The Next Frontier of Electronic Discovery: A Primer on Litigation Issues Relating to New Digital Messaging Systems

Beth Newton*

I. Introduction

In the 1990s and early 2000s, the widespread adoption of email as a form of business communication changed the landscape of litigation discovery. As one commentator wrote in 2002:

> In the past ten years, electronic mail (e-mail) has significantly altered how we communicate with each other in the industrialized world. Attracted by its relatively low cost, speed, and ease of use, individuals and businesses have turned to e-mail to replace or supplement traditional communication tools such as the written letter or the telephone. As a result, legislatures and courts have been forced to examine whether existing legal structures are sufficiently flexible to resolve issues that are either not present in other communications tools or present but to a different degree. . . . The e-mail revolution also had a profound effect in the area of civil discovery.[1]

That "profound effect" manifested itself in many ways. The burden of document collection and production increased by orders of magnitude given the sheer volume of

* Ms. Newton is a partner in the New York office of Sullivan & Cromwell LLP. Her practice focuses on complex commercial litigation, regulatory and enforcement matters, and internal investigations.

[1] Michael Marron, *Discoverability of "Deleted" E-Mail: Time for A Closer Examination*, 25 SEATTLE U. L. REV. 895, 895–96 (2002) (footnotes omitted).

email produced by litigants. In light of the new links between discovery and technology, parties began to retain specialized e-discovery vendors and negotiate e-discovery protocols in litigation. And litigants faced new issues regarding document preservation, privacy, and confidentiality.

Over the past several years, another shift in electronic communication has been underway as new digital messaging systems like Slack, Signal, and WhatsApp (among others) have become increasingly popular, including for business purposes. Communication on these systems (collectively, "New Digital Messaging Systems") typically takes the form of chats or text messages and is accompanied by customizable settings affecting privacy and message retention, such as auto-deletion, advanced encryption, and cross-platform integration capability. New Digital Messaging Systems now supplement—and in some instances compete with—email as modes of workplace communication.[2] Further, especially given the rise in remote work as a result of the COVID-19 pandemic, employees increasingly use these systems to conduct business activities on personal rather than company-issued devices.[3]

New Digital Messaging Systems may offer significant benefits to corporate users, including enhanced privacy and data security and facilitation of collaborative, efficient communication among employees. As New Digital Messaging Systems have become

[2] Todd Bishop, *Salesforce's $27.7B Slack deal combines two Amazon allies, creates big new rival for Microsoft*, GEEKWIRE (Dec. 1, 2020, 1:55 PM), https://www.geekwire.com/2020/salesforces-27-7b-slack-deal-combines-two-amazon-allies-creates-big-new-rival-microsoft/ (reporting analyst commentary that the acquisition of messaging application Slack by cloud computing company Salesforce "promise[s] to create a formidable new competitor for Microsoft in enterprise technology").

[3] Deyan G., *43+ Stunning BYOD Stats and Facts to Know in 2022*, TECHJURY (Mar. 14, 2022), https://techjury.net/blog/byod-stats/ (reporting that "78.48% of organizations in the US had BYOD ["Bring-Your-Own-Device"] activities since 2018" and that "COVID-19 has catapulted BYOD into a regular work mode in most firms in 2021").

more popular, they have also begun to pose issues of first impression in connection with electronic discovery. "[L]egislatures and courts" now again need to "examine whether existing legal structures"—which are based on the email paradigm—"are sufficiently flexible to resolve" those issues.[4]

This article explores four categories of questions that have arisen relating to companies' use of New Digital Messaging Systems:

- **Use**: How should companies decide whether to adopt New Digital Messaging Systems in addition to (or instead of) email, and how should they select particular systems? Section III below identifies potential considerations that may be useful in answering those questions.

- **Preservation**: To what extent do New Digital Messaging Systems pose issues concerning document retention and preservation? Section IV below discusses issues that have arisen regarding (i) "ephemeral" messaging systems, which feature auto-deletion of messages, and (ii) employees' use of personal devices to conduct business communications.

- **Collection and production**: How will use of New Digital Messaging Systems affect document collection and production? Section V below explores issues that may arise concerning collection sources, isolation of relevant communications, and related burden considerations.

- **Privilege and confidentiality**: Do New Digital Messaging Systems pose unique issues regarding assertions of attorney–client privilege or the protection of confidential

[4] *See* Marron, *supra* note 1, at 895.

information? Section VI below addresses issues that may arise in this regard with respect to chat-based messaging platforms.

It remains to be seen how significantly the e-discovery landscape will shift as a result of New Digital Messaging Systems, but meaningful change appears inevitable—and, indeed, is already underway. The areas of focus outlined below may be useful to companies as they navigate the impending changes.

