Grasping Ephemeral Messages

BY MICHAEL KOENIG AND DAVID CRAIG

By now, most everyone in the defense bar has heard of ephemeral messages and the challenges they present to compliance and litigation. The importance of having a plan to confront those challenges persists across administration. Keeping in line with the Biden Administration's position, Gail Slater—AAG of the Antitrust Division—announced on August 29 the formation of a "Comply with Care" taskforce dedicated to addressing (among other related things) ephemeral messages. AAG Slater forewarned the bar: the Division "will not hesitate to bring [such issues] to court" and "will not shy away from pursuing them, taking advantage of the full range of available penalties." Assistant Attorney General Gail Slater, Remarks to the Ohio State University Law School (Aug. 29, 2025).

At the same time, the trend toward normalizing ephemeral communications is accelerating faster than anticipated. Meta's latest WhatsApp advertising campaign goes beyond merely highlighting privacy and instead actively promotes inaccessible messaging as appropriate for both personal and professional use. For those of us who work in investigations, compliance, and litigation, this only adds fuel to the fire. As encrypted platforms become mainstream, the already-complicated task of auditing compliance, issuing and enforcing litigation holds, and conducting effective discovery becomes even more difficult. We are moving quickly from trying to keep communications on the record to grappling with the fact that there may be no record at all.

Although a complete, infallible preservation and retrieval solution does not exist, there are reasonable and defensible measures counsel can take to manage the rapidly evolving ephemeral messaging landscape. To ensure a common starting point for this discussion, the question must be asked: What exactly is an "ephemeral" message? For many, it is a self-deleting message such as one sent via Signal. But the concept is broader than that. It includes platforms such as

MICHAEL KOENIG (mkoenig@secretariat-intl.com) is a former federal prosecutor in DOJ's Antitrust Division serving as a managing director in the Global Investigations & Disputes group at Secretariat in Washington, DC. **DAVID CRAIG** (dcraig@secretariat-intl.com) is a communications and compliance expert serving as a managing director in the Global Investigations & Disputes group at Secretariat in New York, NY.

> *Expecting employees to have business conversations only on certain approved platforms is often unrealistic, considering client demands and the practical realities of doing business in an evolving world.*

iMessage and other peer-to-peer applications that corporate IT cannot unilaterally locate or capture and where end-users can permanently delete content. The challenge is not only from self-deleting features per se, but rather IT’s lack of visibility into or control over those platforms.

To address this broader scope, we have previously proposed that “‘ephemeral’ should be defined as any messaging system where a company cannot systematically enforce a litigation hold [or a records-retention policy, in the context of compliance] without end-user involvement.” David Craig et al., *Personal and Ephemeral Messaging Platforms: A Priority Target for Enforcement and Regulators*, Compliance & Enf’t (Mar. 20, 2025), https://tinyurl.com/7n9uy9bu.

Our definition is broad enough to encompass communications such as iMessage on BYOD devices where the employees have complete control, as well as communications that could be retained but are nevertheless not readily accessible to corporate IT. In the case of an investigation or under a reasonable anticipation of litigation, the latter types of messages require some sort of additional effort outside of normal IT practices to preserve. For example, it became readily apparent late in the discovery process that key communications threads about relevant issues in *Epic v. Google*, No. 3:20-cv-5671-JD (N.D. Cal.), occurred via the company’s internal Instant Messaging (IM) platform, Google Chat. Although the company had the ability with the flip of a switch to archive messages for key individuals in response to a litigation hold, Google opted instead to rely on individual employees to recognize and save Chat messages on an ad hoc basis. The messages were thus “ephemeral” under our definition because Google ceded visibility and control.

The ever-increasing tendency of employees to engage in ephemeral messaging is, from litigation and compliance perspectives, fraught with peril. One needs to look no further than the SEC’s off-channel communication sweeps or the litigation hold violations uncovered in *Epic v. Google*; *FTC v. Amazon*, No. 2:23-cv-1495-JHC (W.D. Wash.); and *FTC v. Kroger-Albertson’s*, No. 3:24-cv-00347-AN (D. Or.). Nevertheless, expecting employees to have business conversations only on certain approved platforms, whether those platforms are on a personal device or a company-provided device, is often unrealistic considering client demands and the practical realities of doing business in an evolving world. Efforts to stop the ephemeral-messaging trend within a company can feel like holding back the tide, placing counsel and their clients in a precarious position when regulators or the courts come knocking.

The old chestnut “an ounce of prevention is worth a pound of cure” has no better place than in the world of ephemeral messages. We are beginning to see companies and their counsel picking up the mantle in an effort to set themselves apart from their peers due to increased publicity. But there continues to be reluctance by many to get ahead of the problem. A cynic might say that reluctance is driven by a head-in-the-sand mentality. And there may be some truth to that. However, we have observed that companies and their counsel operate under false assumptions about cost and effectiveness: Anything that will work is going to be pricey.

