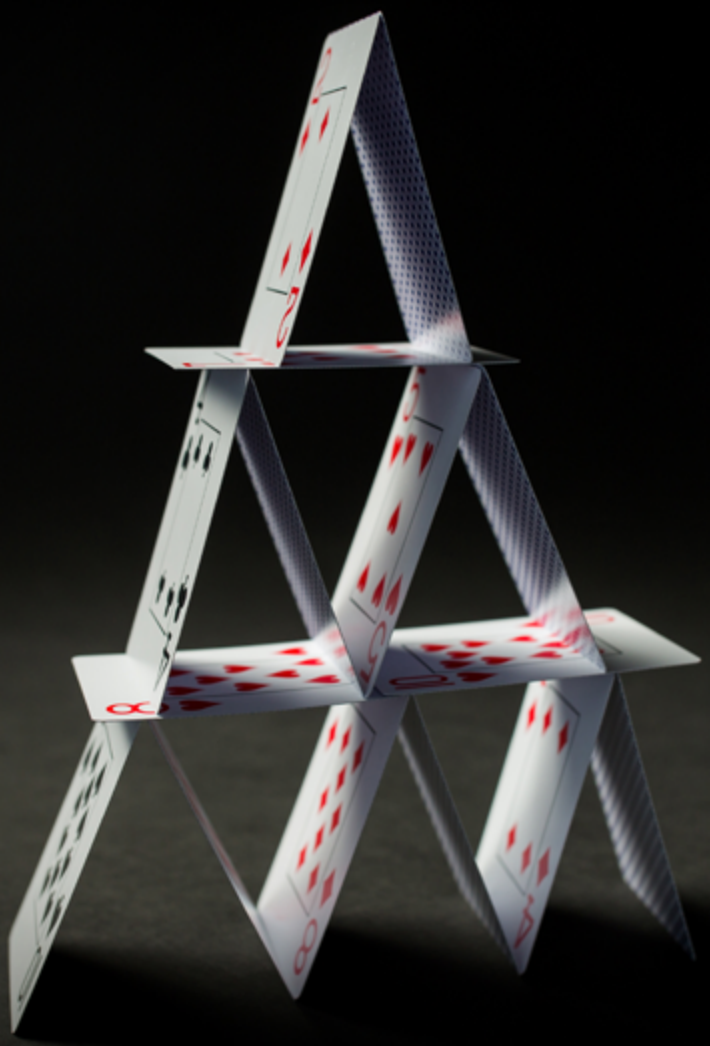
OFF-CHANNEL AND EPHEMERAL MESSAGING IN ANTITRUST INVESTIGATIONS: LEGAL RISKS, REGULATORY FOCUS, AND EDISCOVERY CHALLENGES



BY DANIEL RUPPRECHT & DR. TRISTAN JENKINSON[1]

1 Sky Discovery is an independent eDiscovery and litigation-support firm founded in Australia and now operating across the UK and EU. Daniel Rupprecht (Managing Director, UK & EU) is a qualified U.S. attorney with a wide-ranging experience of eDiscovery in the UK, US and Europe. He specialises in antitrust and regulatory investigations. Dr Tristan Jenkinson (Head of Forensics & Investigations, UK & EU) is an expert witness with considerable experience in digital forensic investigations and eDiscovery best practices.

CPI ANTITRUST CHRONICLE
June 2025

Visit www.competitionpolicyinternational.com for access to these articles and more!

OFF-CHANNEL AND EPHEMERAL MESSAGING IN ANTITRUST INVESTIGATIONS: LEGAL RISKS, REGULATORY FOCUS, AND EDISCOVERY CHALLENGES

By Daniel Rupprecht & Dr. Tristan Jenkinson

The use of ephemeral and off-channel messaging apps like WhatsApp, Signal, and Telegram in corporate settings has become a critical concern for regulators, especially in antitrust investigations. These platforms, designed for privacy and message deletion, hinder compliance efforts, frustrate eDiscovery, and raise obstruction risks. Regulators in the U.S., UK, and EU are tightening expectations, with agencies such as the DOJ, FTC, SEC, and CMA issuing updated guidance, sanctions, and procedural obligations targeting message preservation — even from personal devices. Legal consequences for non-compliance include spoliation sanctions, fines, and obstruction charges, with potential liability extending to legal counsel. The paper outlines forensic and eDiscovery methods to detect use of these apps, and urges companies to adopt robust messaging policies, enforce legal holds, and implement compliance monitoring. As enforcement intensifies, proactive governance over digital communications is essential to avoid penalties and ensure regulatory cooperation.

