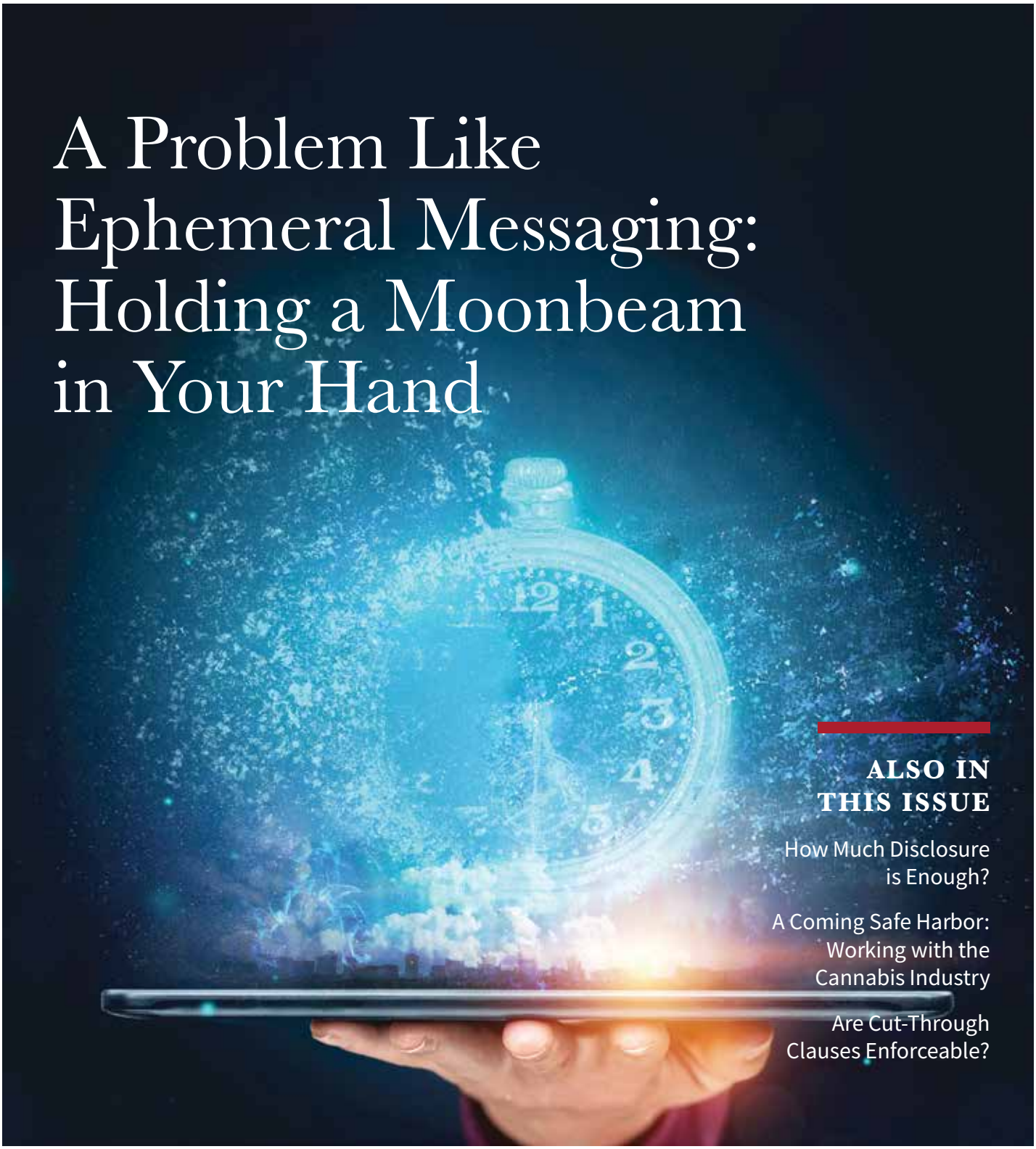
ARIAS U.S.

QUARTERLY

A Problem Like Ephemeral Messaging: Holding a Moonbeam in Your Hand



ALSO IN THIS ISSUE

Q2 • 2021

A Problem Like Ephemeral Messaging: Holding a Moonbeam in Your Hand

By Kirsten Fraser and Andrew Foreman

Even if you think you've never heard of ephemeral messaging, you've probably heard of ephemeral messaging. While the term itself may not be well known, it's likely you know of at least one ephemeral messaging app, especially if you know anyone under the age of 25: Snapchat. Nearly half of U.S. internet users under age 25 use Snapchat [1], and hundreds of millions of users worldwide send ephemeral messages through the Snapchat app daily [2].

