

The Sedona Conference

Commentary on Ephemeral Messaging



The Sedona Conference Commentary on Ephemeral Messaging

The Sedona Conference



Recommended Citation:

The Sedona Conference, *Commentary on Ephemeral Messaging*, 22 SEDONA CONF. J. 435 (2021).

Copyright 2021, The Sedona Conference

For this and additional publications see: <https://thesedonaconference.org/publications>

THE SEDONA CONFERENCE COMMENTARY
ON EPHEMERAL MESSAGING

*A Project of The Sedona Conference Working Group on International
Electronic Information Management, Discovery, and Disclosure
(WG6)*

Author:

The Sedona Conference

Editor-in-Chief:

Philip J. Favro

Contributing Editors:

Bennett Arthur

Starr Turner Drum

Stacey Blaustein

David K. Gaston

Oliver Brupbacher

Alan Geolot

Guillermo Santiago Christensen

Jennifer L. Joyce

Andrea D'Ambra

Agnieszka McPeak

Robert DeCicco

Hon. Anthony E. Porcelli

Steering Committee Liaisons:

Denise E. Backhouse

Wayne Matus

Taylor Hoffman

Staff Editors:

David Lumia

Michael Pomarico

Copyright 2021, The Sedona Conference.
All Rights Reserved.

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 6. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any other organizations to which any of the participants belong, nor do they necessarily represent official positions of The Sedona Conference.

We thank all of our Working Group Series Annual Sponsors, whose support is essential to our ability to develop Working Group Series publications. For a listing of our sponsors, just click on the “Sponsors” navigation bar on the homepage of our website.

This publication may be cited as follows:

The Sedona Conference, *Commentary on Ephemeral Messaging*, 22 SEDONA CONF. J. 435 (2021).

PREFACE

Welcome to the July 2021 final version of The Sedona Conference *Commentary on Ephemeral Messaging* (“*Commentary*”), a project of The Sedona Conference Working Group 6 on International Electronic Information Management, Discovery, and Disclosure (WG6). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, intellectual property rights, and data security and privacy law. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The mission of WG6 is to develop principles, guidance and best practice recommendations for information governance, discovery and disclosure involving cross-border data transfers related to civil litigation, dispute resolution and internal and civil regulatory investigations.

The Sedona Conference acknowledges Editor-in-Chief Phil Favro for his leadership and commitment to the project. We also thank Contributing Editors Bennett Arthur, Stacey Blaustein, Oliver Brupbacher, Guillermo Christensen, Andrea D’Ambra, Robert DeCicco, Starr Drum, David Gaston, Alan Geolot, Jennifer Joyce, Professor Agnieszka McPeak, and Judge Anthony Porcelli for their efforts, and Denise Backhouse, Taylor Hoffman, and Wayne Matus for their guidance and input as Steering Committee liaisons to the drafting team. We also thank Natascha Gerlach for her contributions.

In addition to the drafters, this nonpartisan, consensus-based publication represents the collective effort of other members of WG6 who reviewed, commented on, and proposed edits to early drafts of the *Commentary* that were

circulated for feedback from the Working Group membership. Other members provided feedback at a WG6 meeting where drafts of this *Commentary* were the subject of the dialogue. The publication was also subject to a period of public comment. On behalf of The Sedona Conference, I thank both the membership and the public for all of their contributions to the *Commentary*.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG6 and several other Working Groups in the areas of electronic document management and discovery, data security and privacy liability, international data transfers, patent litigation, patent remedies and damages, and trade secrets. The Sedona Conference hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law, both as it is and as it should be. Information on membership and a description of current Working Group activities is available at <https://thesedonaconference.org/wgs>.

Craig Weinlein
Executive Director
The Sedona Conference
July 2021

TABLE OF CONTENTS

| | | |
|------|---|-----|
| I. | INTRODUCTION..... | 441 |
| II. | EPHEMERAL MESSAGING—NATURE AND SCOPE | 446 |
| | A. Automated Disposition of Message Content | 446 |
| | B. E2E Encryption | 447 |
| | C. Other Characteristics of Ephemeral Messaging..... | 449 |
| | 1. Purely Ephemeral Messaging | 449 |
| | 2. Quasi-Ephemeral Messaging | 451 |
| | 3. Non-Ephemeral Messaging..... | 452 |
| III. | TENSIONS ASSOCIATED WITH THE USE OF EPHEMERAL MESSAGING APPLICATIONS | 454 |
| | A. Benefits of Ephemeral Messaging..... | 454 |
| | 1. Organizational Benefits..... | 454 |
| | (a) Information Governance | 454 |
| | (b) Legal Compliance Support..... | 456 |
| | (c) Privacy by Design | 459 |
| | (d) Data Security..... | 460 |
| | (e) Productivity | 461 |
| | 2. Benefits to Individual Users | 462 |
| | B. Risks of Ephemeral Messaging | 464 |
| | 1. Regulatory Risks | 465 |
| | 2. Legal Risks | 468 |
| | 3. Operational Risks..... | 469 |
| IV. | GUIDELINES | 471 |
| | A. Guideline One: Regulators and Courts Should Recognize that Ephemeral Messaging May Advance Key Business Objectives | 471 |

- B. Guideline Two: Organizations Should Take
Affirmative Steps to Manage Ephemeral
Messaging Risks474
- C. Guideline Three: Organizations Should Make
Informed Choices and Develop Comprehensive
Use Policies for Ephemeral Messaging
Applications476
- D. Guideline Four: Regulators, Courts, and
Organizations Should Consider Practical
Approaches, Including Comity and Interest
Balancing, to Resolve Cross-Jurisdictional
Conflicts over Ephemeral Messaging.....480
- E. Guideline Five: Reasonableness and
Proportionality Should Govern Discovery
Obligations Relating to Ephemeral Messaging
Data in U.S. Litigation482

I. INTRODUCTION

Ephemeral messaging is increasingly used around the globe. With its ability to automate the deletion of content shared with others, ephemeral messaging offers organizations a robust option to strengthen aspects of their corporate information governance programs. This feature, combined with end-to-end encryption (“E2E encryption”) that enables secure communications, may also facilitate compliance with data protection and privacy laws. Indeed, these laws—including the European Union (EU) General Data Protection Regulation (GDPR)¹—are among the considerations driving organizations toward the use of ephemeral messaging.

Beyond these considerations are issues such as convenience and ease of use. Users find that by keeping discussions confidential, ephemeral messaging enhances their ability to collaborate and exchange information without significant information technology (IT) infrastructure. These collective factors make ephemeral messaging a potentially attractive communication option for organizations and their employees.

Despite the growing use of ephemeral messaging, there are concerns about its widespread adoption.² Government

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119/1), *available at* <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679#PP3Contents> [hereinafter GDPR]. GDPR is a single, binding, EU-wide regulatory framework that became effective on May 25, 2018.

2. The Council of the European Union recently renewed its consideration of a resolution regarding the use of encrypted messaging applications that attempts to balance the needs of data subjects for strong encryption against government security interests seeking access to

regulators at the U.S. Department of Justice (U.S. DOJ) and the U.S. Securities & Exchange Commission (U.S. SEC) worry that ephemeral messaging can lead to increased criminal activity such as bribery, fraud, and money laundering. The U.S. DOJ and the U.S. SEC have implemented policies that discourage organizational adoption of ephemeral messaging without careful consideration of their compliance obligations. While the U.S. DOJ recently modified its policy toward a potentially more accommodating view in the context of corporate compliance programs,³ the fact remains that certain government regulators around the world disfavor the use of ephemeral messaging absent strong corporate governance.⁴

Other complications related to the use of ephemeral messaging include the legal obligation in common law countries that parties preserve evidence for litigation. For example, civil litigation in U.S. federal and state courts generally requires that litigants (at a minimum) keep information relevant to the claims and defenses in a particular action. Once the common law duty to preserve attaches, use of

encrypted data. See Natasha Lomas, *What's all this about Europe wanting crypto backdoors?*, TECH CRUNCH (Nov. 9, 2020), <https://techcrunch.com/2020/11/09/whats-all-this-about-europe-wanting-crypto-backdoors/>.