I. INTRODUCTION

The growing use of off-channel and ephemeral messaging applications in corporate environments has raised complex questions for regulators, legal practitioners, and compliance teams, particularly in the context of antitrust investigations. Well known platforms such as Signal, WhatsApp, Telegram, and Snapchat, as well as lesser-known applications such as Dust, Confide and Wickr (now owned by Amazon) are increasingly used by employees for both personal and, more concerningly, professional communications – often without business approval to do so. While these messaging tools can offer speed, convenience, and privacy, their design, in particular regarding limiting the lifespan of messages, poses significant risks when it comes to regulatory compliance, legal hold obligations, and the ability to preserve and produce discoverable communications.

Over the last few years, antitrust authorities across jurisdictions have sharpened their focus on the use of these tools, seeing them as potential avenues for concealing misconduct or as a method to hide evidence in sensitive matters such as price fixing, market allocation, or other anti-competitive practices. The resulting enforcement activity and guidance underscore a key theme: corporate policies that permit or fail to control ephemeral messaging may be viewed as a red flag, or even as obstruction.

This article explores several topics relating to the regulatory landscape surrounding ephemeral messaging in antitrust investigations, including the legal and practical challenges it poses for eDiscovery, steps that can be taken to investigate or identify the use of ephemeral messaging applications, and best practices for organizations seeking to navigate this evolving area.

II. DEFINING OFF-CHANNEL AND EPHEMERAL MESSAGING

Before discussing the relevant legal considerations, it is first necessary to define terms:

- ***Off-Channel Communications*** - Communications relating to business which are sent or received using platforms or applications which have not been approved or authorised by the business. For example, typically a business may expect you to use business email addresses for business, but may not have approved the use of a personal email account. Therefore, messages sent about business matters using that personal email account would be deemed to be 'off-channel'. In comparison, the phrase 'on-channel' communication is sometimes used to represent the platforms and applications authorised for business use.

- ***Ephemeral Messaging*** - Digital communication that is designed or set up to automatically delete messages after a specific period, or even immediately after being viewed. In some cases such messages cannot be saved, forwarded, or screenshots taken, without alerting the sender.

Ephemeral messaging is more widespread than many appreciate. Popular messaging applications such as Signal and Telegram became popular, at least in part, because of their security and privacy features. These features include the ability to automatically delete messages after seconds, minutes, or days. However, many other messaging applications now have similar capabilities. WhatsApp includes a disappearing message function, which can be applied at the individual or group level, and iMessages on an iPhone can be set to automatically delete after 30 days, or a year. This means that iMessages sent or received on a business mobile device could be considered ephemeral messages - A key point that could easily be overlooked.

In addition to the automated deletion of messages, a common feature of ephemeral messages systems is end-to-end-encryption, ensuring that messages are only accessible to the sender and recipient, not to any third parties, such as the developers of the messaging application being used. In addition, many of the messaging applications with ephemeral messaging capabilities only store message data on the phone itself, so there is no copy of the data on the server side (owned by the application developer). Typically, the systems are also designed so that there is limited, if any, metadata or logging available once messages have been deleted.

While these features can enhance privacy and security, they also inhibit traditional methods of corporate oversight and data preservation, which are key pillars of antitrust compliance and litigation readiness.

III. REGULATORY SCRUTINY: GLOBAL TRENDS AND ENFORCEMENT

Regulators across a range of global jurisdictions, including the United States and the European Union, have increasingly voiced concerns over the use of ephemeral messaging platforms in corporate environments, particularly when these tools are used for business-related discussions that fall outside of established, auditable channels.

For example, in 2021, the Federal Trade Commission recently sought and received an adverse inference sanction against the defendants for the use of (and spoliation of data from) Signal and ProtonMail.[2]

In recent years, enforcement authorities have expanded their focus beyond substantive violations to include the adequacy of corporate compliance infrastructures, including policies governing the retention of electronic communications. Officials have signalled that the use of self-deleting or encrypted messaging tools may pose significant compliance risks, especially if such practices hinder regulatory oversight or obstruct investigations.