II. Overview of New Digital Messaging Systems

Dozens of New Digital Messaging Systems, if not more, have been created over the past several years, and this article does not attempt to explore each of them. Instead, we focus on a (likely non-exhaustive) subset of systems that are widely used and have features relevant to e-discovery issues of first impression. In particular, this article addresses the following New Digital Messaging Systems:

- **Signal**. Signal is a "privacy-focused messaging and voice talk app" accessible on mobile devices and desktop computers.[5] Signal markets its application as providing heightened privacy and security settings, including encryption of message content and optional auto-deletion of messages.[6] In addition, Signal "collects virtually no data on its users" beyond a phone number.[7]

- **Slack**. Slack is a messaging application "meant for teams and workplaces [that] can be used across multiple devices and platforms."[8] Slack allows users to send messages

[5] Rachel Kraus, *What is Signal? The basics of the most secure messaging app.*, MASHABLE (July 16, 2021), https://mashable.com/article/what-is-signal-app.
[6] *Id.*
[7] *Id.*
[8] Maggie Tillman, *What is Slack and how does it work? Plus plenty of Slack tips and tricks*, POCKET-LINT (Apr. 7, 2021), https://www.pocket-lint.com/apps/news/150925-what-is-slack-and-how-does-it-work-tips-tricks.

through "channels" organized within broader "workspaces."[9] In addition to instant messaging functionality, Slack provides "integrated file sharing, video and phone calls, and screen sharing directly through its platform, and the ability to invite others from outside your organization to collaborate."[10] According to the company's statistics, more than ten million people use Slack daily, and the platform is employed by more than 600,000 organizations.[11] In 2021, Slack was acquired by cloud computing company Salesforce, resulting in the incorporation of Slack's messaging system into Salesforce's "suite of enterprise software."[12] Commentators opined that following the combination, Slack would become "a consolidated competitor on even footing" with Microsoft in the market for workplace communication systems.[13]

- **Snapchat**. Snapchat is a "messaging app that lets users exchange pictures and videos (called snaps) that are meant to disappear after they're viewed."[14] The default setting on Snapchat causes messages to be deleted automatically (i) once they have been viewed by all recipients or (ii) once the applicable expiration period has passed (thirty

[9] *Id.*
[10] Sarah Wyland, *What is Slack and Why You Should Use It*, DROPLR (Feb. 6, 2020), https://droplr.com/how-to/productivity-tools/what-is-slack-and-why-you-should-use-it/.
[11] Jacquelyn Bulao, *21 Impressive Slack Statistics You Must Know About in 2022*, TECHJURY (Feb. 6, 2022), https://techjury.net/blog/slack-statistics/#gref.
[12] Richard Lawler, *Now Salesforce officially owns Slack*, THE VERGE (July 21, 2021, 6:30 PM), https://www.theverge.com/2021/7/21/22587666/slack-acquisition-salesforce-closed-messaging-cloud. In connection with the acquisition, Sullivan & Cromwell LLP represented Goldman Sachs as financial adviser to Slack. *S&C Advises Goldman Sachs as Financial Adviser to Slack in $27.7 Billion Acquisition by Salesforce*, SULLIVAN & CROMWELL LLP (Dec. 22, 2020), https://www.sullcrom.com/client-highlight-sandc-advises-goldman-sachs-as-financial-adviser-to-slack-277-billion-acquisition-by-salesforce.
[13] Lawler, *supra* note 12.
[14] Christine Elgersma, *Everything you need to know about Snapchat*, PHYS.ORG (June 18, 2018), https://phys.org/news/2018-06-snapchat.html.

days for most messages and twenty-four hours for messages sent to "Group Chats").[15] Snapchat currently estimates that it has more than 293 million daily active users worldwide.[16]

- **Vaporstream**. Vaporstream is "an enterprise communication platform that enables private business conversations."[17] The company states that its "advanced content controls protect [users'] information from being uploaded to the cloud, stored on devices, saved on servers or shared with unintended recipients."[18] Vaporstream features automatic message deletion but also offers a "Governance Module" that allows enterprises to "archive messages, in a secure on premise store . . . while leaving nothing on the [employees'] devices."[19]

- **WhatsApp**. WhatsApp is a messaging service that can be used for text messaging; voice and video calls; voice messaging; and document, photo, and video sharing. The platform also provides secure messaging using end-to-end encryption.[20] Ranked as the

[15] *When does Snapchat delete Snaps and Chats?*, SNAPCHAT, https://support.snapchat.com/en-US/article/when-are-snaps-chats-deleted (last visited Mar. 4, 2022).
[16] Brian Dean, *Snapchat Demographic Stats: How Many People Use Snapchat in 2022?*, BACKLINKO (Jan. 5, 2022), https://backlinko.com/snapchat-users.
[17] *How It Works*, VAPORSTREAM, https://www.vaporstream.com/how-it-works/ (last visited Mar. 4, 2022).
[18] *Privacy and Security First*, VAPORSTREAM, https://www.vaporstream.com/security/ (last visited Mar. 4, 2022).
[19] Mike Koclanes, *Ephemeral Messaging Protects Privacy in a BYOD Environment*, VAPORSTREAM (Nov. 4, 2015), https://www.vaporstream.com/blog/ephemeral-messaging-protects-privacy-in-a-byod-environment/.
[20] Grace Eliza Goodwin, *What is WhatsApp? A guide to navigating the free internet-based communication platform*, BUSINESS INSIDER (Nov. 3, 2020, 8:06 AM), https://www.businessinsider.com/what-is-whatsapp-guide?op=1.

most used mobile messaging application in the world, WhatsApp currently has more than two billion active users worldwide.[21]

