ALERT MEMORANDUM

US Antitrust Regulators Threaten Ephemeral Messaging Users and Their Counsel with Obstruction Charges

June 7, 2024

In recent months, federal regulators have made statements that companies and their counsel may be subject to criminal prosecution if they fail to preserve ephemeral messaging data when they receive a subpoena or other legal process. In January 2024, the Deputy Assistant Attorney General for Criminal Enforcement at the DOJ Antitrust Division warned "failure to produce" ephemeral messaging may result in obstruction charges.[1] Speaking at the ABA Antitrust Spring Meeting in April 2024, a lawyer for the Antitrust Division echoed that the DOJ "will not hesitate to bring obstruction charges" against company counsel and their clients if clients fail to properly retain so-called "ephemeral messages."[2] This is consistent with other recent warnings from the DOJ.[3]

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors

WASHINGTON

Jeremy Calsyn
+1 202 974 1522
jcalsyn@cgsh.com

Nowell Bamberger
+1 202 974 1752
nbamberger@cgsh.com

Charles P. Balaan
+1 202 974 1725
cbalaan@cgsh.com

NEW YORK

Joseph M. Kay
+1 212 225 2745
jkay@cgsh.com

The agencies' focus on features of ephemeral messaging, which they argue can be used to hamper investigations, ignores the fact that ephemeral messaging applications have a legitimate role in the workplace where data security and management is paramount. Despite the advantages of ephemeral messaging, clients should be aware of the legal and other risks presented by these applications and implement clear information retention policies that account for the organization's duty to preserve information for litigation and government investigations.

[1] Press Release, U.S. Dep't of Justice, Justice Department and the FTC Update Guidance that Reinforces Parties' Preservation Obligations for Collaboration Tools and Ephemeral Messaging (Jan. 26, 2024), https://www.justice.gov/opa/pr/justice-department-and-ftc-update-guidance-reinforces-parties-preservation-obligations.

[2] Khushita Vasant, Antitrust counsel vulnerable to prosecution for obstruction if clients improperly delete ephemeral messages, DOJ official says, MLex (Apr. 11, 2024), https://mlexmarketinsight.com/news/insight/antitrust-counsel-vulnerable-to-prosecution-for-obstruction-if-clients-improperly-delete-ephemeral.

[3] *See*, *e.g.*, Khushita Vasant, Ephemeral messaging requests 'big deal' for US FTC in merger reviews, Liu says, MLex (Apr. 18, 2024), https://mlexmarketinsight.com/news/insight/ephemeral-messaging-requests-big-deal-for-us-ftc-in-merger-reviews-liu-says.

I. Recent Statements About Ephemeral Messaging

Ephemeral messaging applications allow users to send and receive messages that are automatically and irretrievably deleted after certain conditions (e.g., the message has been viewed or after a set period of time). Popular examples of applications with ephemeral messaging features include Signal, Telegram, and WhatsApp. These applications typically combine the automatic deletion feature with end-to-end ("E2E") encryption, a secure communication process that limits third-party access. Ephemeral messaging offers obvious security, data management, and privacy advantages in the corporate context. Automatic deletion and E2E encryption facilitate compliance with data protection laws such as the EU's General Data Protection Regulation ("GDPR") that have data minimization and storage limitation requirements. Automatic deletion also helps organizations manage the immense volume of data they generate daily and limits the amount of data that could be compromised in the event of a breach. Because of these benefits, workplaces across the world are implementing use of ephemeral messaging applications.