Ephemeral messages, sometimes called self-destructing messages, are essentially text messages that disappear after a fixed period of time. Snapchat is not alone in the ephemeral messaging space—there's also Wickr, Confide, and CoverMe, while Signal, Telegram, WeChat, WhatsApp, Facebook Messenger, and Instagram offer ephemeral messaging as an option. And in case you might have thought of Snapchat (and, by proxy, ephemeral messaging) as just a way for teenagers to communicate, think again. Wickr describes its target audience as military installations, government agencies, private enterprise, and individuals [3], and Confide was created to be the Snapchat for professionals [4]. More and more, individuals and businesses are turning to ephemeral messaging as a secure means of communicating.

While there are legitimate business uses for ephemeral messaging, its use

can also raise questions and present challenges within the context of litigation or arbitration. In this article, we aim to explain in broad terms the nature of ephemeral messaging, identify some of the challenges ephemeral messaging raises in relation to document preservation and discovery, describe some recent cases involving ephemeral messaging, and provide suggestions and ideas for litigants and arbitrators alike to consider.

Ephemeral Messaging Basics

Ephemeral messaging apps (aka disappearing messaging apps) allow users to share content that is automatically deleted immediately after it's viewed or within a defined period of time after receipt. The length of time a message will remain visible can usually be controlled by the sender. Messages can contain text, images, or videos, depending on the platform, and they are generally end-to-end encrypted and stored on your personal device. Often there is screenshot protection to prevent the recipient from bypassing the self-destruct feature. Ephemeral messages thus function much like oral communications—once the conversation has ended, the communications live on only in the memories of the participants.

The business case for ephemeral messaging can be robust, depending on the needs of an organization. The benefits can include saving on data storage, protecting trade secrets, protecting against data breaches, controlling e-discovery costs, and maintaining privacy. If confidential communications no longer exist, there is no risk of their inadvertent (or intentional) disclosure. By the same token, ephemeral messaging may be a useful tool for arbitration panel members to confer with one another candidly when a call, video conference, or other oral communication isn't feasible, without the risk of disclosure or breach of the confidentiality requirements that usually accompany arbitration.

> "While there are legitimate business uses for ephemeral messaging, its use can also raise questions and present challenges within the context of litigation or arbitration."

Litigation and Arbitration Challenges

While there are legitimate reasons for using ephemeral messaging, it can also create challenges. For example, it may complicate corporate compliance obligations by circumventing regulatory retention requirements, violating the duty to preserve, and violating corporate information governance programs. And even if ephemeral messaging is used only for non-nefarious reasons, it can give the appearance of impropriety.

For example, the U.S. Department of Justice views ephemeral messaging apps with a suspicious eye. Indeed, in the 2017 version of its Foreign Corrupt Practices Act (FCPA) Enforcement Policy, the DOJ took aim at ephemeral messaging apps, requiring companies to prohibit employees from "using software that generates but does not appropriately retain business records or communication" as a remediation measure to receive full cooperation credit in connection with voluntarily self-disclosed misconduct [5]. In 2019, the DOJ refined its policy to loosen the outright prohibition on ephemeral messaging apps—it now requires that companies implement "appropriate guidelines and controls on the use of personal communications and ephemeral messaging platforms" as remediation [6]. However, the DOJ remains skeptical of ephemeral messaging apps, noting they "undermine the

> “As you might imagine, the disappearing nature of ephemeral messages can cause problems when it comes to these duties and obligations, and courts and litigants are just starting to wade into these issues.”

company’s ability to appropriately retain business records” [7].

The U.S. Securities and Exchange Commission (SEC) likewise is mistrustful of ephemeral messaging apps. In a 2018 National Exam Program Risk Alert, the SEC advised registered broker-dealers and investment advisers that they should specifically prohibit “business use of apps and other technologies that can be readily misused by allowing an employee to send messages or otherwise communicate anonymously, allowing for automatic destruction of messages, or prohibiting third-party viewing or back up” to comply with the SEC’s books and records rule [8].