- **Wickr**. Wickr is a messaging application that offers "secure, end-to-end encrypted, communication technology" with "advanced security features."[22] The platform's services include "messaging, voice and video calling, file sharing, and collaboration."[23] Wickr is used by both private companies and government agencies and has marketed its services as compliant with the security criteria prescribed by the National Security Agency.[24] In June 2021, Wickr was acquired by Amazon Web Services (Amazon's cloud services platform).[25]

III. Use

A company's digital communication framework starts with the considered selection of business communication systems and the creation of policies and procedures to govern employees' use of those systems. This decision-making process was relatively simple when email was the principal form of workplace electronic communication. In light of the proliferation of new technologies over the past several years—many of which have customizable privacy, security, and preservation settings—the calculus facing companies has become more complex. Although this calculus will be unique to each organization, some broadly applicable considerations that should inform the decision-making process include the following:

---

[21] Brian Dean, *WhatsApp 2022 User Statistics: How Many People Use WhatsApp?*, BACKLINKO (Jan. 5, 2022), https://backlinko.com/whatsapp-users.
[22] Steve Schmidt, *AWS welcomes Wickr to the team*, AWS SECURITY BLOG (June 25, 2021), https://aws.amazon.com/blogs/security/aws-welcomes-wickr-to-the-team/.
[23] *Id.*
[24] Annie Palmer, *Amazon acquires secure chat app used by government agencies*, CNBC (June 25, 2021, 11:47 AM), https://www.cnbc.com/2021/06/25/amazon-acquires-wickr-secure-messaging-app-used-by-government-agencies.html.
[25] *Id.*

- **The company's business needs**. For example, in what circumstances does the company seek to optimize collaborative communication across teams or departments? Are there other contexts in which privacy is the chief concern? Do some or all communications contain proprietary data or other particularly sensitive information? In what circumstances and how often do employees need to interact with third parties? Which platforms do critical third parties employ for digital communication purposes?

- **Compliance and regulatory considerations**. Can the systems a company seeks to use be effectively monitored to detect any unauthorized communications within those systems? Are the systems a company is considering compatible with its document-retention obligations, including both regular-course obligations and any obligations arising in connection with legal proceedings? Does the company train its employees regarding the appropriate use of electronic communication systems in order to minimize excessive or overly informal messaging among employees?[26]

- **Technology considerations**. Are a company's systems compatible with its information technology infrastructure, such as company-issued mobile and desktop devices, storage solutions, and document management systems?

Given the rapidly changing frontier of digital communication, companies may need to revisit these and other pertinent questions periodically in order to keep their systems, policies, and processes up to date.

[26] *See*, *e.g.*, Oracle Am., Inc. v. United States, 144 Fed. Cl. 88, 107 n.10 (2019), *aff'd*, 975 F.3d 1279 (Fed. Cir. 2020) (describing review of digital chats as "a cautionary tale about ill-considered use of instant messaging").

IV. Preservation

Adoption of New Digital Messaging Systems also raises issues concerning document retention and preservation. In particular, courts, commentators, and regulators have begun to consider whether ephemeral messaging systems like Signal, Wickr, Vaporstream, and Snapchat are compatible with users' document-retention obligations. Although guidelines regarding the use of ephemeral messaging are beginning to come into focus, there remains substantial uncertainty on this issue. Ongoing monitoring of case law and regulatory guidance is advisable as the landscape continues to develop.

Another issue garnering increased attention—especially from federal regulators—is employees' use of personal devices and unapproved messaging channels to conduct business communications. As an ongoing regulatory probe of the financial services industry has shown, government agencies are increasingly focused on whether such use has compromised regulated entities' compliance with document-preservation obligations. Employers face a significant challenge in their efforts to monitor employees' use of personal devices and ensure that business communications sent or received from such devices are retained and available for collection as needed.

Each of these issues is addressed below.

A. Ephemeral Messaging

1. Applicable Legal Standards

Obligations to retain electronic communications can arise from various sources, either in the regular course of business or in connection with pending or anticipated legal proceedings. For example, Securities and Exchange Commission (SEC) regulations require certain broker-dealers to retain (among other things) all communications "relating to [their] business as such" for three years.[27] That obligation applies to covered

[27] 17 C.F.R. § 240.17a-4(b)(4).

entities regardless of the subject matter of a particular communication or the presence or absence of anticipated litigation.

In the context of litigation, "[t]he obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation."[28] This duty has been held to attach "at the time that litigation [i]s reasonably anticipated," and it obligates the party not to "destroy unique, relevant evidence that might be useful to an adversary."[29] As one court has explained:

> While a litigant is under no duty to keep or retain every document in its possession . . . it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request.[30]

Failure to comply with those parameters may result in the imposition of sanctions. In federal court, "[i]f electronically stored information that should have been preserved in the anticipation or conduct of litigation is lost because a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional dis-

[28] Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 216 (S.D.N.Y. 2003) (quoting Fujitsu Ltd. v. Federal Express Corp., 247 F.3d 423, 436 (2d Cir. 2001)).
[29] *Id.* at 217.
[30] *Id.* (quoting Turner v. Hudson Transit Lines, Inc., 142 F.R.D. 68, 72 (S.D.N.Y. 1991)).