In January 2024, the Antitrust Division and the FTC announced that the agencies were updating their standard language in preservation letters "to address the increased use of collaboration tools and ephemeral messaging platforms in the modern workplace."[4] The announcement quoted Deputy Assistant Attorney General Manish Kumar of the Antitrust Division: "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."[5] In April 2024, speaking at the ABA Antitrust Spring Meeting, a counsel with the Antitrust Division told the audience that "it's up to you all to find a way to preserve those [messages] if they are responsive to a subpoena," and indicated that if responsive ephemeral messages are deleted, the Antitrust Division would "not hesitate to bring obstruction charges, and . . . 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."[6]

II. Obligations to Preserve and Obstruction of Justice

In civil litigation, the duty to preserve attaches when litigation is pending or reasonably foreseeable.[7] Once the duty attaches, parties must make reasonable efforts to preserve information that is relevant to the anticipated litigation.[8] In federal court, Federal Rule of Civil Procedure 37(e) governs the failure to preserve electronically stored information ("ESI") if the ESI "is lost because a party failed to take reasonable steps to preserve it." If a party is prejudiced by such a loss of ESI, Rule 37(e) permits a court to "order measures no greater than necessary to cure the prejudice."[9] The most

[4] Press Release, U.S. Dep't of Just., Justice Department and the FTC Update Guidance that Reinforces Parties' Preservation Obligations for Collaboration Tools and Ephemeral Messaging (Jan. 26, 2024), https://www.justice.gov/opa/pr/justice-department-and-ftc-update-guidance-reinforces-parties-preservation-obligations.

[5] *Id.*

[6] Vasant, *supra* note 2.

[7] *Micron Tech., Inc. v. Rambus Inc.*, 645 F.3d 1311, 1320 (Fed. Cir. 2011).

[8] FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment ("This rule recognizes that "reasonable steps" to preserve suffice; it does not call for perfection.").

[9] FED. R. CIV. P. 37(e)(1); Sanctions under Rule 37(e)(1) can vary, but sometimes include the payment of attorney's fees or the party being prohibited from making certain arguments. *See*, *e.g.*, *Charlestown Cap. Advisors, LLC v. Acero Junction, Inc.*, 2021 WL 1549916 at *1 (S.D.N.Y. 2021) (finding a violation of Rule 37(e)(1) and precluding the party responsible from denying receipt of the relevant ESI, authorizing affected party to present evidence to the jury concerning deletion of ESI, and ordering the responsible party to pay attorney's fees).

serious sanctions, the presumption that the lost information was unfavorable to the responsible party, adverse jury instructions, and default judgments against the spoliating party, are only available under Rule 37(e) if the party "acted with the intent to deprive another party of the information's use in the litigation."[10]

Criminal federal obstruction statutes address a broad range of conduct that impedes governmental activities. This includes witness tampering, witness retaliation, and destruction or falsification of evidence. Thus, deletion of ESI with the intent to hinder an investigation can be a criminal offense. For example, 18 U.S.C. § 1519, provides that:

> Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than 20 years, or both.[11]

Although the federal rules and obstruction statutes prohibit spoliation, alteration, falsification, or destruction of evidence, there is not a general duty to *create* records. For example, parties are ordinarily not required to record phone calls, even if the discussion is relevant to a litigation or investigation. However, they may be required to retain relevant voicemails that are created.

In certain regulated industries, there are additional record keeping requirements. SEC Rule 17a-4 requires certain securities exchange members, brokers, and dealers to retain records of "all communications received and copies of all communications sent . . . by the member, broker or dealer (including inter-office memoranda and communications) relating to its business as such."[12] The Commodity Futures Trading Commission's Rule 23.202 similarly requires swap dealers and major swap participants to retain certain trading information and records, including "communications provided or received concerning quotes, solicitations, bids, offers, instructions, trading, and prices, that lead to the execution of a swap, whether communicated by telephone, voicemail, facsimile, instant messaging, chat rooms, electronic mail, mobile device, or other digital or electronic media." These rules have been at the center of numerous enforcement actions against financial services firms with more than $2 billion in total fines levied to date.[13]

III. Implications for Clients

Using ephemeral messaging without preserving the messages while subject to litigation hold or subpoena carries risk. Companies should be aware of the risks ephemeral messaging carries in regulatory investigations and civil litigation. Courts have held that organizations and individuals subject to preservation obligations that fail to disable auto-delete settings could face monetary penalties.[14] In some cases courts may

