THE VANISHING POINT

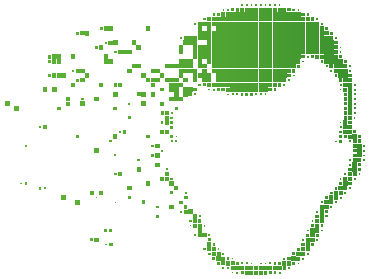
ANTITRUST RISKS RAISED BY EPHEMERAL MESSAGES

Authored by: Daniel Vowden (Partner), Kathryn Lloyd (Senior Associate), Sarah Wilks (Knowledge Counsel) & Megan Stride (Associate) - Mayer Brown

Ephemeral messaging is a form of multimedia digital communication characterised by the automatic disappearance of messages after receipt. The ubiquity of ephemeral messaging, including through popular software applications such as SnapChat, WhatsApp, Telegram and Signal, is increasingly a cause of concern among competition authorities.

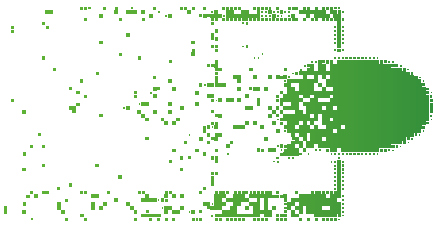
Cartels are characteristically conducted in secret. Ephemeral messaging, which in addition to automated deletion also typically offers end-to-end security encryption, provides an ideal means for secret collusion.

In 2024, the European Commission imposed a €15.9 million fine for the deletion of incriminating WhatsApp messages during an antitrust inspection.



Notwithstanding this fine, the European Commission has yet to issue guidance or otherwise significantly amend its investigatory practices to address ephemeral messaging. In January 2025, the UK Competition and Markets Authority ("CMA") gained new investigatory powers under the Digital Markets, Competition and Consumers Act ("DMCCA"). These powers, intended to be "fit for purpose" in a digital world, provide the agency with means to target ephemeral messaging in antitrust investigations. The DMCCA also places more extensive obligations on businesses to preserve evidence, including ephemeral messages.

In the United States, the Department of Justice ("DoJ") and the Federal Trade Commission ("FTC") have gone further, issuing specific guidance to businesses on the treatment of ephemeral messages, particularly around appropriate document preservation practices.



1. New CMA Powers Target Ephemeral Messages

The CMA, like competition authorities across Europe, employs sophisticated tools to collect audio files, emails, text messages and instant messages during antitrust investigations. Historically, however, a "gap" arguably existed in relation to ephemeral messaging, with technology evolving at a faster pace than agency practice.

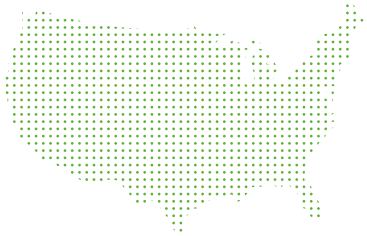
The DMCCA looks to address this gap. It confers on the CMA extensive new investigatory powers that better reflect contemporary working practices.

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). This applies to searches both of domestic and company premises. Additionally, the CMA can now require production of passwords, encryption keys and assistance from employees in identifying and accessing remotely stored digital documents. This brings ephemeral messages, including messages accessible via personal devices used for business purposes, within the scope of the CMA's search powers.

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. The CMA's Guidance on Investigation Procedures in Competition Act 1998 Cases (CMA8) expressly notes that "[t]he CMA is unlikely to regard automatic destruction of relevant documents following a business' document retention policy as a 'reasonable excuse'...".

Reforms under the DMCCA mean that intentional or negligent obstruction of investigations - including destruction of or tampering with relevant evidence - carry significant penalties in the UK. Businesses are now at risk of fixed penalties of up to 1% of global turnover (with fixed penalties formerly limited to amounts not exceeding £30,000).



2. Learnings from the US

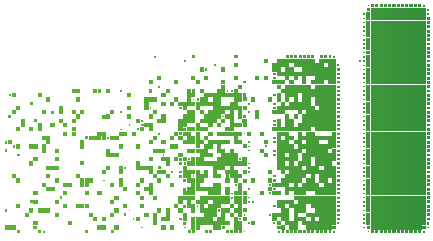
In 2023, the DOJ announced[1] a number of updates to its guidance covering its Criminal Division's Evaluation of Corporate Compliance Programs that targeted ephemeral messaging.

The DOJ explained that it would consider the extent to which a company's policies on ephemeral messaging are tailored to particular risks and needs, as well as whether those policies adequately ensure that such communications can be preserved and accessed. If a company under investigation does not produce communications from third-party messaging platforms, DOJ prosecutors will ask questions, and a lack of answers could affect how the DOJ assesses a company's cooperation efforts.

The DOJ Antitrust Division struck a similar tone in November 2024 when it updated its guidance explaining how it evaluates companies' antitrust compliance programs. In that context, the Antitrust Division will consider what "electronic communication channels" are permitted under company policies, how the company has attempted to manage and preserve ephemeral messaging and other information within those channels, and the company's rationale for any preservation or deletion settings it permits. The Antitrust Division will look at how companies communicate these policies to employees as well.

The FTC has observed that companies risk civil or criminal sanctions if they fail to preserve ephemeral messages when they were obliged to do so. In those contexts, companies should turn off any automatic deletion settings, and may even need to stop the use of certain applications altogether.

Both the DOJ and FTC have also acknowledged that using ephemeral messaging can increase the likelihood that personal devices fall in the scope of an inquiry.



3. Key takeaways

Reforms under the DMCCA, effective 1 January 2025, substantially bolster the CMA's ability to target ephemeral messages during antitrust investigations. Digital evidence, including ephemeral messages, are regarded as a key source of evidence in antitrust investigations.

Firms that are under investigation should take steps to preserve documents early on in an investigation by implementing a "litigation hold" on all relevant data. In practice, firms may need to navigate challenges on this front including in relation to technical limitations and privacy concerns. In the UK, the DMCCA requires this step to be taken once a person "knows or suspects that an investigation… is being, or is likely to be, carried out" by the CMA. Where possible, such "litigation holds" should set out as a key priority the disabling of auto-delete features of ephemeral messaging apps.

Organisations will need to be ready to explain their document preservation policies. A proportionate balance will need to be struck between a business's need to retain documents for only limited periods versus its legal obligations to cooperate during inspections.

In the absence of specific guidance from the CMA, much can be learned from the best practices advocated by the DoJ and FTC. In devising antitrust compliance policies, companies would be well-advised to consider how precisely ephemeral messaging is treated and what specific safeguards should be adopted, balancing commercial imperatives with legal risks. Effective training and the dissemination of guidance to employees is of paramount importance, as a means to avoid wrongdoing in the first instance and to ensure retention policies accord with employee practices and can therefore withstand scrutiny during an antitrust investigation.

1 https://www.mayerbrown.com/en/insights/publications/2023/03/dojs-criminal-division-announces-further-updates-to-doj-policy-on-key-topics-ephemeral-messaging-compensation-clawbacks-and-selection-of-corporate-monitors