covery, the court" may impose sanctions to redress any resulting prejudice to the opposing party.[31] In cases of intentional destruction, such sanctions may be as severe as an adverse inference instruction or entry of a default judgment.[32]

2. Preservation in the Litigation Context

a. Pre-Ephemeral Messaging Case Law

Before the advent of ephemeral messaging, courts rarely needed to apply these preservation standards to self-deleting digital information. In the infrequent instances in which the issue arose, courts tended to hold that such data need not be preserved unless it had a "semi-permanent existence" and was the subject of a pending discovery request. For example, in *Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey*,[33] the court rejected a request for spoliation-based sanctions resulting from a party's failure to preserve temporary cache files that were automatically deleted in the regular course of business. Similarly, in *Convolve, Inc. v. Compaq Computer Corp.*,[34] the court held that failure to preserve digital "wave form" data—images representing audible or electronic signals—did not constitute sanctionable spoliation because the data was "ephemeral" and "exist[ed] only until [a] tuning engineer makes the next adjustment."[35] The court explained that "[n]o business purpose ever dictated that [the data] be retained, even briefly"; that preservation "would have required heroic efforts far beyond those consistent with [the party's] regular course of business"; and that the party was not subject to a preservation order regarding the data.[36]

---

[31] FED. R. CIV. P. 37(e).
[32] *Id.*
[33] Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey, 497 F. Supp. 2d 627 (E.D. Pa. 2007).
[34] Convolve, Inc. v. Compaq Computer Corp., 223 F.R.D. 162 (S.D.N.Y. 2004).
[35] *Id.* at 177.
[36] *Id.* at 176–77.

By contrast, in *Arista Records v. Usenet.com, Inc.*,[37] the court sanctioned defendant Usenet for bad-faith destruction of digital data consisting largely of records of user activity on a network of computer servers operated by Usenet. That data, although transitory, typically remained on Usenet's system for a period of approximately ninety days.[38] The court found that after receiving discovery requests seeking the data, defendants "took affirmative steps" to reduce the standard retention period, leading to permanent deletion of the data and precluding plaintiffs from accessing it.[39]

Under this line of authority, although courts hesitated to penalize destruction of ephemeral data absent a pending discovery request and evidence of bad faith, they also made clear that regular-course automatic deletion of potentially relevant electronic communications could violate a preservation obligation in some contexts. As the *Convolve* court held:

> [I]n the world of electronic data, the preservation obligation is not limited simply to avoiding affirmative acts of destruction. Since computer systems generally have automatic deletion features that periodically purge electronic documents such as e-mail, it is necessary for a party facing litigation to take active steps to halt that process.[40]

The court explained that, unlike the ephemeral wave form data that need not be preserved, "e-mails . . . normally have some semi-permanent existence. They are transmitted to others, stored in files, and are recoverable as active data until deleted, either deliberately or as a consequence of automatic purging."[41]

---

[37] Arista Records L.L.C. v. Usenet.com, Inc., 608 F. Supp. 2d 409 (S.D.N.Y. 2009).
[38] *Id.* at 433.
[39] *Id.* at 436, 439.
[40] *Convolve*, 223 F.R.D. at 175–76.
[41] *Id.* at 177.

Similarly, the Advisory Committee note accompanying the 2006 amendment to Federal Rule of Civil Procedure 37(f) states that:

> [A] party is not permitted to exploit the routine operation of an information system to thwart discovery obligations by allowing that operation to continue in order to destroy specific stored information that it is required to preserve. When a party is under a duty to preserve information because of pending or reasonably anticipated litigation, intervention in the routine operation of an information system is one aspect of what is often called a "litigation hold."[42]

b. Case Law Regarding Ephemeral Messaging Systems

The authority described above appears to permit regular-course destruction of "transitory" data while also requiring intervention in automatic deletion processes in some circumstances. Those rules do not map cleanly onto ephemeral messaging systems like Signal, Snapchat, Vaporstream, and Wickr, which are specifically designed to destroy communications within seconds, hours, or days of their transmission. As courts have begun to consider preservation questions concerning these systems, they nonetheless appear to have continued applying existing rules rather than developing a new framework. Although this authority remains limited, several noteworthy trends have emerged to date.

Spoliation based on transition to auto-deletion while under a preservation obligation. Recent decisions reflect that a party may engage in unlawful spoliation if it transitions to using ephemeral messaging to conduct relevant business communications after a preservation obligation arises. Such a finding is more likely if the court

[42] FED. R. CIV. P. 37 advisory committee's note to 2006 amendment.

determines that the party acted in bad faith. For example, in *FTC v. Noland*,[43] the court held that the defendants engaged in intentional spoliation of evidence when, after learning of an FTC investigation into their business, they abruptly ceased using their existing electronic communication platform and began using Signal and ProtonMail accounts to send encrypted, auto-deleting communications regarding business matters.[44] After the FTC obtained an order requiring the defendants to produce relevant electronic communications, the defendants deleted the Signal application from their mobile devices "in coordinated fashion" and failed to disclose the Signal and ProtonMail accounts in response to "direct [deposition] questioning about the existence of any encrypted communications platforms."[45] In light of those "deeply troubling" "systematic efforts to conceal and destroy evidence," the court granted the FTC's request for an adverse inference "that the spoliated evidence [was] unfavorable to the Individual Defendants."[46]