3. See Section III.B.1, *infra*.

4. See, e.g., Financial Conduct Authority, *Newsletter on market conduct and transaction reporting issues* (Jan. 2021), <https://www.fca.org.uk/publications/newsletters/market-watch-66> (warning that encrypted messaging applications may enable regulated companies to circumvent mandatory recordkeeping obligations); Sarah Basford Canales, *Australia's Controversial Encrypted Messaging Laws, Explained*, GIZMODO (Aug. 7, 2020), <https://www.gizmodo.com.au/2020/08/assistance-and-access-law-encrypted-messaging-explained/> (discussing the status and impact of Australia's new encryption cracking law, which impacts the use of encrypted messaging applications).

ephemeral messaging may cause relevant data to be discarded, which could violate that duty.⁵

These and similar competing demands spotlight a clear tension that has created a quandary for organizations wishing to implement ephemeral messaging. In the face of that tension, organizations need direction on how they should address these competing demands. This is particularly the case for organizations seeking to use ephemeral messaging to comply with cross-border data protection directives without violating other legal requirements.

This tension is also apparent for government regulators and judges who have been tasked with evaluating an organization's efforts at compliance with a particular law or regulation. These decision-makers may be inclined to presume that ephemeral messaging is being used to prevent regulators, courts, litigation adversaries, or the public from obtaining critical information about the inside workings of an organization. A closer, more thorough inspection could provide a more balanced perspective, revealing that a corporate ephemeral messaging program is meritorious and designed to advance business objectives, including compliance with cross-border data protection regimes. Just as organizations could profit from guidance on the issues, regulators and courts may also benefit from direction on how

5. See *WeRide Corp. v. Kun Huang*, No. 5:18-cv-07233, 2020 WL 1967209 (N.D. Cal. Apr. 24, 2020) (criticizing defendants and imposing terminating sanctions for, among other things, implementing an enterprise grade ephemeral messaging application to conceal relevant communications from discovery); *Herzig v. Arkansas Found. for Med. Care, Inc.*, No. 2:18-cv-02101, 2019 WL 2870106 (W.D. Ark. July 3, 2019) (holding that plaintiffs' use of Signal during litigation was designed to prevent discovery of relevant communications, was "intentional, bad-faith spoliation of evidence," and justified the imposition of sanctions).

to address ephemeral messaging. In particular, regulators and courts should understand how to identify and distinguish a legitimate ephemeral messaging program from uses of this technology that may be inappropriate.

All of which has led The Sedona Conference Working Group 6 to prepare The Sedona Conference *Commentary on Ephemeral Messaging* (“*Commentary*”). Section II of the *Commentary* defines the nature and scope of ephemeral messaging, while Section III provides a detailed sketch of the tension and competing demands facing organizations that wish to use these tools.⁶ Section IV encompasses a series of guidelines that provide direction to organizations on how to navigate the landscape of uncertainty surrounding the use of ephemeral messaging.⁷ The guidelines also offer recommendations to regulators and judges for evaluating good-faith uses of corporate ephemeral messaging.

In particular, Guideline One provides that regulators and courts should recognize that ephemeral messaging may advance key business objectives. Guideline Two proposes that organizations recognize—and take affirmative steps to manage—ephemeral messaging risks. Guideline Three states that organizations should make informed choices and develop comprehensive use policies for ephemeral messaging applications. Guideline Four recommends that regulators, courts, and organizations consider practical approaches, including comity and interest balancing, to resolve cross-jurisdictional conflicts over corporate uses of ephemeral messaging. Guideline Five emphasizes how reasonableness and proportionality should govern discovery obligations relating to ephemeral messaging data in U.S. litigation.

6. See Sections II & III, *infra*.

7. See Section IV, *infra*.

These guidelines are designed to help organizations and their counsel, in addition to regulators and courts, as they evaluate and address conflicting obligations for organizations regarding their use of ephemeral messaging.

II. EPHEMERAL MESSAGING — NATURE AND SCOPE

Ephemeral messaging refers to secure written communications between one or more parties that are generally considered dynamic, nonstatic,⁸ and “lasting a very short time.”⁹ The two central components of ephemeral messaging that distinguish this technology from other electronic communication media are: (1) automated disposition of message content on the sender’s application *and* that of the recipient; and (2) E2E encryption functionality.

A. Automated Disposition of Message Content

As ephemeral messages are intended to be short-lived, the applications used to generate these communications are designed to enable automatic disposition or expiration of the messages. The specialized functionality of ephemeral messaging applications to delete these messages automatically or after a predefined duration (most often a very short time) also eliminates the message and (in some cases) the underlying metadata residing on the user’s application *and* on the applications of those who either sent or received the messages in question.¹⁰

8. See The Sedona Conference, *Primer on Social Media, Second Edition*, 20 SEDONA CONF. J. 1, 10 (2019) (discussing the dynamic characteristics of social media and messaging application content including that such information “may be easily modified or destroyed by the user, the recipient, the application provider, or by the technology itself.”).

9. <https://www.merriam-webster.com/dictionary/ephemeral>.

10. Wickr’s ephemeral messaging offering is one such example. *How private are my Wickr messages?*, WICKR, <https://support.wickr.com/hc/en-us/articles/115005145108-How-private-are-my-Wickr-messages> (“Wickr then deletes all metadata from its communications and our Secure File Shredder cleans the RAM after each message or picture is opened.”).

For some technologies, the deletion of such content is instantaneous upon closing the message.¹¹ For others, users can set a period of time—from moments to days or even months—before such information is discarded.¹² They can also modify retention and deletion periods by sender or recipient.¹³

B. E2E Encryption

Another significant point of distinction between ephemeral messaging and certain electronic communication tools is that of E2E encryption.¹⁴ Encryption involves the use of cryptography to take a plain text and, through use of keys and algorithms, transforms that plain text into coded text that cannot be read. At the other end, the process is reversed to

11. See *Your Confidential Messenger*, CONFIDE, <https://getconfide.com> (“Confide messages self-destruct. After they are read once, they are gone.”).

12. See *Disappearing messages for Signal*, SIGNAL, <https://signal.org/blog/disappearing-messages/> (“... any conversation can be configured to delete sent and received messages after a specified interval. The configuration applies to all parties of a conversation, and the clock starts ticking for each recipient once they’ve read their copy of the message.”).

13. See *What makes Wickr different from other productivity tools?*, WICKR, <https://support.wickr.com/hc/en-us/articles/115002632813-What-makes-Wickr-different-from-other-productivity-tools-> (“In Wickr, administrators can enforce policies for message retention similar to email retention policies. Retention can be customized for different groups of users or teams depending upon internal policies and compliance requirements.”).

14. Non-ephemeral messaging applications like iMessage may also offer users E2E encryption. *Privacy*, APPLE, <https://www.apple.com/privacy/features/> (“Your Messages and FaceTime conversations are encrypted end-to-end, so they can’t be read while they’re sent between devices.”). In contrast, workplace collaboration tools may not have the most robust forms of encryption necessary to safeguard user confidentiality. See Gennie Gebhart, *What if All Your Slack Chats Were Leaked?*, NEW YORK TIMES (July 1, 2019), <https://www.nytimes.com/2019/07/01/opinion/slack-chat-hackers-encryption.html>.

decrypt a message sent to an intended recipient. Encryption enhances privacy by making it more difficult for hackers and other unintended data recipients to read encrypted data. Encryption can take many forms and provides varying degrees of protection depending on the sophistication of the keys and algorithm.

E2E encryption provides the user with enhanced control over the disposition of messages and enables ephemeral messaging technology to support the objective of transient message content.¹⁵ This type of encryption safeguards communicated data by making it unintelligible in the absence of the algorithm and keys before the data is scheduled for expiration. By so doing, E2E encryption ensures there are no other points in the transmission chain where the data would be accessible to a third party (barring a technical flaw in the implementation of the encryption). This, in turn, typically prevents third parties from obtaining or viewing message content and other transmission details. To further enhance security of the communications and notions of user control, many ephemeral messaging technologies implement endpoint encryption schemes that typically provide no external key management or escrowing capability. This, in effect, shields message content from third parties, including the ephemeral messaging provider, its data stores, and its employees.¹⁶

15. See *Primer on Social Media, Second Edition*, *supra* note 8, at 15 (“Different applications offer competing features, including the ability to control distribution of messages (to a small group versus a community of users), message encryption, private messaging capability, prevention of screenshots, untraceable messages, and removal of messages from others’ devices.”).

16. See, e.g., *Viber Encryption Overview*, RAKUTEN VIBER, <https://www.viber.com/app/uploads/viber-encryption-overview.pdf> (“... all of Viber’s core features are secured with end-to-end encryption ... This

C. Other Characteristics of Ephemeral Messaging

Beyond automated disposition and E2E encryption, ephemeral messaging applications have a variety of characteristics and features. To better understand the nature of their functionality and the corresponding impact they have on senders and recipients, this *Commentary* categorizes ephemeral messaging applications as follows: purely ephemeral, quasi-ephemeral, and non-ephemeral. These categories provide additional understanding for determining whether a messaging application is actually ephemeral and what other features might distinguish an ephemeral messaging application from one that is non-ephemeral. These categories are not mutually exclusive. Some applications may have features from more than one category. Nor are the factors delineated under the respective categories exhaustive. Certain applications may have additional features not discussed in this *Commentary*.