Concern about the cost of proactive measures is perfectly understandable. As we explained in our earlier article, the rapid expansion of bring-your-own-device (BYOD) policies was the primary culprit behind the ephemeral messaging problem. *See* Craig et al., *supra*. That being the case, the first instinct is often to scrap BYOD and instead provide employees with company-owned and controlled devices that lock down access to and use of ephemeral-messaging apps, such as iMessage and Signal, and minimize employee’s expectation of privacy—the idea being that if all business-related communications can be confined to company-owned devices and approved messaging apps, then corporate IT has visibility and retention control for compliance and lit-hold purposes.

For large companies, procuring, distributing, and maintaining thousands of devices across the organization is an unquestionably huge expense. But it works, right? Our observation has been that it is an ineffective (and cumbersome) approach. Consider an employee whose success (i.e., paycheck) depends on long-standing relationships with clients-turned-friends (or vice versa) who have always used the same method of communication. Is it realistic to expect that employee, upon receiving a company-owned device stripped of privacy, to tell the client-turned-friend to use one number for business and another for pleasure? Unlikely. (Especially if iMessage is blocked . . . people want to text in blue bubbles, not green.) The result we have seen is that such employees continue to generate ephemeral messages on their personal devices.

Mandating the installation of a mobile device management (MDM) application to manage and monitor communications on personal devices is a proactive approach for BYOD companies to avoid the cost of provisioning and maintaining company-owned devices. MDM is often thought of as a lower-cost and equally effective approach. The problem is that MDM tends to be wildly *un*popular with employees because of its intrusiveness. And employees have been known to buy a second device anyway, so the effectiveness of an MDM solution is likely little better than issuing company-owned devices.

On the back end, when a need arises to implement a litigation hold and collect documents, the provision of company-owned devices will make it more difficult to obtain ephemeral messages from an employee's personal device. Practically speaking, the baseline assumption is that employees follow policy and use only company-owned devices for work-related communications. Whereas the presumption in a BYOD environment is that the employee's personal device houses company documents, the presumption in a non-BYOD environment is exactly the opposite. Absent strong evidence to the contrary, counsel for the company will not image the personal device. Even in a BYOD environment, telling employees to hand over personal devices is a prickly endeavor, especially higher up the ladder. Again, absent strong evidence of relevant and responsive off-channel messages on the device, counsel may be granted access only to firm-approved applications and storage areas.

Locating evidence to justify the deeper search of a personal device or personal apps is a task for which a traditional "linear" approach is ill-suited. As we previously described that approach: "identify a list of custodians and collect massive amounts of data and frequently hand over that data to a third-party team for relevance review that is an arm's-length removed from the fact team conducting the investigation," noting that "the review team is not trained nor expected to look for discovery gaps or clues in the data that suggest additional sources of relevant information." Craig et al., *supra*. Often, counsel has a comprehensive list of ephemeral-related questions to ask every custodian, but when there is a denial (e.g., "I don't use WhatsApp"), that is pretty much the end of the road. That is the opposite of what we have called "trust but verify." Years into discovery, counsel learns that the denials were misleading, at best, resulting in potential spoliation claims.

We think there is a better approach, one that complements (but does not necessarily replace) the traditional methods. While no solution can be perfect, our experience has taught us that a risk-based, investigative approach, used both proactively as a form of compliance and reactively when the company receives a subpoena or other document demand, can be very effective in uncovering ephemeral messages without breaking the bank.

Compliance

Perfect compliance is achieved when there is no gap between policies and practices. However, we have learned that a company's communications and retention policies are sometimes worth little more than the paper on which they are written—something the SEC's off-channel communications sweeps confirmed by uncovering, for example, "widespread and longstanding failure of Goldman Sachs employees throughout the firm, including at senior levels, to adhere to certain of these essential requirements and the firm's own policies." *Goldman Sachs & Co. LLC*, Exchange Act Release No. 95922, ¶ 2 (Sept. 27, 2022), https://tinyurl.com/4uyhracu.

> “*Whereas the presumption in a BYOD environment is that the employee's personal device houses company documents, the presumption in a non-BYOD environment is exactly the opposite.*”

Proactively auditing compliance with those policies in a meaningful way is therefore critical. That means going beyond a list of questions and investigating. We suggest a cost-effective three-stage approach. First, focus on low-hanging fruit by analyzing existing repositories of communications for indicia of behavior inconsistent with policy. That can be as simple as keyword searches across all repositories for terms such as "WhatsApp" or "text me" or "offline," and as sophisticated as designing a bespoke AI tool capable of flagging departures from official channels of communication. It also can involve probing known instances of ephemeral communication that may or may not have been fixed.