Turning to civil litigation, parties also have a duty to preserve evidence where litigation is reasonably anticipated or ongoing—or, as the Federal Rules of Civil Procedure put it, “... potential litigants have a duty to preserve relevant information when litigation is reasonably foreseeable” [9]. This duty requires parties to retain documents, suspend destruction, and put in place litigation holds, and it includes electronically stored information (ESI), such as text messages. Failure to preserve ESI can lead to sanctions under Rule 37(e), as seen in certain of the cases discussed below, although the rule “does not apply when information is lost before a duty to preserve arises” [10].

While arbitral discovery is usually less onerous than discovery in civil litigation, the same preservation and spoliation issues may nevertheless appear in arbitration, and the litigation rules regarding preservation provide guidance for an arbitration panel addressing these issues. Although the scope of discovery in arbitration is often more limited than in litigation, sanctions for spoliation of evidence likely come within the arbitrators’ authority.

In discovery under the Federal Rules, ESI must be produced in a form “in which it is ordinarily maintained or in a reasonably usable form” [11]. That said, “[a] party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost” [12].

As you might imagine, the disappearing nature of ephemeral messages can cause problems when it comes to these duties and obligations, and courts and litigants are just starting to wade into these issues. For example, does the “duty to preserve relevant information” require a company to change the functioning of an ephemeral messaging app to preserve (rather than delete) messages going forward? Developing case law says yes. Are ephemeral messages “reasonably accessible” if it is possible to retrieve them through extraordinary means, since not everything deleted electronically is unrecoverable? More and more parties are turning to stipulated ESI orders to set the boundaries, defining what is and is not “reasonably accessible.” And if messages haven’t yet been deleted, is there an obligation to intervene and prevent their deletion or turn them over in discovery? Probably.

At one point, Snapchat revealed that over a six-month period it had produced unopened messages to law enforcement in response to about a dozen search warrants [13]. The messages had not self-destructed because they had not been opened. These issues are not isolated to the courts: arbitrators

may soon find themselves in a similar position, being asked to issue discovery orders, draw adverse inferences, and apply sanctions in connection with ephemeral data.

Recent Cases Involving Ephemeral Messaging

In three cases over the past few years, ephemeral messaging has played a central role in the dispute. In each case, ephemeral messaging proved problematic (or at least potentially so).

In *Waymo LLC v. Uber Technologies, Inc.*, Waymo claimed that Uber misappropriated its trade secrets [14]. The litigation was beset by discovery disputes. Waymo filed motions, motions in limine, and multiple requests for relief for Uber's alleged discovery misconduct [15]. In a comprehensive discovery order prior to trial, the court ruled on the extent to which Uber's litigation misconduct might feature at trial. The court allowed Waymo to argue that Uber's use of ephemeral messaging was to purposefully conceal evidence that it had stolen trade secrets, while also allowing Uber to argue that its ephemeral messaging use was legitimate [16]. There was no final resolution of the issue, as the case settled before trial.

After litigation began in *Herzig v. Arkansas Foundation for Medical Care, Inc.*, the plaintiffs installed Signal on their phones, with the app set to delete messages [17]. One of the plaintiffs disclosed that they were messaging over Signal at his deposition [18]. The court inferred that the messages sent over Signal would have been responsive and held that the plaintiffs' installation and use of Signal represented an intentional act "to withhold and destroy discoverable evidence" [19]. While the court held that "[t]his intentional, bad-faith spoliation of evidence was an abuse of the judicial process and warrant[ed] a sanction," the court declined to determine the appropriate severity of the sanction, as it dismissed the case on merits in summary judgment [20].

In *WeRide Corp. v. Kun Huang*, after the start of litigation, the defendant CEO instructed his company to use DingTalk to correspond internally [21]. A company 30(b)(6) witness confirmed the company was unable to recover any DingTalk ephemeral messages, although the CEO said he had stored some messages but could not find a vendor to extract them [22]. The plaintiff moved the court to issue sanctions against the defendants for spoliation of evidence.

In deciding whether to impose sanctions under Rule 37(e) for spoliation of ESI, the court explained that it should consider whether "(1) the ESI should have been preserved in the anticipation or conduct of litigation; (2) the ESI is lost because a party failed to take reasonable steps to preserve it; and (3) [the ESI] cannot be restored or replaced through additional discovery" [23]. "Before terminating the action, the Court must find that 'the party acted with the intent to deprive another party of the information's use in the litigation'" [24].

The defendants continued to delete emails older than 90 days, deleted entire email accounts, wiped laptops, and began using DingTalk. Taking all of this conduct together, the court found it appropriate to issue terminating sanctions under Rule 37(b) and (e) [25].