For example, in March 2023, the U.S. Department of Justice updated their Evaluation of Corporate Compliance Programs document. The updated document highlights that:

> *"In evaluating a corporation's policies and mechanisms for identifying, reporting, investigating, and remediating potential misconduct and violations of law, prosecutors should consider a corporation's policies and procedures governing the use of personal devices, communications platforms, and messaging applications, including ephemeral messaging application" as well as "[p]olicies governing such applications should be tailored to the corporation's risk profile and specific business needs and ensure that, as appropriate and to the greatest extent possible, business-related electronic data and communications are accessible and amenable to preservation by the company."*[3]

Under questions to be considered regarding risk management factors, the evaluation document highlights the below question: "Has the use of personal devices or messaging applications—including ephemeral messaging applications—impaired in any way the organization's compliance program or its ability to conduct internal investigations or respond to requests from prosecutors or civil enforcement or regulatory agencies."

Also in March 2023, Google were sanctioned by District Judge James Donato as part of the Google Play Store antitrust case, for allowing the automated deletion of messages on Google Chat, despite being under legal hold.[4] When chat history was turned off (the default state) one to one chats were retained for just 24 hours, effectively making Google Chat an ephemeral messaging application. The findings of Judge Donato are summarized well in an article from Sidley Austin.[5]

Senior officials from leading enforcement agencies have warned that companies relying on ephemeral messaging could face enhanced scrutiny and more severe penalties where such technologies impede document preservation obligations. Following updates to how some enforcement agencies request data (discussed below), potential liability for legal advisors has also been highlighted with regard to off-channel and ephemeral messaging.

In January 2024, the FTC and DOJ announced updates relating to the preservation of ephemeral messages, also covered in a joint press release.[6] The main thrust of the announcement relates to updates in various standard letters and specifications. As quoted in the press release, FTC Bureau of Competition, Henry Liu stated:

> *"Companies and individuals have a legal responsibility to preserve documents when involved in government investigations or litigation in order to promote efficient and effective enforcement that protects the American public. Today's update reinforces*

2 *Fed. Trade Comm'n v Noland*, 2021 WL 3857413 [D. Ariz. Aug. 30, 2021]. For a discussion on this case see for example https://www.jdsupra.com/legalnews/court-sends-signal-to-parties-who-7102770/.

3 A copy of this document, with the March 2023 updates can be found on the Internet Archive - https://web.archive.org/web/20240226132649/https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl?inline.

4 See https://fingfx.thomsonreuters.com/gfx/legaldocs/dwpkdknlmvm/Donato-Google-sanctions-order-2023-03-28.pdf.

5 https://www.sidley.com/en/-/media/uploads/ediscovery/2023/in-re-google-play-store-antitrust-litigation--f-supp-3d--2023-wl-2673109-no-21md02981.pdf.

6 https://www.justice.gov/archives/opa/pr/justice-department-and-ftc-update-guidance-reinforces-parties-preservation-obligations.

that this preservation responsibility applies to new methods of collaboration and information sharing tools, even including tools that allow for messages to disappear via ephemeral messaging capabilities."

Manish Kumar, Deputy Assistant Attorney General of the DOJ Antitrust Division highlighted also quoted in the press release, went further:[7]

"These updates to our legal process will ensure that neither opposing counsel nor their clients can feign ignorance when their clients or companies choose to conduct business through ephemeral messages"

"… The Antitrust Division and the Federal Trade Commission expect that opposing counsel will preserve and produce any and all responsive documents, including data from ephemeral messaging applications designed to hide evidence. Failure to produce such documents may result in obstruction of justice charges"

Providing comments on the announcement, Cleary Gottlieb highlight some important implications for those having to respond to requests from the DOJ and the FTC, in light of these changes. In particular, they highlight that the lack of preservation of ephemeral data (outside of regulatory requirements to do so) would likely not by itself be enough to support a criminal charge, but that failure to preserve the messages while subject to litigation hold or while under subpoena carries a risk.[8] Further Cleary Gottlieb refer to the *FTC v Noland* case above, explaining that starting to use ephemeral messaging while in the middle of litigation or investigation would carry a (significantly) higher level of risk.