1. Purely Ephemeral Messaging

The following features generally characterize purely ephemeral messaging applications.

- *Deliberate, Permanent, and Automated Message Deletion Built into the Application.* This is one of the core components of an ephemeral messaging application for both the sender and the recipient of a message.

means that the encryption keys are stored only on the clients themselves and no one, not even Viber itself, has access to them.”); *Telegram FAQ*, TELEGRAM, <https://telegram.org/faq#secret-chats> (“All messages in secret chats use end-to-end encryption. This means only you and the recipient can read those messages—nobody else can decipher them, including us here at Telegram.”).

- *Unchangeable Deletion Trigger.* Once a time frame (e.g., 24 hours) or trigger (e.g., once viewed by recipient) is established for deletion, it cannot be changed after a message is sent. The time frame may be shortened or lengthened for future messages, typically with a corresponding notification to a recipient through that conversation or channel. For some applications, these triggers are built into the application's functionality as a "read and burn" function and cannot be modified.
- *No Archiving or Storage Capability.* Purely ephemeral messaging applications disable archiving and storage capacity to better ensure that content and metadata are permanently deleted. They also have mechanisms such as forwarding protection and message overwriting to safeguard message deletion. Nevertheless, indirect means of archiving, such as screen shots, are always possible. While some applications provide a warning when a screen shot is made on the same device, this is easily bypassed with a second device.¹⁷
- *Deletion Consistent within the Application for Senders and Recipients.* Senders cannot retain messages that are removed from a recipient's application and vice-versa.

17. See *United States v. Engstrom*, No. 2:15-cr-00255-JAD-PAL, 2016 WL 2904776 (D. Nev. May 16, 2016) (observing that Wickr's screen protection feature could be circumvented by taking "pictures of texts with a camera to document them.").

- *E2E encryption.* Third parties, including the application provider, cannot access message content without encryption keys.

2. Quasi-Ephemeral Messaging

The following features may characterize quasi-ephemeral messaging applications.

- *Preservation Possible in Certain Circumstances.* Applications that are quasi-ephemeral provide senders, recipients, or administrators with the ability to set deletion as a default while also configuring the application to preserve certain message content. In like manner, senders, recipients, or administrators also have the ability to override preservation as a default and implement ephemeral deletion mechanisms for certain messages, senders, recipients, or components of the application.
- *Deletion May be Impeded by External Mechanisms.* Quasi-ephemeral applications do not disable external mechanisms such as message forwarding or screenshots that prevent total deletion.
- *Content is Deleted, But Metadata is Preserved.* Quasi-ephemeral messages are completely deleted and their content is not preserved, but certain metadata—including the time a message was sent or received or the identity of the sender or recipients—is retained.
- *Combination of Other Features.* Messaging applications may be quasi-ephemeral if they

combine a series of features from both purely ephemeral and non-ephemeral applications.

3. Non-Ephemeral Messaging

The following features often characterize non-ephemeral messaging applications and are included to distinguish ephemeral messaging technologies from those that are non-ephemeral.

- *Deliberate and Permanent Message Deletion not Built into the Application.* The intentional, irrevocable deletion of messages is a key component of an ephemeral messaging application. Applications that do not provide this feature in some form cannot be considered ephemeral.
- *Deletion is Not Consistent across Senders and Recipients.* If a sender cannot automate deletion of the message from both the sender's device *and* the recipient's device, the application from which the message was sent is not ephemeral.
- *Deletion from the Application Does Not Delete Content from Other Sources.* If a message can be deleted from an application but is still kept in some format on a server, backups, or other storage mediums, the application from which the message was sent is not ephemeral.
- *Deletion Time Frame is Variable.* Where the time frame for message deletion is indefinite, can be determined or modified after the message is sent, or can be based on nontemporal factors that could accelerate deletion (such as size

limitations), the application from which the message was sent is not ephemeral.

- *Lack of E2E Encryption.* Encryption is either entirely lacking or is limited to data that is in transit and at rest. Under either scenario, third parties—including the provider—have the ability to access messages, making the application from which the message was sent non-ephemeral.

The aforementioned descriptions provide important context on how the *Commentary* views ephemeral messaging, both in terms of understanding the tensions associated with its operation and delineating guidelines regarding the use of this technology.

III. TENSIONS ASSOCIATED WITH THE USE OF EPHEMERAL MESSAGING APPLICATIONS

The widespread use of ephemeral messaging applications reduces a number of privacy and data protection risks but also creates new challenges for governments and private sector organizations. Organizations and their counsel must consider how to balance these opposing interests, taking into account the views of government regulators and courts. Section III of this *Commentary* explores the underlying nature of these considerations by examining the laws, practices, and perspectives that support and oppose the use of ephemeral messaging.

A. *Benefits of Ephemeral Messaging*

1. Organizational Benefits

There are a number of benefits of ephemeral messaging—both for organizations and for individual users. For organizations, in particular, ephemeral messaging supports information governance best practices by reducing unnecessary data. It also facilitates, among other things, compliance with legal requirements to protect personal data, privacy by design, and data security objectives.

(a) Information Governance

The massive growth in data volumes has driven organizations to adopt policies that seek to manage the life cycle of data. The focus of those policies is on retention of data with ongoing business value and early identification and action to discard data without such value. Responsible usage of ephemeral messaging tools can offer significant economies in data storage and records management. Established record retention policies naturally weigh the business value of a data

asset against the costs of retention and remove data assets that have aged beyond their use in an organization.

In practice, enforcing the deletion of obsolete data is difficult and generally not prioritized by organizations. Stale data is often challenging to destroy because its value is hard to ascertain later in time. It may require laborious review long after the reason for its creation or retention has been forgotten.

Effective governance of messaging and emails is more likely when the method is built on a “read then delete/action/store” process versus the more common accumulation without limit or until the mailbox exceeds its quota. The consequences for adopting the latter, laissez-faire approach include enforcement actions and fines against organizations that fail to remediate “data graveyards” with “years-old private data.”¹⁸ The €14.5 million fine that the Berlin Commissioner for Data Protection and Freedom of Information imposed on Deutsche Wohnen in 2019 for failing to implement an effective information management system exemplifies the folly of this approach.¹⁹

Ephemeral messaging can assist with implementation of the life-cycle process by eliminating data with no ongoing business value, particularly since a sizeable portion of the data growth involves this type of information (e.g., routine communications, meeting requests, duplicative email chains to large groups, etc.). Such a practice removes large volumes of low-value data, offering significant benefits to the organization. Likewise, information governance policies that

18. European Data Protection Board, *Berlin Commissioner for Data Protection Imposes Fine on Real Estate Company* (Nov. 5, 2019), https://edpb.europa.eu/news/national-news/2019/berlin-commissioner-data-protection-imposes-fine-real-estate-company_en.

19. *Id.*

prioritize data assets with business value, rather than controlling all information equally, enhance the usefulness of retained information and are more responsive to changing end-user preferences.

(b) Legal Compliance Support

The 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (“Convention 108”) was the first binding international law addressing privacy and data protection.²⁰ Convention 108 mandates a number of personal data protection and privacy requirements that are facilitated by ephemeral messaging, including the implementation of security measures to protect personal data, data minimization, storage limitation, and the right of individuals to have their personal data deleted. In the decades since, Convention 108 has been ratified by fifty-five countries. Numerous additional data protection laws have been adopted across the globe with similar requirements.

One of the most significant pieces of recent data protection legislation is the GDPR, which establishes data protection and privacy requirements for personal data of individuals within the European Economic Area (EEA) and governs the export of personal data outside the EEA. Like Convention 108 and the EU Data Protection Directive, the GDPR requires the implementation of security measures to protect personal data, including by imposing the principles of data minimization and storage limitation on all personal data processing operations. The GDPR also provides individuals with the right to have their personal data deleted.