> "At one point, Snapchat revealed that over a six-month period it had produced unopened messages to law enforcement in response to about a dozen search warrants."

What Does This Mean for You?

Based on the issues presented in *Waymo*, *Herzig*, and *WeRide*, arbitrators and parties need to be proactive about addressing issues related to ephemeral messaging. The case law suggests that decisions about the use of ephemeral messaging should be based on specific business justifications and not made "on the fly" (and especially not once there is already a duty to preserve evidence). As with other types of ESI, when litigation or arbitration is reasonably anticipated, parties should take steps to preserve any ephemeral messages that still exist and disable automatic deletion of messages. Once litigation or arbitration begins, parties may need to determine whether responsive ephemeral messages exist, discuss with each other the role of ephemeral messaging in discovery, and negotiate whether ephemeral messages should be part of the discovery plan.

Where ephemeral messaging is in play, arbitrators should understand how the ephemeral messaging apps used by the parties function, including whether automatic deletion can be disabled and whether use of the app can be avoided entirely. Arbitrators should also understand the implications of a party's decision to use ephemeral messaging—did the party start using ephemeral messaging before arbitration was reasonably anticipated for one of the legitimate business reasons described above, or is the situation more like *WeRide*, where the CEO's instruction to use ephemeral messaging came after the start of litigation? Finally, arbitrators should be prepared to craft discovery orders and relief, such as sanctions or adverse inferences, if evidence that could have been preserved is deleted.

With a greater understanding of the function and legitimate use of ephemeral messaging as well as the questions and challenges it can present in the context of litigation or arbitration, parties and arbitrators should be well positioned to handle any ephemeral messaging issues that may arise.

NOTES

1. Statista. 2021. Percentage of U.S. internet users who use Snapchat as of 3rd quarter 2020, by age group. Accessed at https://www.statista.com/statistics/814300/snapchat-users-in-the-united-states-by-age/.

2. Statista. 2021. Number of daily active Snapchat users from 1st quarter 2014 to 4th quarter 2020. Accessed at https://www.statista.com/statistics/545967/snapchat-app-dau/.

3. Wickr. 2021. Who is Wickr for? Accessed at https://wickr.com/.

4. Carr, Austin. 2014. Confide: A Snapchat for Professionals, Not Sext-Obsessed Teens. *Fast Company.* Accessed at https://www.fastcompany.com/3024603/confide-a-snapchat-for-professionals-not-sex-obsessed-teens.

5. Davis Polk & Wardwell LLP. 2018. USAM Insert: 9-47.120 – FCPA Corporate Enforcement Policy. Accessed at https://www.davispolk.com/sites/default/files/doj_policies_2018.pdf.

6. U.S. Department of Justice. 2020. Foreign Corrupt Practices Act of 1977: 9.47.120 – FCPA Corporate Enforcement Policy. Accessed at https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977#9-47.120.

7. *Id.*

8. U.S. Securities and Exchange Commission. 2018. National Exam Program Risk Alert. Office of Compliance Inspection and Examinations. Accessed at https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Electronic%20Messaging.pdf.

9. Fed. R. Civ. P. 37(e), Comm. Notes.

10. Fed. R. Civ. P. 37(e), Comm. Notes.

11. Fed. R. Civ. P. 34(2)(E)(ii).

12. Fed. R. Civ. P. 26(b)(2)(B) (emphasis added).

13. "Who Can View My Snaps and Stories." 2013. Snap. Accessed at https://newsroom.snap.com/viewing-snaps-stories

14. 2018 U.S. Dist. LEXIS 16020 (N.D. Cal. 2018).

15. *Id.* at *13–14.

16. *Id.* at *69–70.

17. 2019 U.S. Dist. LEXIS 111296 (W.D. Ark. 2019).

18. *Id.* at *12–13.

19. *Id.* at *13.

20. *Id.* at *15.

21. 2020 U.S. Dist. LEXIS 72738, at *29 (N.D. Cal. 2020),

22. *Id.*

23. *Id.* at *31–32 (internal quotation marks omitted).

24. *Id.* at *32.

25. *Id.*

Kirsten Fraser is a senior associate at Porter Wright Morris & Arthur LLP who focuses her practice on commercial litigation and internal investigations.

Andy Foreman, a partner at Porter Wright Morris & Arthur LLP, concentrates his practice on complex commercial litigation and reinsurance disputes.