In *Herzig v. Arkansas Foundation for Medical Care, Inc.*,[47] the court similarly held that the plaintiffs engaged in "intentional . . . bad faith" spoliation when, following the commencement of litigation and service of discovery requests, they "switched to using a communication application [Signal] designed to disguise and destroy communications."[48] Based on the plaintiffs' "familiarity with information technology, their reluctance to produce responsive communications, the initial misleading response from [one plaintiff] that he had no responsive communications, their knowledge that they

[43] FTC v. Noland, No. CV-20-00047-PHX-DWL, 2021 WL 3857413 (D. Ariz. Aug. 30, 2021), *appeal denied*, 2021 WL 5138280 (D. Ariz. Nov. 4, 2021).
[44] *Id.* at *1.
[45] *Id.*
[46] *Id.* at *1, *14.
[47] Herzig v. Ark. Found. for Med. Care, Inc., No. 2:18-CV-02101, 2019 WL 2870106 (W.D. Ark. July 3, 2019).
[48] *Id.* at *4–5.

must retain and produce discoverable evidence, and the necessity of manually configuring Signal to delete text communications," the court inferred that the content of the deleted messages was likely responsive and concluded that the destruction of those communications "was intentional and done in bad faith."[49] The court deemed sanctions warranted but declined to impose any in light of the dismissal of the plaintiffs' claims on other grounds.[50]

Spoliation based on failure to disable auto-deletion during litigation. In *WeRide Corp. v. Huang*,[51] the court found bad-faith spoliation based in part on the defendant's failure to change preexisting auto-delete settings once a preservation obligation arose. Following issuance of a preliminary injunction forbidding the parties from destroying information relevant to the action, defendant AllRide "left in place the autodelete setting on its email server, began using [messaging system] DingTalk's ephemeral messaging feature, and maintained a policy of deleting the email accounts and wiping the computers of former employees."[52] The court held that "AllRide's conduct demonstrate[d] both willfulness and bad faith" because AllRide was in possession of court filings "indicat[ing] the relevance of" the deleted data before the destruction occurred.[53] To remedy the discovery violation, the court imposed the severe sanction of a default judgment against the defendants and ordered them to pay the plaintiff's reasonable fees and costs incurred in connection with the spoliation issue.[54]

[49] *Id.* at *5.
[50] *Id.*
[51] WeRide Corp v. Huang, No. 5:18-CV-07233-EJD, 2020 WL 1967209 (N.D. Cal. Apr. 16, 2020).
[52] *Id.* at *10, *16.
[53] *Id.* at *10.
[54] *Id.* at *16.

Use of ephemeral messaging to explain evidentiary gaps. In addition, at least one court has held that a party's use of ephemeral messaging may be relevant and admissible to account for gaps in the evidence at trial. In *Waymo v. Uber Technologies, Inc.*,[55] following a protracted dispute regarding alleged discovery abuses, the court permitted the plaintiffs to introduce the defendant's "use of ephemeral messaging . . . to explain gaps in [the plaintiff's] proof that [the defendant] misappropriated trade secrets or to supply proof that is part of the *res gestae* of the case."[56] Although the court also held that the plaintiff had "considerable ground[s]" supporting its contention that the defendant had violated Federal Rule of Civil Procedure 37(e)(2), the court reserved decision on whether to issue an adverse inference instruction pending the presentation of evidence at trial.[57]

All of the outcomes described above were heavily dependent on the facts of the particular cases and do not provide a precise roadmap for future rulings. However, these cases provide relevant data points that companies should bear in mind when crafting rules and policies to govern the use of ephemeral messaging, particularly in the context of a litigation-based preservation obligation.

Open questions. The existing case law also leaves open questions that could be material to the design of digital messaging policies. For example, once a party reasonably anticipates litigation, does the deletion of relevant ephemeral messages constitute per se improper spoliation, even in the absence of a discovery request, an injunction against destruction, or any evidence of bad faith? Stated differently, are parties obligated to stop using ephemeral messaging systems (or at least to disable auto-deletion in those systems) once a preservation obligation arises if ongoing communication

[55] Waymo L.L.C. v. Uber Tech., Inc., No. C 17-00939 WHA, 2018 WL 646701 (N.D. Cal. Jan. 29, 2018).
[56] *Id.* at *3.
[57] *Id.* at *18.

could be relevant to litigation? Cases like *Convolve*, *Herzig*, and *WeRide*, as well as the 2006 Advisory Committee note to Rule 37, suggest that the answer may be yes. However, companies could have arguments against such a blanket rule. For example, if a business uses ephemeral messaging for highly sensitive communications requiring strong security measures, and altering that system would be complicated and costly, the company might contend that such alteration falls outside the reasonable scope of its preservation obligations. It is also possible that courts will consider the likely importance of ephemeral communications to a given case in determining whether to require preservation of such communications (or deem their deletion improper). Any such determinations would be context-specific.