20. Council of Europe, European Treaty Series No. 108 (Jan. 28, 1981), <https://rm.coe.int/1680078b37>.

The use of ephemeral messaging can facilitate GDPR compliance. The automated deletion features of ephemeral messaging applications can help meet GDPR data minimization and storage limitation requirements. Ephemeral messaging can also minimize the effort required to respond to data subject deletion or access requests, since certain data will be subject to automatic erasure. Finally, the encryption protections and automatic deletion of personal data through ephemeral messaging platforms reduces exposure in the event of a breach. Notification to data subjects is not required where the breach is not likely to result in a “high risk” to their rights and freedoms, and regulatory notification is not required where the breach is “unlikely to result in a risk to the rights and freedoms of natural persons.”²¹ The protections afforded by ephemeral messaging can reduce or eliminate these risk factors, regardless of the sensitive nature of any information communicated through ephemeral messaging.

The GDPR is particularly significant given its broad reach. It applies to organizations established within the EEA. It also applies to organizations located outside the EEA that offer goods or services in the EEA, monitor behavior of data subjects within the EEA, or to which EU law applies due to public international law. Violations of the GDPR can carry severe consequences, including regulatory penalties of up to €20,000,000 or 4 percent of global revenues, whichever is greater.²²

21. GDPR arts. 33, 34.

22. GDPR art. 82. See Adam Satariano, *Google Is Fined \$57 Million Under Europe's Data Privacy Law*, NEW YORK TIMES (Jan. 21, 2019) <https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html> (discussing €50 million fine imposed by French data protection authority on Google for not disclosing how user's data is collected across its services).

The GDPR is not the only significant data protection law that has taken effect recently. Various countries have enacted or updated data protection laws to enhance privacy safeguards in the digital age, including Australia,²³ Bermuda,²⁴ Brazil,²⁵ and Israel.²⁶ In the U.S., the Federal Trade Commission enforces data protection pursuant to Section 5 of the FTC Act,²⁷ though much of the movement on data protection has originated with state governments. For example, some state data breach statutes impose proactive storage limitation requirements.²⁸ In 2016, New York State promulgated cybersecurity regulations requiring financial institutions to develop and implement cybersecurity policies, including “policies and procedures for the secure disposal on a periodic basis of [certain] Nonpublic Information.”²⁹ The California Consumer Privacy Act (CCPA) incentivizes organizations to reduce their data footprint and enhance security protections in

23. Privacy Amendment (Notifiable Data Breaches) Act 2017.

24. Personal Information Protection Act 2016.

25. Lei Geral de Proteção de Dados Pessoais [Brazilian General Data Protection Act], Law No. 13,709/2018.

26. Protection of Privacy Regulations (Data Security) 5777-2017.

27. *See* In the Matter of Snapchat, Inc., FTC Docket No. C-4501, FTC File No. 132-3078 (December 23, 2014) (consent order) (approving final order settling charges that Snapchat misrepresented the ephemeral nature of messages sent through the service); FEDERAL TRADE COMM’N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESS AND POLICYMAKERS (March 2012), <https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf> (calling for enhanced focus on privacy, data security, and data minimization of consumer personal data).

28. *See, e.g.*, ALA. CODE 1975 § 8-38-10; COLO. REV. STAT. § 6-1-713.

29. Cybersecurity Requirements for Financial Services Companies, N.Y. DEPT. OF FIN. SERV., 23 NYCRR 500.13 (2016).

the face of statutory penalties for breaches of personal information.³⁰ The CCPA also provides individuals with new rights to access and delete their personal information.³¹

As a result of increased data protection legislative activity, ephemeral messaging may gain even more traction as a beneficial tool for legal risk mitigation.

(c) Privacy by Design

Privacy by design is an increasingly popular information management approach. It includes privacy and security protection as fundamental goals, embedding privacy into the design of the information technology system and business practices as a core functionality. This policy is designed to be proactive rather than reactive. It requires end-to-end security for the data at issue and directs operators to keep privacy as the default mode to ensure a user's privacy is protected without the user having to take any action. Operators are

30. The CCPA allows California residents the right to know the personal data collected about them, to access such data, to know whether their data has been sold or disclosed to another organization, and to refuse to allow the sale of their personal data. *See* CAL. CIV. CODE § 1798.100 *et seq.* (West 2020). Companies that suffer a security breach of personal information can be subject to a civil lawsuit and be ordered to pay California residents statutory damages of \$100-\$750 “per consumer per incident or actual damages, whichever is greater.” CAL. CIV. CODE § 1798.150(a)-(b) (West 2020).

31. Effective Jan. 1, 2023, the California Privacy Rights Act (CPRA) will replace the CCPA. The CPRA will generally augment the duties of regulated businesses toward California consumers and impose new limitations on their use of consumers' personal information. *See* Cynthia Cole, Matthew R. Baker, & Katherine Burgess, *Move Over, CCPA: The California Privacy Rights Act Gets the Spotlight Now*, BLOOMBERG LAW (Nov. 16, 2020), <https://news.bloomberglaw.com/us-law-week/move-over-ccpa-the-california-privacy-rights-act-gets-the-spotlight-now>.

accountable for the collection of data, maintaining data security, making data available to the user upon request, and protecting data with appropriate security measures.³² This emphasis on privacy encourages corporate adoption of ephemeral messaging technologies to address privacy issues.

(d) Data Security

Organizations may actively seek to use ephemeral messaging in situations where data security is paramount. For example, organizations bringing a new product to market or otherwise handling sensitive information relating to intellectual property may rely on ephemeral messaging to better ensure communications are secure and reduce the likelihood they are subject to interception.

Ephemeral messaging tools minimize the amount of data vulnerable to compromise.³³ This is one of the most effective means of ensuring data security and may prevent hackers from gaining access to important information. Even if a mobile device is lost or otherwise compromised, for example, the automatic deletion of data provides protection against loss.

Another advantage that flows indirectly from the use of ephemeral messaging is derived from E2E encryption that is integral to these platforms.³⁴ The use of reliable and easy to implement E2E encryption allows for more effective authentication of each user, something that is more difficult to do at scale with email or text messaging. This helps to secure an organization's networks by mitigating the risk of spoofed

32. See Ann Cavoukian, *Privacy by Design: The Seven Foundational Principles*, IAPP (2011) https://iapp.org/media/pdf/resource_center/pbd_implement_7found_principles.pdf.

33. See Section III.A.1.a, *supra*.

34. See Section II.B, *supra*.

senders and by ensuring the integrity and confidence in the identity of a particular sender or a group.

Even when well implemented, encryption is not foolproof. For example, it is possible to take a screenshot of an ephemeral message that has been decrypted and appears on an intended recipient's screen.³⁵ Depending on the level of security required, it may be necessary to use encryption in conjunction with other ephemeral data management methods.

(e) Productivity

Large organizations are also taking advantage of ephemeral messaging to facilitate collaboration among employees in different locales. Certain messaging applications allow personnel to work on a collaborative basis. Those applications establish data minimization processes that govern data retention on a platform so that information is not retained unnecessarily and provide E2E encryption of data, which limits access to authorized users. These features allow users to work together across the globe while reducing unnecessary retention of incidental communications and prioritizing the retention of those critical to the organization's mission. This has the further benefit of providing customers in certain circumstances with greater security regarding a corporate relationship, product or other intellectual property

35. See Section II.C, *supra*. Indeed, many encryption systems typically contain flaws of various kinds that enable decryption or allow discovery of a shortcut to the clear text. The field of cryptography is full of examples of cryptographic systems that have failed to protect the communications involved because of flaws or other design features in some part of the device or software. See Greg Miller, *How the CIA Used Crypto AG Encryption Devices to Spy on Countries for Decades*, THE WASHINGTON POST (Feb. 11, 2020), <https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/>.

development, or joint business venture. These benefits stand in contrast to non-ephemeral workplace collaboration tools, which may have comparatively relaxed limitations on authorized users of the platform and may also lack E2E encryption to safeguard confidentiality.³⁶

2. Benefits to Individual Users

Concern over data privacy and user control of data has grown in importance in recent years. Given the raft of business and government data breaches and news stories that service providers are more focused on monetizing the value of customer data than protecting it, users have become aware that their online data may not be secure.³⁷ As a result, interest has grown in tools that give users more protection and control over their data and allow them to reduce their individual data footprints. As concepts such as data minimization and erasure gain further traction globally, ephemeral messaging offers individual users a check against unknown retention schemes and objectives.

36. See Gennie Gebhart, *What if All Your Slack Chats Were Leaked?*, NEW YORK TIMES (July 1, 2019), <https://www.nytimes.com/2019/07/01/opinion/slack-chat-hackers-encryption.html>. (“Right now, Slack stores everything you do on its platform by default—your username and password, every message you’ve sent, every lunch you’ve planned and every confidential decision you’ve made. That data is not end-to-end encrypted, which means Slack can read it, law enforcement can request it, and hackers—including the nation-state actors highlighted in Slack’s S-1—can break in and steal it.”).