Covington also provided commentary on the announcement, providing more focus on the updates to the standard letters. For example, Covington highlight changes to the language in the letter specifying information sought in a second request, which update the definition of what constitutes a document:

"The FTC also supplemented the definition of "documents" in the Model with a separate definition of "Messaging Application", which goes beyond more traditional means of communication, like email, to capture 'platforms, whether for ephemeral or non-ephemeral messaging, for . . . chats, instant messages, text messages, and other methods of group and individual communication (e.g., Microsoft Teams, Slack).'"[9]

Covington also raise a further important point that the new language

"… places a greater emphasis on preserving [the FTC and DOJ's] ability to obtain information from personal devices that employees use for work purposes"

This demonstrates further plans to look into off-channel communications from personal devices, though Covington also stress that despite the updated language:

"While the FTC and the Antitrust Division identify the types of information they expect to obtain, it is important to remember that courts are the ultimate arbiters of what information companies must preserve and produce in an investigation or litigation, as well as of questions regarding potential spoliation"[10]

*In addi*tion to the above, there are some further statements that are worth highlighting, in particular in order to highlight the emphasis being put on how non-compliance would be viewed, and the potential resulting legal exposure.

As a precursor to the release of the above announcement and press release from the DOJ and FTC on 26 January 2024, the day prior, Leslie Wulff, chief of the DOJ Antitrust Division in San Francisco is reported as stating:

---

7 *Ibid.*

8 https://www.clearygottlieb.com/news-and-insights/publication-listing/us-antitrust-regulators-threaten-ephemeral-messaging-users-and-their-counsel-with-obstruction-charges#_ftn16.

9 https://www.cov.com/en/news-and-insights/insights/2024/02/antitrust-agencies-clarify-their-position-on-companies-preservation-obligations-ephemeral-messaging-platforms-and-collaboration-tools/.

10 *Ibid.*

"Decisions that counsel make here are really important, because missteps can result in further criminal exposure for the employees at the company involved in the conduct, but perhaps even more importantly, can also result in criminal exposure for the attorneys and company counsel."[11]

While Counsel to the Assistant Attorney General of the Antitrust Division of the DOJ, Jill Rogowski, is quoted as stating the below:

"… we will not hesitate to bring obstruction charges, and of course, if the client was not properly advised by their attorney or if the attorney was otherwise involved in the deletion of those messages or in allowing those messages to be deleted, then the attorney could also be subject to charges."

In April 2025, the SEC issued an order regarding 16 settlements regarding the use of off-channel communications reached with firms during the period of September 2023 – September 2024. The 16 firms involved sought to "equalise" the settlements, since latter agreements were considered to be on better terms that some of the earlier agreements.

The firms sought to remove some of the restrictions included in their settlements. One of these was a requirement that *"[r]espondents report employee discipline regarding offchannel communications to the Commission for two years."*

The SEC made it clear that they would not revisit the terms of any of the settled orders.[12] Overall, the comments from Regulators indicate that messaging practices will be a key consideration in evaluating an organisation's overall cooperation, as well as considering any remediation efforts, and eligibility for leniency or reduced sanctions.

U.S. Agencies responsible for merger control have likewise underscored the importance of maintaining complete records during transactional review processes. Standard instructions in connection with in-depth inquiries now routinely require companies to identify and, where possible, produce business communications transmitted over ephemeral platforms.

The strong messages issued from U.S. authorities are echoed by their European colleagues, though perhaps at a lower volume, emphasising that digital evidence may be collected from any source, regardless of perceived privacy settings or default retention limitations. In the context of unannounced inspections and forensic data collection, they have made it clear that no platform is beyond the reach of enforcement.

The approach of the FCA (Financial Conduct Authority) has been quite diplomatic. Initially the FCA raised the issue of employees using systems such as WhatsApp back in January 2021:

"… Use of such apps can present challenges and significant compliance risks, since firms will be less able to effectively monitor communications using these channels. … Firms will need to ensure that, if such apps are used for in-scope activities on business devices, they are recorded and auditable."[13]

In the same announcement it was noted that action had been taken by the FCA against "individuals and firms for misconduct which involved the use of WhatsApp and other social media platforms." Despite raising their concerns not much further action has been taken, though it is clear that the FCA are discussing these points and the importance of ensuring relevant communication data is maintained with City firms. A number of discussions between the regulator and their regulated firms discussing the use of off-channel and ephemeral messaging have been reported by Financial News, for example.[14]

The CMA (Competition and Markets Authority) has set out their expectations regarding the automated destruction of documents - the Digital Markets Competition Regime Guidance explains that:

"The CMA is unlikely to regard automatic destruction of relevant documents under such a programme as a 'reasonable excuse' for the purposes of any penalty that might be applicable for failure to comply with the duty to preserve information."[15]

11 https://www.proskauer.com/pub/doj-messaging-app-warnings-undermine-trust-in-counsel.