[10] FED. R. CIV. P. 37(e)(2).
[11] *See United States v. Katakis*, 800 F.3d 1017, 1023 (9th Cir. 2015) (reviewing a district court's vacatur of an obstruction conviction under § 1519 for deleting incriminating emails during a bid rigging investigation).
[12] 17 CFR § 240.17a-4(a).
[13] *See*, *e.g.*, Press Release, U.S. Sec. & Exch. Comm'n, SEC Charges 16 Wall Street Firms with Widespread Recordkeeping Failures (Sept. 27, 2022), https://www.sec.gov/news/press-release/2022-174; Press Release, Commodity Futures Trading Comm'n, CFTC Orders 11 Financial Institutions to Pay Over $710 Million for Recordkeeping and Supervision Failures for Widespread Use of Unapproved Communication Methods (Sept. 27, 2022), https://www.cftc.gov/PressRoom/PressReleases/8599-22; Press Release, U.S. Sec. & Exch. Comm'n, SEC Charges 11 Wall Street Firms with Widespread Recordkeeping Failures (Aug. 8, 2023), https://www.sec.gov/news/press-release/2023-149.
[14] *See*, *e.g.*, *Nacco Materials Handling Grp., Inc. v. Lilly Co.*, 278 F.R.D. 395, 404, 407 (W.D. Tenn. 2011) (finding sanctions warranted where defendant "failed to timely issue an effective written litigation hold, to take appropriate steps to preserve any existing electronic records, to suspend or alter automatic delete features and routine overwriting features, and to timely and effectively collect ESI").

permit a litigant to present evidence and argument that an adverse party's use of ephemeral messaging explains why the litigant failed to turn up more evidence in discovery.[15]

Starting the use of ephemeral messaging in the middle of a litigation or investigation carries even more risk: courts and regulators are more likely to infer an inappropriate intent when key custodians begin using ephemeral messaging applications after they become aware of an investigation or lawsuit.[16] Ephemeral messaging also carries risk because even completely innocent use may raise suspicions in the eyes of regulators, courts, and the public.

Use of ephemeral messaging may also complicate the merger clearance process. The FTC's Model Second Request defines ephemeral messages as communications sent through messaging applications as documents.[17] Regulators may take the position that parties to a Second Request have not complied with their preservation and production obligations if ephemeral messages are not preserved. To mitigate these risks, companies should consult with counsel early on in the process, to provide guidance to employees in connection with legal holds and the retention of all relevant documents.

As a general matter, organizations and employees should also be aware of the risks related to the use of personal devices for work communication. Companies with a "bring your own device" (or "BYOD") policy allow or require employees to conduct company business on their personal devices. Courts have found that ESI on employees' personal devices is discoverable when subject to a BYOD policy that gives an employer the right to access content on the device.[18] Organizations should consult with counsel and consider whether personal devices are discoverable or should be subject to litigation holds.

Merely not preserving ephemeral messaging should not be enough to support a criminal obstruction charge. The recent statements made by Antitrust Division officials threatening companies and counsel with obstruction of justice for not preserving ephemeral messaging ignore that federal criminal obstruction of justice statutes all require a showing of intent.

Section 1519 was "intended to prohibit, in particular, corporate document-shredding to hide evidence of financial wrongdoing."[19] It has been interpreted broadly: the government is not required to prove a nexus between the defendant's conduct and an official proceeding,[20] or even that the document was material to any investigation.[21] But the government is still required to prove that the defendant acted "with the intent to impede, obstruct, or influence" an actual or contemplated investigation.[22] Merely using ephemeral messaging applications, without other evidence of obstructive intent, is not sufficient to satisfy the intent element. Despite the DOJ's suggestion that ephemeral messaging is "designed to hide evidence," ephemeral

[15] *See*, *e.g.*, *Waymo LLC v. Uber Techs., Inc.* 2018 WL 646701, at *21 (N.D. Cal. Jan. 30, 2018).