37. See Christopher Mele, *Data Breaches Keep Happening. So Why Don’t You Do Something*, NEW YORK TIMES (Aug. 1, 2018), <https://www.nytimes.com/2018/08/01/technology/data-breaches.html>; Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, NEW YORK TIMES (Mar. 19, 2018), <https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html>.

Certain ephemeral messaging platforms have been widely adopted on a worldwide basis. For example, WhatsApp, a messaging application offering E2E encryption and a limited automated deletion feature, is estimated to have over 2 billion users in 180 countries.³⁸ Another popular messenger service, Snapchat, which features deletion of messages after review, reports that it has approximately 238 million daily active users, with approximately 90 million North American active users and 71 million European active users.³⁹ Ephemeral messaging has become popular in part due to the enhanced control it provides to users in disseminating and deleting data as they choose.⁴⁰ Wide-scale acceptance of these applications suggests that ephemeral messaging may continue to be popular into the foreseeable future.

38. See Mansoor Iqbal, *WhatsApp Revenue and Usage Statistics (2020)*, BUSINESS OF APPS (Jan. 12, 2021), <https://www.businessofapps.com/data/whatsapp-statistics/>. The largest WhatsApp country markets are India (340 million users) and Brazil (99 million users). In some markets, including the Netherlands, Spain and Italy, WhatsApp has achieved penetration of over 80 percent.

39. Snapchat's services appear to be particularly popular with the young, reaching over 80 percent of those between the ages of 18-24 in the U.S. See Mansoor Iqbal, *Snap Inc. Revenue and Usage Statistics (2020)*, BUSINESS OF APPS (Nov. 27, 2020), <https://www.businessofapps.com/data/snapchat-statistics/>.

40. Ephemeral messaging that provides secure encryption or deletes messages after review can also have an important political role in authoritarian countries. Applications that provide users control over dissemination of data allow dissidents to engage in more secure communications, with less fear that their data and messages will be subject to interception by government officials. See Ron Synovitz, *Encrypted messaging apps struggle against authoritarian regimes*, RADIO FREE EUROPE/RADIO LIBERTY, https://internetfreedom.io/rferl__encrypted-messaging-apps.html.

B. Risks of Ephemeral Messaging

Longstanding government regulatory policies and litigation practices in the U.S. and elsewhere discourage the use of ephemeral messaging, sometimes directly but more often informally or indirectly. Organizations typically face legal and regulatory risks from the improper or sometimes unintended deletion of data. The focus in some regulated settings and in litigation contexts is often on the importance of long-term access to relevant data, and as a consequence, negative consequences can arise when such access is denied or diminished due to a failure to preserve. Because ephemeral messaging might be misused, those charged with risk management in organizations may be reluctant to adopt these technologies if they perceive a likelihood that the organization will be seen as uncooperative with law enforcement, regulators, or in litigation.

Ephemeral messaging can also disrupt traditional approaches to information governance. When data may be destroyed immediately after creation, use, or consumption, organizations will have to adjust their retention policies to either redirect certain communications to a different channel or adopt software that disables or otherwise controls data deletion in certain situations. Additionally, ephemeral messaging applications are dynamic platforms, i.e., features may be removed, changed, or added without the knowledge or consent of the organization. This aspect of ephemeral messaging injects unpredictability to data resources that are volatile by design. Accordingly, the risks and consequences of improper data deletion may be amplified and should be considered before an ephemeral messaging application is deployed. Specific regulatory and legal risks are considered in turn below.

1. Regulatory Risks

As noted above, the focus in some regulated settings is often on the importance of long-term access to relevant data, which conversely can lead to serious negative consequences when such access is denied or diminished due to a failure to preserve. Complying with regulatory controls that require strict retention protocols, including various reporting and audit requirements, is often seen as a key inhibitor to adopting ephemeral messaging. In addition, certain organizations must securely retain particular classes of information or risk robust penalties for noncompliance.

For example, the U.S. SEC's National Office of Compliance Inspections and Examinations advises regulated entities to specifically prohibit "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."⁴¹ This guidance, coupled with the requirement that brokers, dealers, and traders keep all communications "relating to its business as such" for three years, could limit the ability of organizations in the financial services industry to use ephemeral messaging.⁴²

Organizations seeking to demonstrate cooperation in Foreign Corrupt Practices Act (FCPA) investigations must

41. See *National Exam Program Risk Alert*, OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS (Dec. 14, 2018), <https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Electronic%20Messaging.pdf>.

42. See 17 C.F.R. § 240.17a-4(b)(4). See also Sridhar Natarajan, Michelle Davis & Dan Wilchins, *JPMorgan Puts Senior Credit Trader on Leave Over WhatsApp Use*, BLOOMBERG (Jan. 13, 2020), <https://www.bloomberg.com/news/articles/2020-01-13/jpmorgan-puts-senior-credit-trader-on-leave-over-whatsapp-use>.

satisfy standards that the U.S. DOJ has promulgated regarding the use of ephemeral messaging. The most recent FCPA guidance states that cooperation can be shown by “appropriate retention of business records . . . including implementing appropriate guidance and controls on the use of personal communications and ephemeral messaging platforms.”⁴³ Nevertheless, this guidance should be construed in the context of the U.S. DOJ’s historical antipathy toward the use of ephemeral messaging.⁴⁴

Similarly, the U.S. DOJ’s Antitrust Division recently promulgated guidance regarding the role of information governance as it relates to developing antitrust compliance programs that require regulatory approval. According to the U.S. DOJ, a key aspect of such information governance should include controls for evaluating “new methods of electronic communication” and addressing “the antitrust risk associated with these new forms of communication.”⁴⁵ While the DOJ guidance does not specifically mention ephemeral messaging,

43. See FCPA Corporate Enforcement Policy (2018), United States Department of Justice, Justice Manual, 9-47.120(3)(c), <https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977>.

44. The U.S. DOJ previously published FCPA guidance on November 29, 2017, generally disapproving the use of ephemeral messaging. See Philip Favro, *Ephemeral Messaging: Balancing the Benefits and Risks*, at *6, PRACTICAL LAW (2020). That guidance declared as follows: “The following items will be required for a company to receive full credit for timely and appropriate remediation . . . Appropriate retention of business records, and prohibiting the improper destruction or deletion of business records, including prohibiting employees from using software that generates but does not appropriately retain business records or communications.”

45. Press Release, U.S. Dept. of Justice, Antitrust Division Announces New Policy to Incentivize Corporate Compliance, (July 11, 2019), <https://www.justice.gov/opa/pr/antitrust-division-announces-new-policy-incentivize-corporate-compliance>.

an organization may want to consider developing a written policy that sets out its business needs for use of an ephemeral messaging application and provides guidance for using that application. As detailed in Guideline Two and Guideline Three of this *Commentary*, the policy could also discuss the benefits and risks of the application and identify appropriate risk mitigation strategies that the organization has implemented.

Beyond the U.S., regulators in other countries and regions have expressed concerns with encrypted messaging applications, which encompass ephemeral messaging. These concerns focus on both the lack of information that encrypted messages retain for investigative purposes and how they may prevent organizations from monitoring message content. These concerns have resulted in enforcement actions in the United Kingdom (U.K.) and in Europe against organizations and individuals using encrypted messaging.⁴⁶ In particular, the U.K.'s Financial Conduct Authority has taken action against firms and individuals that have used WhatsApp to transmit sensitive information and conduct deal and investment-related activities.⁴⁷ To address concerns, organizations may consider selecting ephemeral messaging applications that have features and functionality that allow for retention of message content.⁴⁸ Organizations may also consider memorializing their

46. See, e.g., Council of the European Union, *Council Resolution on Encryption—Security through encryption and security despite encryption*, (Nov. 24, 2020), <https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/en/pdf>.

47. See Financial Conduct Authority, *Newsletter on market conduct and transaction reporting issues* (Jan. 2021), <https://www.fca.org.uk/publications/newsletters/market-watch-66>.

48. See Section IV.C, *infra*.

technology selection process into an overall ephemeral messaging use policy.⁴⁹

2. Legal Risks

The use of ephemeral messaging poses risks to any party that must retain information for a legal matter. Noncompliance with common law or court-imposed retention requirements may impact the organization's ability to assert or defend its claims in legal actions, run afoul of discovery obligations in litigation, or invite further scrutiny into its affairs.

