PLI Chronicle

January 2021

Discovery Considerations When Choosing and Using Virtual Meeting Platforms and Ephemeral Apps

Gail L. Gottehrer

Law Office of Gail Gottehrer LLC

Ronald J. Hedges

Dentons US LLP

Carrie S. Parikh

Horizon Blue Cross Blue Shield of New Jersey

Introduction

New and ever-changing communication technologies create challenges for lawyers. The use of virtual meeting platforms (VMPs) has become standard practice in the legal industry, and they are being used for everything from client meetings to judicial proceedings. In addition, purportedly "disappearing" messaging apps are being used by some attorneys and clients who later learn that the communications did not actually disappear.

While these technologies differ, VMPs and so-called ephemeral messaging apps raise similar issues for attorneys in the context of preservation and discovery, including:

- Whether content of a virtual meeting or an ephemeral message is a "record" and in the possession, custody, or control of a sender or recipient;
- How discovery of content from these communication technologies might be undertaken;
- Whether ephemeral content is actually ephemeral;
- Whether the content is subject to a duty to retain or preserve; and
- What the consequences might be if content is lost.

Definitions

VMPs are "applications and other digital platforms that let you bring people together over the internet. Usually, these apps include a form of video conferencing, as well as tools like chat, reactions and screen sharing. Examples include Zoom, Webex, [and] Google Meet."

Ephemeral messaging apps "are a popular form of communication.… All messages are purposely short-lived, with the message deleting on the receiver's device, the sender's device, and on the system's servers seconds or minutes after the message is read.… [T]hey are now a ubiquitous part of corporate culture."

"Records" and "Possession, Custody, and Control"

It is unlikely that companies are explicitly authorizing the use of ephemeral messaging apps. Nonetheless, we have seen that large portions of the workforce are using them. With the onset of the COVID pandemic and the mass shift to remote work, we have seen a significant (and often company-sanctioned) increase in the use of VMPs and, with that, the creation of video recordings and in-VMP electronic messaging and chatting. Companies need to consider whether these data are business records and, if so, who is ultimately responsible for them.

Not surprisingly, the Federal Rules of Civil Procedure (FRCP) do not define ephemeral communications. Recognizing that technology is constantly changing, the Rules Committee chose not to define "electronically stored information" (ESI). As a result, we must infer the specifics of what constitutes ESI and whether ephemeral communications are encompassed in that definition. FRCP 34(a)(1)(A) provides some

context by requiring a litigant to produce just about anything "stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form." Based on this, one could reasonably argue that ephemeral communications are encompassed in the Rules as they are "created electronically," but questions remain as to whether they are stored and in whose possession, custody or control they reside.

By definition, ephemeral messages are not typically stored. If, however, the messages are stored by a third-party, a determination must be made about who has "possession, custody or control" of them.

A party must consider the extent to which it has the right to obtain the information upon request. ESI is within a party's custody or control not only when the party has actual possession or ownership of the information, but also when the party has "the legal right to obtain the documents on demand." *In re Bankers Trust*, 61 F.3d 465, 469 (6th Cir. 1995), cert. dismissed, 517 US 1205 (1996); *Flagg v. City of Detroit*, 252 F.R.D. 346, 352 (E.D. Mich. 2008) (defendant was obligated to produce texts stored with its third-party service provider because messages were within defendant's control). Based on this case law and interpretation of the FRCP, it could be argued that to the extent an ephemeral communication is stored, even by a third-party, it is in the party's possession, custody and control and, therefore, the party likely has a duty to preserve and produce it.

Discovery of Content from VMPs and Ephemeral Apps

The analysis of whether content from VMPs and ephemeral apps is discoverable follows the analysis for the discovery of other electronically stored information. FRCP 26(b)(1) provides that, generally, a party is entitled to discovery regarding any nonprivileged matter that is relevant to its claim or defense and proportional to the needs of the case. Relevant evidence is defined broadly as evidence that "has any tendency to make a fact more or less probable than it would be without the evidence, and the fact is of consequence in determining the action."

If a party has reason to believe that the content of a virtual meeting, whether it be the recording of the meeting, a transcript of the chat from the meeting, or documents and slides shared during the meeting, is relevant to its claims or defenses in the case, it can request that the content be produced in discovery. Similarly, a party can request the production of the communications sent or received through an ephemeral messaging app if the content is relevant to the case.

Depending on the ephemeral app's settings and features, the sender or the recipient may have retained the content (which could be a message, photo, or video or audio recording) on their device. Even if the app's settings prevent the content from being saved, the sender or the recipient could have taken a screenshot of the content, printed the screenshot, or forwarded or saved the photo or recording, which could be discoverable.

Depending on the VMP or ephemeral app, the platform or app developer may retain a copy of the content of a virtual meeting conducted on its platform or of messages exchanged using its app. If the developer is not a party to the action, and a party asserts that the content is relevant to a claim or defense in a case, it can seek to obtain that content from the developer by subpoena.