[16] *See FTC v. Noland,* 2021 WL 3857413 (D. Ariz. Aug. 30, 2021) ("The most decisive factor [in determining Defendants acted with intent to deprive the FTC of information] is the timing of the installation and use of Signal and ProtonMail. The Individual Defendants installed these apps . . . one day after [Defendant] discovered the FTC was investigating him and SBH.").

[17] Model Second Request, Federal Trade Commission (Jan. 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/Final-Rev-Model-Second-Request-01-26-2024.pdf

[18] *See H.J. Heinz Co. v. Starr Surplus Lines Ins. Co.*, 2015 WL 12791338 (W.D. Pa. July 28, 2015); *but see In re Pork Antitrust Litig.*, 2022 WL 972401 at *4–*5. (D. Minn. Mar. 31, 2022) (finding a company did not have possession, custody, or control over employee text messages on personal devices subject to a BYOD policy that permitted the company to delete all data from the device).

[19] *Yates v. United States*, 574 U.S. 528, 536 (2015).

[20] *See United States v. Gray*, 642 F.3d 371, 377–78 (2d Cir. 2011) ("Thus, in enacting § 1519, Congress rejected any requirement that the government prove a link between a defendant's conduct and an imminent or pending official proceeding.").

[21] *United States v. Yielding,* 657 F.3d 688, 712 (8th Cir. 2011) (stating that an attempt to obstruct an investigation, even if unsuccessful because the document was unimportant, could constitute a violation of § 1519).

[22] *See United States v. Kernell*, 667 F.3d 746 (6th Cir. 2012). Alternative obstruction statutes also have intent elements that are at least as demanding as the intent element in Section 1519. *See*, *e.g.*, 18 U.S.C. § 1512(c); 18 U.S.C. § 1505.

messaging applications have innocent and practical applications in the workplace and roles to play in an organization. And courts have not required in all cases the retention of all documents for an unlimited time. As the Federal Circuit explained in the analogous civil discovery context, "where a party has a long-standing policy of destruction of documents on a regular schedule, with that policy motivated by general business needs, . . . destruction that occurs in line with the policy is relatively unlikely to be seen as spoliation."[23]

Aside from the intent element, it is far from clear that communicating using ephemeral messages would satisfy the element that the individual "knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object." Charges brought under Section 1519 generally involve deliberate manual destruction or deletion of evidence. Electing to communicate using ephemeral messaging (without having the ability to retain messages) is arguably more like the choice to make a phone call over sending an email. Although a phone conversation may include a discussion relevant to a litigation or investigation, there is no general duty to record phone calls.

Even if a company fails to implement a legal hold process sufficient to retain relevant ephemeral data, the government would, at a minimum, have to prove the inadequate system was implemented with obstructive intent. If there is no evidence of obstructive intent, an obstruction charge should not succeed against the company or its antitrust counsel.

IV. Conclusion

Ephemeral messaging applications have important roles to play in a world where data security and management is paramount for both organizations and individuals. Despite the advantages of ephemeral messaging, clients should be aware of the legal and other risks presented by these applications and implement clear information retention policies that account for the organization's duty to preserve information for litigation and government investigations. Federal law forbids the destruction or deletion of documents and information with the intent to deprive regulators or litigants of evidence, but criminal penalties should not be available where ESI such as ephemeral messages are deleted pursuant to a good-faith information retention policy.

…

CLEARY GOTTLIEB

[23] *Micron*, 645 F.3d 1322; *see also Arthur Andersen LLP v. United States*, 544 U.S. 696, 704 (2005) ("It is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under ordinary circumstances.") (ruling on jury instructions in a federal obstruction of justice conviction under 18 U.S.C. § 1512(b)(2)(A) and (B)).