Another apparently open question is whether a party's use of ephemeral messaging in the regular course of business—*before* any preservation obligation arises—is admissible to explain evidentiary gaps. Such a rule arguably would go beyond the holding in *Waymo*, where evidence of the defendant's use of ephemeral messaging *while under a preservation obligation* was deemed admissible to "explain gaps in [the plaintiff's] proof" (and where the court concluded that the defendant may also have violated Rule 37(e)(2)).[58]

3. Preservation in the Regulatory Context

In recent years, government authorities have also increasingly focused on preservation issues specific to ephemeral messaging. Both the Department of Justice (DOJ) and the SEC have issued guidance in this area. Although neither agency has stated that it views ephemeral messaging systems as categorically improper, the guidance reflects skepticism that such systems are compatible with record-keeping and preservation obligations in some circumstances.

[58] *Id.*

The DOJ first published guidance on the use of ephemeral messaging in an update to its FCPA Corporate Enforcement Policy in November 2017. The update provided that in order to obtain full credit for remediating criminal wrongdoing, companies must prohibit employees from using software that generates but does not appropriately retain business records or communications.[59] In March 2019, however, the DOJ revised that policy to require instead that companies "implement[] appropriate guidance and controls on the use of personal communications and ephemeral messaging platforms that undermine the company's ability to appropriately retain business records or communications or otherwise comply with the company's document retention policies or legal obligations."[60]

This revision suggests that the DOJ does not view ephemeral messaging as categorically impermissible from a document-preservation standpoint. However, the guidance also makes clear that use of such messaging must be consistent with users' retention obligations. That stance suggests that the DOJ may expect companies to take steps to preserve otherwise ephemeral communications—for example, by disabling auto-delete functionality—when under a preservation obligation. It is also possible that the DOJ will favor more aggressive investigative and discovery tactics when the subject of an investigation uses ephemeral messaging systems.[61]

The SEC has adopted an arguably stricter stance than the DOJ in guidance regarding ephemeral messaging. In particular, a "risk alert" published in December 2018 by the

[59] U.S. DEP'T JUSTICE, U.S. ATT'Y'S MANUAL § 9-47.120 (2017), https://www.justice.gov/criminal-fraud/file/838416/download.
[60] U.S. DEP'T JUSTICE, U.S. ATT'Y'S MANUAL § 9-47.120(3)(c) (2019).
[61] *Cf.* United States v. Bradley, 488 F. App'x 99, 104 (6th Cir. 2012) (affirming conclusion that warrantless seizure of computer was constitutional and noting that "the governmental interest in protecting evidence from destruction is particularly high where digital evidence is involved, because such evidence is inherently ephemeral and easily destructible").

SEC's Office of Compliance Inspections and Examinations (OCIE) suggests that OCIE considers the use of ephemeral messaging to be generally problematic.[62]

The 2018 alert documents OCIE's observations from an examination of electronic messaging systems used by registered investment advisers. The alert notes that "changes in the way mobile and personally owned devices are used pose challenges for advisers in meeting their obligations" pursuant to record-keeping and other regulations under the Investment Advisers Act of 1940.[63] Among a set of exemplary practices that "may assist advisers in meeting" those obligations, OCIE included the following: "Specifically prohibiting 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."[64] OCIE stated further that, although its examination was limited to investment advisers, "other types of regulated financial services entities may face similar challenges with new communication tools and methods."[65]

In October 2021, Gurbir Grewal, the Director of the SEC's Enforcement Division, provided additional, enforcement-specific guidance in remarks at the Practicing Law Institute's "The SEC Speaks" conference. Mr. Grewal stated that if the Enforcement Division were to:

---

[62] OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS, U.S. SEC. & EXCH. COMM'N, OBSERVATIONS FROM INVESTMENT ADVISER EXAMINATIONS RELATING TO ELECTRONIC MESSAGING (2018), https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Electronic%20Messaging.pdf.
[63] *Id.* at 2.
[64] *Id.* at 3.
[65] *Id.* at 5.

> learn that, while litigation is anticipated or pending, corporations or individuals have not followed the rules and maintained required communications, have ignored subpoenas or litigation hold notices, or have deliberately used the sort of ephemeral technology that allows messages to disappear, *we may well conclude that spoliation of evidence has occurred* and ask the court for adverse inferences or other appropriate relief.[66]

Enforcement authorities' guidance will be important to consider in the development of control frameworks governing the use of ephemeral messaging systems. For example, regulated entities might assess (i) whether an ephemeral messaging system would permit the entity to disable the automatic deletion function on demand and (ii) whether the company has processes and procedures in place that would facilitate prompt assessment of whether to take that step when a potential preservation obligation arises.

B. Use of Personal Devices

Another critical retention and collection issue relating to New Digital Messaging Systems is the proliferation of BYOD ("Bring Your Own Device") arrangements, in which employees use personal devices for business communications. BYOD offers convenience and efficiency but also poses security and preservation issues for employers by (among other things) increasing the risk that employees will conduct work-related communications using unapproved New Digital Messaging Systems. Absent effective control over the systems used by employees on BYOD devices, an employer risks failing to preserve communications that could be subject to document-retention

[66] Gurbir Grewal, *Remarks at SEC Speaks 2021,* U.S. SEC. & EXCH. COMM'N (Oct. 13, 2021) (emphasis added), https://www.sec.gov/news/speech/grewal-sec-speaks-101321.

obligations. Further, where data is preserved, collection from employees' personal devices in connection with litigation or regulatory investigations may raise privacy issues.

