plaintiffs were intentionally deleting responsive communications based on, among other reasons, Plaintiffs' reluctance to produce responsive messages during the initial request for production and the manual setting to delete the subsequent Signal messages after they were read. Not helping their argument, both Plaintiffs were information technology professionals who were expected to be aware of the technical capabilities of Signal. As a result, the Court held that both Plaintiffs had the requisite knowledge to produce and retain responsive communications, and that they intentionally used Signal to withhold responsive data in bad faith. While the Court found that the Plaintiffs' conduct was sanctionable, it did not actually issue sanctions, as it dismissed their case on the merits instead.

Three Steps to Avoid Sanctions

Herzig demonstrates that litigants cannot use ephemeral messaging applications to sidestep their duty to preserve responsive communications. The *Herzig* court found that manually configuring these applications to destroy responsive messages while under the duty to preserve was an intentional act of bad faith. With that context in mind, here are three steps practitioners can take to avoid sanctions when ephemeral messages are in scope for discovery:

1. Ephemeral messaging is not an end-around for a litigant's preservation obligations. Attorneys should be aware of the use of ephemeral messaging applications and include language in the litigation hold and preservation memos. Turning off auto-delete functions for email and other systems is standard across IT departments, and should apply to messaging applications as well. As in *Herzig*, a sudden switch from permanent to ephemeral messaging applications, or suddenly switching on the auto-delete function of an ephemeral messaging application, will look suspicious in the event of a discovery dispute.
2. Organizations should utilize ephemeral messaging platforms that allow them to meet their legal obligations. In some instances, an organization may need to ensure that it has the ability to turn the auto-delete functionality

off and on as needed. For example, regulated industries have requirements that pertain to data preservation, retention, and archiving. Understanding these requirements will help you know when ephemeral messaging may be in direct violation of those regulations.

3. As with any other business communication tool, policies and guidelines should be in place to govern the use of ephemeral messaging applications. Asking about your client's policies during your initial investigation and your opponent's policies during pre-trial conferences will help you structure your discovery requests.

Moving Forward

While there are clear business benefits to the use of ephemeral messaging applications, there are also ways they can be misused—either intentionally or otherwise—in a way that can put an organization at odds with its preservation obligations. Attorneys should be aware of this risk and take active steps to ensure that their clients do not use these applications in a sanctionable manner.

By: Stuart Claire, TLS Senior Director and Robert Alarcon, TLS Vice President, Consulting & Information Governance