A primary consideration for organizations that are subject to U.S. jurisdiction is the duty to preserve information relevant to reasonably anticipated or pending litigation in the U.S.⁵⁰ Failure to comply with this duty may expose an organization to legal consequences that can significantly add to the time and costs required to litigate a matter, regardless of the merits of the underlying lawsuit. As a result, the duty to preserve creates a separate and distinct set of risks that may involve records beyond those normally retained for operational utility. Once a duty to preserve has been triggered, a company must take steps to preserve data as required by a particular jurisdiction. Organizations may need to have policies and procedures to allow for the suspension of the use of ephemeral messaging for affected custodians or alternatively disable the ephemerality function as to affected custodians until a preservation obligation has been satisfied.⁵¹

49. *See id.*

50. *See* DR Distribs. v. 21 Century Smoking, Inc., --- F. Supp. 3d ---, 2021 WL 185082, at *54 (N.D. Ill. Jan. 19, 2021) ("Once a party reasonably anticipates litigation, it is duty-bound to take good faith steps to preserve documents and data that may be relevant to the litigation.").

51. *See* Section IV.E, *infra*.

3. Operational Risks

The massive increase in data volumes in most organizations is primarily due to the daily flow of operations information. The challenge for most organizations is managing this information—including communications—in a way that does not overwhelm their systems. Organizations need to ensure business records are both accessible and properly retained to safeguard their integrity. At the same time, they should also develop protocols and procedures to dispose of nonessential materials. Depending on the industry, various corporate communications may fall outside the ambit of business records and may not require long-term retention. In that event, organizations may use ephemeral messaging in the same way as email, or they may choose to limit the scope of use to text messages.

Adoption of ephemeral messaging systems may pose operational risks to organizations regarding the governance of its information. Information governance is premised on notions of transparency regarding the information an organization generates, receives, and maintains. It generally requires the implementation of corporate policies and procedures both to enforce these principles and to accomplish corporate information objectives. Policies and procedures can define and implement controls regarding the types of business records that a company requires to be stored for certain periods of time or in certain locations. The policies and procedures can also be designed to disallow the use of ephemeral messaging with respect to certain categories of records, to provide guidance on the types of records that require retention, and to identify those that may be appropriate for ephemeral systems, such as those with no ongoing business value. Without such policies or procedures, organizations may risk not retaining essential records,

communications, or other information required for business purposes and legal and regulatory needs.

IV. GUIDELINES

Against the backdrop of these conflicting considerations, this *Commentary* has promulgated five guidelines regarding use of ephemeral messaging. These guidelines provide recommendations for organizations and their counsel, along with government regulators and courts, that spotlight how they can best implement, evaluate, or address organizational use of ephemeral messaging.⁵²

A. Guideline One: Regulators and Courts Should Recognize that Ephemeral Messaging May Advance Key Business Objectives

Regulators and courts should acknowledge that ephemeral messaging applications may be a valuable aspect of an organization's information governance program. Ephemeral messaging offers automated message deletion and E2E encryption, which can confer significant business benefits. Those benefits include confidentiality and security for sensitive electronic information in the face of increasing threats of inadvertent disclosure of such information.⁵³

Other benefits include data minimization, which ephemeral messaging facilitates by reducing data volumes and safeguarding personal information. Limiting the retention of corporate data that has no ongoing business value and decreasing the risk of exposing personal data to third parties are recognized as proper information governance practices and

52. Guideline One and Guideline Two, which respectively address the benefits and risks of ephemeral messaging, should be considered holistically.

53. Cf. Health Insurance Portability and Accountability Act of 1996, 45 CFR § 164.306 (requiring covered entities and business associates to implement security policies and procedures to protect patient data).

as key components of safeguarding sensitive user information under the principle of privacy by design.⁵⁴

Given these considerations, regulators and courts may view ephemeral messaging as facilitating corporate compliance with data protection laws, including the GDPR. Satisfying these laws is an increasingly significant business imperative given the growing importance of privacy—both internationally and domestically—for organizations and individuals.

Regulators and courts may also consider the benefits surrounding ephemeral messaging in connection with four principal areas of information governance: recordkeeping, data preservation, regulatory scrutiny, and cross-border data transfers.⁵⁵ Concerns over the interplay of ephemeral messaging and these four areas can impact a party's legal interests as well as its reputation.⁵⁶ This is particularly the case where regulators and courts may be inclined to presume that ephemeral messaging is a means to conceal improper conduct. While ephemeral messaging—like phone calls, email, and

54. Cf. Federal Trade Commission Staff Report, *Internet of Things: Privacy & Security in a Connected World* (January 2015), at 33 *et seq.*; GDPR, *supra* note 1, art. 1(c).

55. See Section III.A.1, *supra*.

56. Robert Mueller observed in his report regarding interference into the 2016 U.S. presidential election that certain witnesses “deleted relevant communications or communicated during the relevant period using applications that feature encryption or that do not provide for long-term retention of data or communications records” and thereby prevented the corroboration of witness statements through contemporaneous communications or the use of such communications to “shed additional light on (or cast in a new light) the events described in the report.” U.S. Department of Justice, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, Special Counsel Robert S. Mueller, III, at *10 (Mar. 2019), <https://www.justice.gov/storage/report.pdf>.

traditional messaging apps—has been used for improper purposes, such a perception may be tempered as regulators and courts consider the business purposes served by this technology.⁵⁷

Perhaps reflecting such understanding, the U.S. DOJ's 2019 FCPA Corporate Enforcement Policy recently abandoned its express prohibition against ephemeral messaging by organizations seeking cooperation credit. Instead, the U.S. DOJ ostensibly provides organizations more latitude to adopt ephemeral messaging and other technologies to further information retention policies and practices that satisfy business objectives. This change to the U.S. DOJ's FCPA Enforcement Policy may be viewed as recognizing the increasing importance of ephemeral messaging to advance those objectives.

Regulators and courts may consider evaluating the attendant circumstances surrounding an organization's use of ephemeral messaging. This includes the various technological

57. *See generally* Arthur Andersen LLP v. United States, 544 U.S. 696, 704 (2005) (“‘Document retention policies,’ which are created in part to keep certain information from getting into the hands of others, including the Government, are common in business.”); *Micron Tech., Inc. v. Rambus Inc.*, 645 F.3d 1311, 1322 (Fed. Cir. 2011) (“where a party has a long-standing policy of destruction of documents on a regular schedule, with that policy motivated by general business needs, which may include a general concern for the possibility of litigation, destruction that occurs in line with the policy is relatively unlikely to be seen as spoliation.”); *Phillip M. Adams & Assoc., L.L.C. v. Dell, Inc.*, 621 F. Supp. 2d 1173, 1193 (D. Utah 2009) (“A court—and more importantly, a litigant—is not required to simply accept whatever information management practices a party may have. A practice may be unreasonable, given responsibilities to third parties. While a party may design its information management practices to suit its business purposes, one of those business purposes must be accountability to third parties.”).

aspects of ephemeral messaging applications. The most widely used applications allow the user to set whether messages will be deleted after a certain time or after being read. Others, aimed at enterprise level applications, provide more centralized control by the organization. As detailed more fully in Guideline Three of this *Commentary*, the features that ephemeral messaging technologies offer are important considerations when organizations select their communication platforms and develop their approach to an ephemeral messaging policy. Regulators and courts need not defer to an organization's use of ephemeral messaging where the selected application cannot be configured to align and satisfy its obligations for information retention.

When organizations have implemented an ephemeral messaging program consistent with the recommendations memorialized in Guideline Two and Guideline Three of this *Commentary*, regulators and courts may consider that such a program (absent contrary circumstances) is both reasonable and executed in good faith.

B. Guideline Two: Organizations Should Take Affirmative Steps to Manage Ephemeral Messaging Risks

Organizations should be aware that communication channels leaving no evidence of wrongdoing may be favored by those engaging in secretive activity for an improper purpose.⁵⁸ Organizations should also understand that

58. In the U.S., an axiom among political insiders states that one should never send an email when a phone call suffices; never make a call when an in-person meeting is possible; and never say something when a nod can get the point across. Similarly, traders at a prominent financial services company once devised the abbreviation "LDL" (let's discuss live) as a way to take an email exchange into a phone conversation to avoid creating an incriminating trail. See Virginia Heffernan, *The Trouble With E-Mail*, THE

ephemeral messaging can provide an effective means for misconduct by enabling more communication than would be possible by phone or even in person and by allowing the sharing of documents or other data. Ephemeral messaging also facilitates the disappearance of a communication (including its metadata) after it is read by the recipient. This may not be possible with a telephone call or in-person meetings, particularly with the technology now available for tracking the use of mobile phones.