12 https://www.sec.gov/files/litigation/opinions/2025/34-102860.pdf.

13 https://www.fca.org.uk/publications/newsletters/market-watch-66.

14 https://www.fnlondon.com/articles/fca-prepares-fresh-probe-into-bankers-encrypted-messaging-use-638b421c.

15 https://assets.publishing.service.gov.uk/media/6762f4f6cdb5e64b69e307de/Digital_Markets_Competition_Regime_Guidance.pdf.

The CMA are also reportedly expected to utilise additional powers which have been granted to them under the DMCCA (Digital Markets, Competition and Consumers Act). As stated by Mayer Brown in an article for "ThoughtLeaders4 Competition":

> *"During an antitrust inspection, the CMA now has the power to access to data, including digital data, "accessible from the premises" under investigation (as opposed to "on" those premises)… The DMCCA also imposes more extensive obligations on business to preserve potentially relevant evidence, including ephemeral messages.*
> *A new duty to preserve documents (including electronic documents and digital communications) is triggered under the DMCCA where a person knows or suspects that an investigation is being, or is likely to be, carried out by the CMA. Ephemeral messages are, in principle, within the scope of this wide duty, raising practical challenges for business when formulating appropriate document preservation policies."*[16]

The CMA also have additional powers with regard to fines. As noted in their April 2025 press release:

> *"Failure to provide information when requested (without a legitimate reason), concealing evidence, or providing false information can likewise result in a fine, with penalties of up to 1% of a business' global turnover and additional daily penalties."*[17]

In certain investigations, authorities have reportedly discovered that senior personnel engaged in sensitive or potentially unlawful conduct using encrypted messaging services. In June 2024, the European Commission issued a €15.9 million fine to International Flavors & Fragrances when a custodian was found to be deleting WhatsApp messages while a dawn raid at the premises was ongoing.[18] While not directly relating to ephemeral communications, this does demonstrate that the European regulators are taking the deletion of chat data particularly seriously. It has been made clear that a failure to properly preserve or disclose such communications can lead to increased penalties or be treated as an aggravating factor reflecting poor corporate governance.

IV. LEGAL AND PROCEDURAL RISKS

The use of ephemeral messaging during the course of an antitrust investigation, or even during the period in which an investigation could be reasonably anticipated, can trigger serious legal consequences. In jurisdictions like the U.S. and Europe, destruction of potentially relevant evidence can give rise to spoliation sanctions. Courts may impose adverse inference instructions, monetary sanctions, or even dismissal in extreme cases. If ephemeral messaging apps are used in a manner that bypasses data retention policies or legal holds, companies and individuals may face obstruction charges.

From a personal accountability perspective, executives or employees who deliberately use ephemeral messaging to hide anticompetitive conduct may be prosecuted individually. Regulators are increasingly adept at identifying messaging patterns and device usage that suggest efforts to evade detection.

From a discovery standpoint, ephemeral messaging creates unique difficulties in preservation, collection, processing, review, and production. Once messages disappear, they're often unrecoverable, particularly where device backups have been disabled or messages were never saved. This complicates legal hold implementation, especially in fast-moving investigations where data may vanish before action can be taken.

Organizations must also grapple with mobile device limitations. Unless a company has robust device control and monitoring policies in place, it may be practically impossible to preserve data from personal or BYOD ("bring your own device") environments.

Even when messages are still present, collecting data from encrypted apps can require complex workflows:

- Device imaging (with proper consent or legal authority)
- Use of specialised forensic tools and methodologies to decrypt or extract application data

16 https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2025/02/the-vanishing-point---antitrust-risks-raised-by-ephemeral-messages.pdf.

17 https://www.gov.uk/government/news/cma-to-boost-consumer-and-business-confidence-as-new-consumer-protection-regime-comes-into-force.

18 See for example https://www.linklaters.com/en/insights/blogs/linkingcompetition/2024/july/hold-the-phone-antitrust-authorities-looking-closely-at-instant-messages-in-dawn-raids.