Second, create risk "scorecards" for employees or groups of employees that account for characteristics of their functions, historical compliance trends, and publicly available information regarding social media presence. Here are some examples:

- *Low risk:* Administrative assistants having (a) almost entirely internal responsibilities and no ability to bind the company on significant decisions, (b) moderate history of policy violations, and (c) high social media presence. Although employees in this group have a high social media presence and a less-than-ideal compliance history, their low level of outward-facing functions and inability to make decisions on behalf of the company are significant offsetting factors.
- *Moderate risk:* C-suite executives having (a) substantial internal and external responsibilities with the ability to bind the company on significant decisions, (b) low history of policy violations, and (c) low social media presence. Employees in this group, who have a solid compliance history and do not use much social media, are nevertheless elevated because of the enormous power they wield both inside and outside the company.
- *High risk:* Sales representatives having (a) almost entirely external responsibilities and a moderate ability to bind the company, (b) high history of policy violations, and (c) high social media presence. Employees in this group clearly need to be monitored closely because, even if they cannot sign off on high-dollar contracts, they are out in the market making representations to clients attributable to the company.

These are simplified examples, but they illustrate how to focus auditing resources.

Third, with the highest-risk groups now identified, data analytics enter the picture. As auditors, we can pull metadata from the company's communications applications for high-risk employees to search for anomalistic trends. If an employee in a high-risk group is adhering to policy and using only on-channel communication methods, we expect to see consistent patterns. For example, a sales employee in a high-risk group is responsible for an annual contract with a customer, and the metadata reveal a spike in communications between the employee and the customer every year in the weeks surrounding the contract renewal date. That would not raise any flags because the spike is similar year-to-year and, intuitively, one would expect communications to increase during that window of time. If, on the other hand, the metadata reveal a year with a missing spike, but the contract was nevertheless completed, then that suggests the employee and customer may have used an ephemeral messaging platform (i.e., unknown, and inaccessible to corporate IT) to conduct business.

In the latter case, a deeper dive is warranted, likely requiring employee interviews and analysis of substantive communications extracted from the company's servers to understand the reason for the anomaly. If there are significant indicia of ephemeral communications (e.g., admissions during interviews or textual clues within the communications themselves), at that point counsel and the company have solid footing to demand employees' personal devices or personal apps to search directly for ephemeral communications. To be sure, a deeper dive implies increased costs, but with the pool of employees already narrowed by risk scoring and data analytics, those costs are far more manageable. And through this process, a company can reap substantial benefits if and when it needs to conduct a reactive investigation.

> “*First focus on low-hanging fruit, then create risk scorecards, and finally take a deep dive with high-risk custodians.*”

Litigation

The investigative discovery approach for litigation—the goal of which is *not* to identify the entire universe of responsive documents for production, but rather to locate relevant ephemeral communications—mirrors the approach for compliance, with a litigation hold as a proxy for a communications policy.

First focus on low-hanging fruit, then create risk scorecards, and finally take a deep dive with high-risk custodians. The low-hanging fruit here looks a little different than in the compliance context. In litigation, time is of the essence, so a preferred strategy is to deploy immediately a small team of tech-savvy and legally informed investigators who can quickly learn the communications culture of the company and triage according to risk. That requires initial interviews of IT personnel to map the company-controlled communications systems and identify potential trouble spots. One surprisingly often-overlooked trouble spot is the on/off switch for autodelete. If the company's email server, for example, follows an X-day retention policy, that feature needs to be disabled on day one. The same goes for any other communications platforms, e.g., Teams or Google Chat. During the IT personnel interviews, the team also should inquire about any known instances of ephemeral communications and what, if anything, was done to remedy that situation. These are low-cost steps that can save major headaches further down the road.

Developing risk scorecards in the litigation context will be a project that starts from scratch, but if the work was already done for compliance purposes, they can serve as a foundation. But unlike compliance, the risk scorecards here also should account for the legal theories at issue in the litigation and focus on only a subset of employees likely to have relevant information.

When taking the deeper dive in step three, the investigative discovery team should be prepared to image personal devices at the outset. That does not mean doing so indiscriminately, but once sufficient indicia of ephemeral communication activity surface, there should be no delay in creating an image of the offending device. Otherwise, as experience has taught us, the probability of the employee attempting to delete material from the device, or even attempting to destroy the device, increases significantly. And if that happens, we are left with just trust because we cannot verify.

Conclusion

In the end, one thing is abundantly clear: Ephemeral messages (as we have defined them) are not going away. Rather than resisting the inevitable by implementing unrealistic policies or litigation holds and hoping they will be followed, counsel should consider adopting the approach we have outlined above to help mitigate fallout from this unstoppable trend. ■

[redacted]