As a result, organizations should carefully select and evaluate their use of ephemeral messaging. As described in Guideline Three of this *Commentary*, an organization's data preservation policy and communications, including any information retention directive, should address the use of ephemeral messaging. This may include extending the duty to preserve (where applicable) to records generated by an ephemeral messaging application. It may also include addressing all forms of sanctioned and nonsanctioned use of such applications for both legal and improper purposes.

If an application does not have legal-hold capability that can retain communications in the event of a data retention directive, the organization should consider reasonable alternatives for addressing retention, including a possible prohibition on the use of ephemeral messaging. A defined policy and evidence of compliance should provide strong support if an organization is called upon by regulators or courts to demonstrate the reasonableness of its ephemeral messaging program. This policy should contemplate the opportunities for misconduct both within the selected enterprise ephemeral application as well as by consumer-

grade, nonsanctioned ephemeral messaging tools that employees may use.

Even with appropriate technology selections and policy implementation, there may be instances where the potential benefits of ephemeral messaging do not outweigh the risks. For example, organizations in highly regulated industries that use purely ephemeral messaging to communicate about regulated aspects of their business may not be able to satisfy recordkeeping requirements or regulatory audits or examinations. The risks associated with regulatory noncompliance or adverse findings from a regulatory examination may exceed the potential benefits gained through data minimization activities, enhanced security, or other organizational benefits.

C. Guideline Three: Organizations Should Make Informed Choices and Develop Comprehensive Use Policies for Ephemeral Messaging Applications

Organizations should consider evaluating which ephemeral messaging applications best address their regulatory, litigation, and business needs. Available technologies offer a range of applications depending on an organization's industry, size, global presence, litigation profile, and appetite for risk.

An organization contemplating the use of ephemeral messaging may consider engaging in a structured approach to selecting an ephemeral messaging technology. Such an approach could involve identifying stakeholders within the organization who can evaluate the appropriate features for such an application. After reaching a determination of those features, the stakeholders could then recommend applications or technologies that best meet the organization's needs. Depending on the size of the organization and the nature of

the process sought to be followed, the stakeholders might include representatives from legal, IT, information security, data privacy, document management, and appropriate business units.⁵⁹

An integral aspect of the stakeholders' work could include the preparation of a written policy addressing the use of ephemeral messaging within the organization. For many organizations, a comprehensive policy that identifies the benefits of ephemeral messaging, the corresponding risks, and actionable risk mitigation measures may be essential for demonstrating the business-use case of this technology to skeptical insiders and outsiders.⁶⁰ Depending on the nature of the organization and its industry profile, this may include company executives, shareholders, regulators, litigation adversaries, courts, and the public.

Depending on its needs and the type of application selected, the organization may decide that acceptable uses should be limited to logistical communications (scheduling calls or meetings) or a slightly broader category of nonsubstantive communications. Alternatively, acceptable uses may include specific types of business communications or other special circumstances. For example, in the incident response field, using out-of-band communications has long been an accepted and highly recommended practice.⁶¹

59. Having a member of the executive team on the committee will help ensure senior management support for this effort and can promote acceptance of ephemeral messaging application(s) and associated policies and practices.

60. See Favro, *supra* note 44, at *6.

61. Out-of-band communication should be reliable and secure in the event that a cyber intruder is monitoring email systems. Ephemeral messaging is ideal for this scenario as it allows for speed in response and security and enhances the openness of the team in communicating

Ephemeral messaging may also be advisable for certain internal investigations involving cross-border matters where counsel is seeking to protect information from third parties to better ensure that the matter is addressed with strict confidentiality. Finally, ephemeral messaging might be used for one-way communication from the organization to recipients where, at the same time, a backend system would store the substance and metadata of the communication.⁶²

In drafting the policy, organizations should understand that the most important information governance factors related to ephemeral messaging are legal-hold capabilities and the availability of customizable retention periods. Organizations that prefer to keep data for longer periods may value the security features of ephemeral messaging more than the opportunities for data minimization. Those organizations will therefore select an application with longer retention periods and the ability to effect legal-hold functionality when the need arises. Other organizations may prioritize minimizing the

information. *See, e.g.,* The Sedona Conference, *Incident Response Guide*, 21 SEDONA CONF. J. 125, 157–60 (2020) (“In the event of a significant cybersecurity incident or intrusion . . . it is essential to have reliable communication channels available to keep key players and essential stakeholders informed, and to lead and manage the incident response. In some cases, this may require alternative (and secure) communications channels. As with other incident response preparations, alternative communications channels should be planned and provisioned in advance to handle situations where corporate communications systems have been completely disrupted.”).

62. *Cf. Toftely v. Qwest Commc’ns Corp.*, No. C3-02-1474, 2003 WL 1908022, at *1 (Minn. App. Apr. 22, 2003) (denying plaintiff employment benefits because she was discharged for violating the company’s confidentiality policy by disclosing to a third party a confidential litigation hold instruction with an embedded “electronic tracer” that allowed defendant to monitor whether the message was forwarded outside the company).

volume of data retained and may instead choose a technology with shorter retention periods, disabling the application entirely once a legal hold is implemented. Organizations may alternatively select a middle ground, allowing employees to communicate with ephemeral messaging until a legal-hold obligation arises, at which time use of the application by key custodians of relevant information may be disabled or otherwise prohibited for any communications related to the subject matter of the hold.

An organization may also choose to adopt more than one ephemeral messaging application to maximize the possible number of acceptable uses. For example, one application could be permitted for all employees, but limited to logistical communications. Another application could be designated for specific departments relating to limited types of communications. Irrespective of the technology selected, organizations should consider the benefits of forbidding employees from using consumer applications for individual, unstructured, or one-off business purposes.

Once implemented, the ephemeral messaging policy should be followed by employee education and training, together with periodic auditing of use and rule observance to better ensure compliance.

In adopting an ephemeral messaging program, the organization should consider undertaking a thorough data mapping exercise to allow data managers to understand how the ephemeral messaging application interacts with other data systems.

With sufficient documentation of acceptable uses and data retention requirements, and selection of appropriate technologies tailored to their requirements, organizations can

better assess and manage risk in taking advantage of the benefits of ephemeral messaging.

D. Guideline Four: Regulators, Courts, and Organizations Should Consider Practical Approaches, Including Comity and Interest Balancing, to Resolve Cross-Jurisdictional Conflicts over Ephemeral Messaging

Conflicts with legal or regulatory requirements may arise where the use of ephemeral messaging fulfills applicable requirements in one jurisdiction while simultaneously conflicting with obligations in another jurisdiction. This is particularly the case with cross-border data transfers where the understanding and priority accorded data privacy and information retention differ between jurisdictions and where conflicts may arise between data retention and data minimization requirements.⁶³ To address these issues, regulators, courts, and organizations may find notions of comity, interest balancing, or other accommodations useful for resolving cross-jurisdictional conflicts over corporate uses of ephemeral messaging.

One accommodation that government regulators might consider is modeling enforcement policies after the U.S. DOJ's 2019 FCPA Corporate Enforcement Policy. Such an approach

63. Compare *Behrens v. Arconic, Inc.*, No. 19-2664, 2020 WL 1250956 (E.D. Pa. Mar. 13, 2020) (citing comity for the French Blocking Statute as a key basis for denying plaintiffs' motion to compel the production of documents pursuant to the Federal Rules of Civil Procedure from the French subsidiary of a defendant rather than resorting to Hague Convention procedures) with *In re Mercedes-Benz Emissions Litig.*, No. 16-cv-0881 (KM) (ESK), 2020 WL 487288 (D.N.J. Jan. 30, 2020) (reasoning that the GDPR and "considerations of international comity" did not relieve defendants from their duty to produce employee names, titles, dates of employment, organizational charts, and other relevant information).

would shift the focus from outright proscription to examining the basis for the organization's implementation of ephemeral messaging, along with related guidance and controls. This would allow the use of ephemeral messaging systems in appropriate cases while also addressing regulatory concerns about unlawful conduct facilitated by ephemeral messaging.