As with the other issues discussed in this article, a company's approach to addressing these challenges will depend on its particular circumstances. Potentially applicable compliance measures could include:

- Clearly delineating which messaging systems or apps employees may use on their personal devices for business purposes.

- Ensuring that permitted systems are linked to the company's systems so that the company can control message retention settings.

- Requiring employees to implement specified security features and to permit the company to alter the device remotely (for example, by wiping data if the device is lost or stolen).

- Establishing controls to deter the use of unapproved messaging systems, including, for example, employee certifications of compliance with communication policies.

- Negotiating the terms of potential data collection from BYOD devices at the outset of employment.

Recent enforcement activity has underscored the imperative for companies to establish effective BYOD compliance programs. In December 2021, the SEC and the Commodity Futures Trading Commission (CFTC) instituted proceedings against a major financial institution under the Securities Exchange Act and the Commodities Exchange Act, respectively, based on the bank's alleged failure to preserve text and

WhatsApp communications exchanged by employees using their personal mobile devices. Both agencies alleged that at least some of the deleted communications were relevant to ongoing enforcement matters. The institution agreed to pay fines totaling $200 million to resolve the record-keeping actions.[67]

This proceeding appears to have been part of a broader probe. In the first quarter of 2022, three other financial institutions disclosed investigations by the SEC and/or the CFTC related to employees' use of unapproved electronic messaging channels for business communications.[68] Regulated entities should continue to monitor these investigations, which could precipitate the publication of agency findings or guidance relevant to the development of BYOD policies.

V. Collection and Production

Adoption of New Digital Messaging Systems will also likely impact the collection and production of electronic communications. Parties may need to develop new collection techniques for these systems, and the burden of producing certain forms of digital messages will likely lead to litigation.

Channel- and chat-based document collection. The widespread adoption of chat-based messaging platforms like Slack could change the framework for collecting and searching electronic communications in litigation. In the email era, document discovery has typically been premised on the identification of relevant document custodians and the negotiation of parameters to search those custodians' records. This approach

[67] *See* J.P. Morgan Sec. L.L.C., Exchange Act Release No. 34-93807, 2021 WL 5986789 (Dec. 17, 2021); *In re* JPMorgan Chase Bank, CFTC No. 22-07, 2021 WL 6098347 (Dec. 17, 2021).
[68] Goldman Sachs Grp. Inc., Annual Report (Form 10-K) 217 (2021); HSBC USA Inc., Annual Report (Form 10-K) 203 (2021); Citigroup Inc., Annual Report (Form 10-K) 300 (2021).

is well-suited to email discovery because email providers typically store email in accounts specific to individual users. Further, email exchanges are typically time-limited and focused on specific issues. Applying topical search terms to a custodian's email within a specified date range thus normally allows parties to identify relevant communications with reasonable precision.

By contrast, conversations on the Slack platform occur in channels, which remain open indefinitely once created and function essentially as chat rooms for ongoing communication (users can also send each other direct messages). Channels exist within broader "workspaces," which often include all of a corporate user's employees. Each channel can be either public (*i.e.*, open to all individuals in the workspace) or private (*i.e.*, open only to users invited to join). As a result of this organizational structure, Slack channels may contain tens or hundreds of thousands of messages, making them potentially cumbersome to collect. Further, a standard export of data from Slack is organized by channel—not by a particular individual's communications.[69]

In addition, the Slack platform contains multiple apps and is capable of integration with outside data sources. For example, a user could upload an external database to a channel or integrate Google Drive into the Slack messaging system.[70]

In light of these features, e-discovery of Slack data is not as simple as selecting relevant custodians and collecting their electronic accounts. Instead, companies will need to work with counsel to craft new search methods designed to retrieve responsive data as precisely as possible and address any external data sources integrated into the messages selected for collection.

---

[69] *The Lawyer's Guide to Discovery and Investigations in Slack*, LOGIKCULL ch. 3, https://www.logikcull.com/slack (last visited Mar. 5, 2022).
[70] *Id.* ch. 2–3.

Collection of records held by individual employees or technology providers. New Digital Messaging Systems may also expand the universe of locations where relevant documents are stored. When workplace electronic communication was limited principally to the exchange of emails using company-provided accounts, collection was correspondingly limited to the email (and other electronic documents) stored on a company's servers or employees' company-issued devices. As noted above, however, given the prevalence of BYOD arrangements, many employees now use New Digital Messaging Systems on their personal devices, sometimes using personal accounts. Any such additional sources of business communications may need to be accounted for in conducting data collection in litigation.