These methods can be time-consuming, expensive, and incomplete, especially where users leverage multiple apps or delete content selectively. Ephemeral messaging apps may store data in non-standard formats, complicating ingestion into review platforms. Additionally, conversations are often fragmented, lacking consistent metadata or thread structure.

From a review standpoint, ephemeral communications may require contextual analysis to understand short, coded, or informal exchanges, particularly in cartel or collusion contexts. Moreover, reviewers must remain alert to patterns that suggest selective message deletion or use of parallel communication channels.

Based on the approaches of regulatory enforcement discussed, if you are responding to, or assisting with the response to regulatory requests, you may need to consider investigating if employees have been utilising off-channel or ephemeral messaging systems. Alternatively, if there are suggestions that custodians may be using such applications, you may need to consider what methodologies are available to you to investigate and confirm.

There are various ways that you can explore such potential usage of off-channel and ephemeral applications. Overall, the main methodologies from a technical perspective split into two main areas – digital forensic approaches, and eDiscovery approaches.

The digital forensic approaches involve looking into system data, rather than looking at user generated content. This may involve inspecting settings stored on a custodian's mobile device, for example. Forensic approaches are usually more focussed than eDiscovery approaches. They are likely to be performed on a per custodian basis, since they involve digging into very specific data sets.

eDiscovery approaches by comparison are typically approaches which can be utilized by using a review platform after data collected from the various custodians has been processed and indexed for search, analysis and review.

In the sections below, we discuss some of the different methodologies for investigating the potential usage of off-channel or ephemeral messaging. This is not an exhaustive list, but an indication of some of the approaches that can be taken to shine a light on the usage of messaging systems.

V. INVESTIGATING EPHEMERAL/OFF-CHANNEL MESSAGING USAGE

A. Data Collection/Preservation

It is key when performing investigation work to ensure that data is collected using a method that allows you to perform the analysis needed down the road. For example, if performing a targeted collection of data from specific folders from a custodian machine, it will not be possible to recover deleted data in future. To do this you would need to take a forensic image of the machine.

Similar considerations are in play for data from mobile devices – the main source when looking for messaging applications. There are several different ways to collect data from mobile devices and not all methods will preserve data from messaging applications which are designed with security and privacy in mind. Typically, forensic professionals would want to collect what are known as "Full File System" collections, which are the most complete type of collection possible. Unfortunately, these collections often require the use of exploits to gain access to the data. This means that they may not always be available. Care should be taken when such collections are not available that data from messaging applications is not missed to ensure that potential data sets are not lost from the investigation.

B. Digital Forensic Approaches

Investigators could rely on some or all of the following techniques:

- Installed Software Lists – It will often be possible to parse and interpret information from various system-based databases and storage. This can include lists of installed applications, or a history of application installations, which can then be checked for known messaging systems, even if they have been subsequently deleted from the device.
- Application Access Lists – It may not be easy to identify messaging applications from a list of all installed applications, especially if an unusual or esoteric application is in use. One way to focus this down can be to look at the access that different application have. Often messaging applications will have access to the contacts database (to store and access contacts) and also to photos taken on the device (in order to share them). Using access databases can be a useful way to focus down on those that may be messaging application when a large number of applications are present.

- Password Management and Browser Saved Password analysis– If a password manager system is in use, then it may be possible to check the entries in the manager to identify if there are usernames and/or passwords present for messaging applications. If users have chosen to save passwords (for example within their internet browsers) then the browser information could hold similar information which can be investigated to identify usage of messaging systems.
- Internet History – A users internet history can be checked for various factors which could imply the usage of ephemeral chat systems. For example, looking for reviews of ephemeral messaging, searching for messaging systems where data can be deleted, or searching for guides on how to set the deletion of messages.
- GenAI History – Similar to internet history, searching a users ChatGPT, or other generative AI application logs for details of what they have been asking can identify evidence of ephemeral messaging. For example, they could ask generative AI which messaging system is best for deletion of messages, ask for assistance on deletion settings, or asking how they can stop regulators or investigators from accessing their data.