Further complicating matters, if an attorney provides legal advice to a client during a virtual meeting or using an ephemeral app, and the developer has access to and retains that content, an argument could be made that the attorney-client privilege has been waived.

Is the Content Actually Ephemeral?

Attorneys must be aware that not all apps that are marketed as ephemeral are actually ephemeral because the implications for discovery can be significant. An example of purportedly ephemeral content not disappearing was the subject of the 2014 settlement between the Federal Trade Commission (FTC) and Snapchat, which resolved alleged misrepresentations Snapchat made to consumers about the "ephemeral" nature of the content sent using the app.

According to the FTC, despite touting its app as giving users the ability to send content that would "disappear forever" after a specified time period, there were several ways that recipients could prevent the content from disappearing, including by using third-party apps to access, view, and save content because the deletion feature only operated in the official Snapchat app. The FTC also alleged that Snapchat misrepresented that the sender would be notified if a recipient took a screenshot of a message when, in fact, there was a simple way for a recipient to get around this feature and take screenshots without the sender being notified.

Duty to Retain or Preserve?

Absent an affirmative duty to preserve, such as a threat of litigation, litigation hold or government investigation, an organization has no general obligation to save or store

its communications. A party cannot be sanctioned for destroying evidence that it has no duty to preserve. *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003). Companies can use technology that assists with the timely destruction of communications. Data destruction must be done responsibly and ideally under the guidance of counsel and subject to a corporate document retention and deletion policy.

Use of ephemeral apps and VMPs, adopted subject to a defensible data retention and destruction policy, can be a key solution for data minimization. It can reduce data storage costs, create a more information-secure way of communicating (reducing potential data breaches) and ultimately reduce discovery costs. However, neither technology is, or should be seen as, a mechanism for avoiding discovery obligations, and companies should be cautious about using ephemeral messaging apps once they reasonably anticipate litigation.

What If Content is Lost?

While there is no case law addressing the loss of VMP content, there are three federal court decisions that deal with the loss of ephemeral messages: *Waymo LLC v. Uber Technologies, LLC*, No. C 17-00939 (N.D. Cal. 2018), *Herzig v. Arkansas Foundation for Medical Care, Inc.,* No. 18-CV-02101 (W.D. Ark. 2019), and *WeRide Corp. v. Huang*, No. 18-cv-07233 (N.D. Cal. 2020).

In *Waymo*, an action for alleged trade secret misappropriation, the court undertook an analysis under Fed. R. Civ. P. 37(e) and held that the corporate defendants' use of ephemeral messaging could be presented to the jury. *Waymo* settled before trial. The case is instructive in its analysis of Rule 37(e) and the steps that a court must take, and parties must address, before imposing sanctions for the loss of content from VMPs or ephemeral apps under that rule.

In *Herzig,* the court found that the plaintiffs installed and used a "communication application designed to disguise and destroy communications" and that they had engaged in intentional bad-faith spoliation. The court did not refer to Rule 37(e). Rather than sanction plaintiffs for the loss of the messages, the court granted summary judgment in defendant's favor on the merits. (Whether the messages at issue in *Herzig* were "ephemeral" at all can be debated.). *Herzig* is of little or no value when a court must engage in a spoliation analysis under Rule 37(e), although it might be helpful in analyzing alleged spoliation under the common law.

In *Huang*, terminating sanctions were imposed against the defendant corporation and two individual defendants pursuant to Fed. R. Civ. P. 37(b) and Rule 37(e) for what the court characterized as "staggering" spoliation of electronic information. As an

example of that intentional misconduct and spoliation, the court pointed to the corporation's decision to switch its internal communications to an ephemeral messaging app at the direction of one of the individual defendants, after the duty to preserve arose. *Huang* is of uncertain assistance for applying Rule 37(e) because it finds, without any analysis, that switching to ephemeral messaging constitutes spoliation and because the decision to make that switch was just one of several acts that led to a finding of intent.

Conclusion

The ubiquity of VMPs and "ephemeral" apps, and the potential for content shared through them to be discoverable, highlight the importance of attorneys educating themselves about these technologies as part of their ethical duty of technological competence.

For more information about the legal implications of ephemeral messages, virtual meeting platforms and related technologies, check out Gail, Ronald and Carrie's Preservation and Discovery of Virtual Meeting Data and Ephemeral Communications **program, available from PLI Programs On Demand.**

Also available from PLI Programs On Demand:

Reasonable Cybersecurity Standards 2020: What Might These Be and How Best to Achieve Them

Defining "Reasonable" Data Security Requirements in a Rapidly Changing World

May It Please the Court: New Technologies on Trial – Part 2

Also available from PLI Press:

Internet of Things and the Law

Cybersecurity: A Practical Guide to the Law of Cyber Risk

Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age (Second Edition)

Disclaimer: The viewpoints expressed by the authors are their own and do not necessarily reflect the opinions, viewpoints and official policies of Practising Law Institute.

To submit an article for consideration, please contact the editor at: editor.plichronicle@pli.edu