In addition, in some cases, data subject to discovery requests may be housed with the technology provider rather than the user. For example, under certain Slack service plans, private-channel and direct messages remain in Slack's possession and cannot be collected by the plan holder. That retention approach has been held to preclude discovery of such messages from plan holders.[71] However, other recent authority suggests that parties may be able to seek non-party discovery from platform providers to obtain records to which plan holders lack access.[72]

---

[71] *See* Laub v. Horbaczewski, No. CV 17-6210-JAK (KSx), 2020 WL 7978227, at *4 (C.D. Cal. Nov. 17, 2020) (denying discovery of private-channel Slack messages because they were "housed at Slack.com and, therefore, [respondent] did not have possession, custody, and control over them"); Calendar Research L.L.C. v. StubHub, Inc., No. CV 17-4062 SVW (SSx), 2019 WL 1581406, at *4 (C.D. Cal. Mar. 14, 2019) (explaining that Slack had "informed Defendants that it would not allow full corporate export of the entire account without the consent of all parties who used the account").

[72] *See* Facebook, Inc. v. Pepe, 241 A.3d 248, 254–56 (D.C. 2020) (ordering Facebook to respond to subpoena served by defendant in criminal case seeking copies of Instagram messages that were no longer preserved on his account); *see also Snap Inc. Law Enforcement Guide* (Sept. 29, 2020), https://storage.googleapis.com/snap-inc/privacy/lawenforcement.pdf (explaining that SnapChat owner Snap Inc. can create, at the request of law enforcement, "preservations" of data deleted from users' devices,

Burden of production. Given the volume of communications exchanged using New Digital Messaging Systems and the collection issues described above, producing parties may be in a position to contend that wide-ranging discovery of such communications is unduly burdensome. Federal courts have begun to address this question under the prevailing proportionality standard codified in Rule 26, with mixed results.

In *Benebone v. Pet Qwerks, Inc.*,[73] for example, the court determined following an evidentiary hearing that "requiring review and production of Slack messages by [plaintiff] is generally comparable to requiring search and production of emails and is not unduly burdensome or disproportional to the needs of this case—if the requests and searches are appropriately limited and focused."[74] The court noted, however, that its conclusion was based in part on the plaintiff's failure to proffer any "witness or declarant on the e-discovery issues."[75]

By contrast, in *Milbeck v. TrueCar, Inc.*,[76] the court denied discovery of the defendant's Slack data, despite its conceded relevance, on the ground that such discovery could not be completed under the governing case schedule "given all of the other discovery that is also relevant."[77] The court reasoned that the defendant had shown that "[c]onversion and processing of the Slack data—which is necessary before any information can be extracted or any particular channel identified— will likely take at least six weeks

including "basic subscriber information, metadata (usage logs) and content (Chats, Snaps, Stories, and Memories)").

[73] Benebone L.L.C. v. Pet Qwerks, Inc., No. 8:20-cv-00850-AB-AFMx, 2021 WL 831025 (C.D. Cal. Feb. 18, 2021).

[74] *Id.* at *3.

[75] *Id.*

[76] Milbeck v. TrueCar, Inc., No. CV 18-02612-SVW (AGRx), 2019 WL 4570017 (C.D. Cal. May 2, 2019).

[77] *Id.* at *3.

and perhaps up to eight weeks," and that "manual review will be necessary to identify the start and end of relevant conversations."[78]

Parties should expect further litigation regarding these burden questions in the coming months and years. As with other e-discovery issues, results are likely to be highly context-specific.

VI. Privilege and Confidentiality

Use of New Digital Messaging Systems also may give rise to unique privilege and confidentiality issues in the discovery context. Two examples are described below.

Potential disclosure of privileged information. Chat- or channel-based digital communication may raise issues concerning the protection of privileged information. For example, Slack users may invite third parties to join channels, including existing channels that contain otherwise internal communications.[79] If a third party joins a channel in which a privileged communication previously occurred—potentially days, weeks, or months earlier—then the company could risk an inadvertent privilege waiver. Although email forwarding poses a similar concern, the risk is arguably more pronounced in the context of conversation channels that remain open indefinitely and address a broad range of topics. One method of managing this risk could be to require employees, including internal counsel, to use private channels or direct messages to seek and provide legal advice.

[78] *Id.* (denying motion to compel without prejudice to renewal in the event of a continuance of the trial date).
[79] *See Using Slack*, SLACK.COM, https://slack.com/help/articles/360017938993-What-is-a-channel (last visited Mar. 5, 2022).

Isolation of relevant information. Because chat-based messaging systems facilitate lengthy exchanges encompassing multiple topics, use of such systems may pose challenges with respect to isolating information that is relevant to litigation and responsive to discovery requests. Companies employing chat-based systems may decide to seek permission either to redact the irrelevant portions of lengthy chats or to produce those portions on an attorneys'-eyes-only basis. There is authority supporting this approach.[80]

VII. Conclusion

The use of New Digital Messaging Systems poses issues of first impression in connection with multiple aspects of electronic discovery, including data preservation, document collection and production, and the protection of privileged or sensitive data. Consideration of these questions by courts and regulators appears to be in its early stages. Companies seeking to leverage the benefits of New Digital Messaging Systems thus should continue to monitor developments and consult with counsel to structure relevant policies and practices.

[80] *See* Podium Corp. Inc. v. Chekkit Geolocation Servs., Inc., No. 2:20-cv-00352-JNP-DAO, 2021 WL 1873989, at *2 (D. Utah May 10, 2021) (permitting designation of sensitive and irrelevant information in Slack data as attorneys'-eyes-only, but denying permission to designate responsive, non-sensitive information as attorneys'-eyes-only).