C. eDiscovery Approaches

The following eDiscovery methods would similarly assist in retrieving relevant data:

- Common application searches – though a simple approach, it can be very helpful to run searches across a review set for ephemeral messaging application names such as Telegram, Signal, WeChat, Dust etc. and it can be helpful to maintain a list of such application for this purpose. This can turn up message such as "Let's discuss this on Signal" which can be smoking gun evidence that such messaging systems were in use. However, it is not just such direct references that may be useful. Indirect references can also be helpful, such as invoices for paid apps, 2FA confirmations or login notifications.
- Filtering Care – For the above reason care should be taken when performing processing and filtering to ensure that messages such as the above (which may be dated outside of the main date range) can be searched. There may be a need to balance the need for a proportionate approach with the risk of missing information that may be useful.
- GenAI Prompting – In addition to basic approaches such as keyword searches, Generative AI prompts could be used to search for information suggesting an intent to use or move existing communications to an ephemeral or off-channel application.

D. Best Practices for Companies

To mitigate the legal and procedural risks associated with ephemeral messaging, organizations should adopt a multifaceted approach that combines policy, training, technology, and compliance oversight. Companies should develop or revise their policies to clearly address the use of ephemeral messaging tools. At a minimum, such policies should:

- Prohibit use of ephemeral messaging for business communications (particularly those involving sensitive or regulated matters)
- Identify approved communication platforms
- Require retention and auditability of business messages
- Apply consistently across all jurisdictions and business units

If employees are permitted to use personal devices for work, organizations should implement controls to ensure compliance:

- Require installation of enterprise-grade messaging apps with retention capabilities
- Leverage device management tools to enforce encryption, backups, and app restrictions
- Establish clear procedures for device imaging and data recovery, where necessary

Legal and compliance teams must ensure that legal hold procedures are triggered promptly upon awareness of potential antitrust exposure. This includes:

- Communicating with custodians about suspending auto-deletion settings
- Capturing messages before they are automatically erased
- Coordinating with IT and forensic experts to preserve relevant data sources

Companies should conduct regular audits to ensure compliance with messaging policies and identify rogue usage of unapproved apps. This may include:

- Reviewing network logs for downloads or use of encrypted apps
- Conducting interviews or surveys about messaging habits
- Monitoring for signs of data loss or off-channel communication

E. The Role of In-House Counsel and eDiscovery Teams

In-house legal teams and their external counsel must work closely with IT and compliance professionals to develop practical protocols for managing ephemeral messaging risks. This includes:

- Staying abreast of evolving regulatory expectations
- Coordinating cross-border data preservation and production
- Advising executives and custodians on acceptable communications
- Preparing to explain limitations and efforts to regulators during investigations

eDiscovery service providers and forensic experts also play a critical role in identifying data sources, executing collections, and advising on feasibility of recovery. Early consultation with these experts can help avoid missteps and build credibility with enforcement authorities.

VI. LOOKING AHEAD: REGULATORY EVOLUTION AND INDUSTRY RESPONSE

We can expect further enforcement activity and regulatory guidance on ephemeral messaging in the near future. Key trends likely to shape this area include:

- Increased regulator cooperation: Especially in cross-border cartel cases, authorities are likely to share investigative techniques and expectations for data recovery.
- More dawn raids and device inspections: As digital raids become more sophisticated, regulators may target mobile devices, including personal phones, for forensic review.
- Potential legislation: Some jurisdictions may seek statutory authority to mandate retention of certain business communications or restrict the use of ephemeral features in corporate contexts.
- Emerging case law: Courts will continue to define the scope of spoliation liability and cooperation obligations in the context of disappearing messages.

Industry groups may also develop standards for acceptable use of messaging tools and minimum retention requirements in regulated sectors.

Ephemeral messaging poses significant risks and challenges in antitrust investigations. While these tools offer legitimate privacy and usability benefits, their unregulated or careless use can undermine legal obligations, frustrate investigations, and result in harsh penalties. Regulators have made clear that ignorance or inaction will not suffice, companies must take proactive steps to ensure transparency, auditability, and preservation of relevant business communications.

Legal teams, compliance officers, and eDiscovery professionals must work together to build a defensible, scalable approach to managing ephemeral messaging and off-channel communications. By addressing policy gaps, leveraging technology, and preparing for potential scrutiny, organizations can navigate this evolving risk landscape while maintaining operational agility.

CPI COMPETITION POLICY® INTERNATIONAL

CPI Subscriptions

CPI reaches more than 35,000 readers in over 150 countries every day. Our online library houses over 23,000 papers, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.