Courts and parties might also consider accommodations to address inconsistent obligations arising from the conflict of international data protection laws and preservation and production requirements in common law litigation over ephemeral messaging data.⁶⁴ If a conflict is found, the parties—and if needed, the court—could define the appropriate scope of preservation and production by balancing the competing needs of the litigation, the consequences of any potential violations of applicable data protection laws, the impact on affected data subjects, and other pertinent considerations.⁶⁵

64. See generally The Sedona Conference, *International Principles on Discovery, Disclosure & Data Protection in Civil Litigation* (Transitional Edition) (2017), https://thesedonaconference.org/publication/International_Litigation_Principles (describing tension between U.S. discovery and preservation obligations and non-U.S. data protection laws). See also Loi 80-538 du 16 juillet 1980 [French Penal Law No. 80-538 of July 16, 1980], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [OFFICIAL GAZETTE OF FRANCE] (blocking statute prohibiting the transfer of data for the purpose of discovery in foreign litigation); *In re* Advocat “Christopher X,” Cour de cassation [Cass.] Paris, crim., Dec. 12, 2007, No. 07-83228 (enforcing blocking statute by fining French lawyer €10,000 for obtaining evidence from a French insurer for use in civil litigation pending in the United States).

65. Compare *Salt River Project Agric. Improvement and Power Dist. v. Trench France SAS*, 17-cv-01468-DGC, 2018 WL 1382529 (D. Ariz. Mar. 19, 2018) (refusing to order defendant to immediately produce relevant documents stored in France outside the bounds of Hague Convention procedures on cross-border discovery) with *In re Mercedes-Benz Emissions Litig.*, No. 16-cv-881 (KM) (ESK), 2020 WL 487288 (D.N.J. Jan. 30, 2020)

Courts in common law jurisdictions may consider allaying preservation and production requirements for ephemeral messaging data where organizations use ephemeral messaging to comply with data minimization principles of cross-border data protection laws.⁶⁶ Those same considerations should also apply when conflicts arise relating to an organization's use of ephemeral messaging to meet domestic data privacy requirements or satisfy other business objectives.

Organizations may also need to consider how to implement approaches to address discovery and data minimization conflicts. One option could include building in accommodations for evaluating whether to deploy ephemeral messaging applications in limited geographic regions (localization) or for specific company divisions. The organization also could implement applications that have technological features allowing otherwise ephemeral messages to be kept in circumstances where a preservation duty is triggered.⁶⁷

E. Guideline Five: Reasonableness and Proportionality Should Govern Discovery Obligations Relating to Ephemeral Messaging Data in U.S. Litigation

Ephemeral messaging data that is stored temporarily is electronically stored information (ESI), even if it may not be reasonably accessible in certain circumstances.⁶⁸ ESI that does

(ordering the production of documents with employee names, titles, employment dates, organization charts, and other materials reflecting personal data and holding that a protective order would sufficiently safeguard such information for GDPR purposes).

66. See *Salt River*, 2018 WL 1382529, at *3–4.

67. See Section IV.C, *supra*.

68. See FED. R. CIV. P. 34(a)(1) advisory committee note to 2006 amendment (“Rule 34(a)(1) is expansive and includes any type of

not exist at the time a preservation duty triggers is not subject to a preservation obligation.⁶⁹

For prospective preservation obligations (i.e., where information is created after the duty to preserve attaches), preservation of relevant ephemeral messaging data may be required, though it will be limited by considerations of reasonableness. For example, it is generally recognized that the preservation obligation requires reasonable, good-faith efforts

information that is stored electronically . . . ‘in any medium,’ to encompass future developments in computer technology.”); *Columbia Pictures, Inc. v. Bunnell*, 245 F.R.D. 443, 446 (C.D. Cal. 2007) (holding that temporarily stored information is electronically stored information under Rule 34). If ephemeral messaging data is truly not “stored in any medium from which information can be obtained,” then such data would not qualify as “electronically stored information” for the purposes of discovery. FED. R. CIV. P. 34(a)(1) advisory committee note to 2006 amendment.

69. *See, e.g.*, FED. R. CIV. P. 37(e) advisory committee note to 2015 amendment (“court decisions hold that potential litigants have a duty to preserve relevant information when litigation is reasonably foreseeable”). For example, courts have not sanctioned parties that configured instant messaging systems to not retain messages. *See, e.g.*, *Williams v. UnitedHealth Group*, No. 2:18-cv-2096, 2020 WL 528604 (D. Kan. Feb. 3, 2020) (finding that defendant did not violate its preservation or production duties by configuring its Cisco Jabber instant messaging system to not retain instant messages); *King v. Catholic Health Initiatives*, No. 8:18-cv-326, 2019 WL 6699705 (D. Neb. Dec. 9, 2019) (holding that defendant did not have a preservation or production obligation relating to instant messages generated by its Microsoft Lync instant messaging system where it designed that system to not retain instant messages). *But see Franklin v. Howard Brown Health Ctr.*, No. 1:17 C 8376, 2018 WL 4784668 (N.D. Ill. Oct. 4, 2018); *report and recommendation adopted*, 2018 WL 5831995 (N.D. Ill. Nov. 7, 2018) (imposing sanctions on defendant for failing to preserve relevant messages from its instant messaging system where defendant configured the system to keep messages for up to two years).

as opposed to perfection.⁷⁰ The determination of this issue could largely depend on the preservation capabilities of the particular application used.⁷¹

Spoliation may occur when a party fails to take reasonable steps to preserve data that is lost and cannot be restored or replaced through additional discovery.⁷² Nevertheless, courts in U.S. litigation should be aware that organizations—particularly with cross-border operations—may use ephemeral messaging to comply with international and domestic privacy norms, along with other corporate objectives.⁷³ As a result, courts should not reflexively presume that ephemeral messaging has been implemented to avoid common law preservation obligations.⁷⁴

70. FED. R. CIV. P. 37(e) advisory committee note to 2015 amendment (“This rule recognizes that “reasonable steps” to preserve suffice; it does not call for perfection.”); *DR Distribs. v. 21 Century Smoking, Inc.*, --- F. Supp. 3d ---, 2021 WL 185082, at *54 (N.D. Ill. Jan. 19, 2021) (“Though a party need not preserve all documents in its possession—again, perfection is not the standard—it must preserve what it knows and reasonably ought to know is relevant to possible litigation and is in its possession, custody, or control.”); The Sedona Conference, *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1, 108, 111 (2018) (providing that “the obligation to preserve normally requires reasonable and good faith efforts” and that a “party’s preservation obligation does not require ‘freezing’ of all ESI”).

71. See Section IV.C, *supra*.

72. FED. R. CIV. P. 37(e).

73. Guideline Five focuses on U.S. litigation in federal courts. Nevertheless, the principles discussed in Guideline Five would be applicable to U.S. state courts or investigatory litigation as well.

74. *Contra WeRide Corp. v. Kun Huang*, No. 5:18-cv-07233, 2020 WL 1967209 (N.D. Cal. Apr. 24, 2020) (imposing terminating sanctions against defendants for, among other things, deploying an enterprise grade ephemeral messaging application (DingTalk) ostensibly to circumvent a

Instead, courts should examine the nature and use of ephemeral messaging against the recommendations memorialized in Guideline Two and Guideline Three of this *Commentary*. In the absence of contrary circumstances, courts may consider a litigant's use of ephemeral messaging that accords with Guideline Two and Guideline Three as being reasonable and executed in good faith. In contrast, it may be appropriate for courts to infer culpable intent with respect to prospective preservation obligations if a litigant's key custodians of relevant information begin to use or continue using ephemeral messaging *after* a duty to preserve has triggered.⁷⁵

As with all preservation obligations, the parties and the court must also consider proportionality factors.⁷⁶ Factors particularly applicable to the preservation of relevant ephemeral messaging data include the accessibility of the information, the relative burdens and costs of the preservation effort, and the probative value of the information.⁷⁷ Privacy considerations, along with the other proportionality

preservation order and to prevent the discovery of relevant communications).

75. See *id.*; *Herzig v. Arkansas Found. for Med. Care, Inc.*, No. 2:18-cv-02101, 2019 WL 2870106 (W.D. Ark. July 3, 2019).

76. See FED. R. CIV. P. 26(b)(1) and 37(e), including advisory committee's note to 2015 amendment: "[T]he routine, good-faith operation of an electronic information system would be a relevant factor for the court to consider in evaluating whether a party failed to take reasonable steps to preserve lost information." The Sedona Conference, *Commentary on Legal Holds, Second Edition: The Trigger & The Process*, 20 SEDONA CONF. J. 341, 367 (2019) (discussing at Guideline 6 that "[f]ulfilling the duty to preserve involves reasonable and good-faith efforts . . . applied proportionately.").

77. *Commentary on Legal Holds, Second Edition*, *supra* note 76, at 367 (Guideline 7). See also The Sedona Conference, *Commentary on Proportionality in Electronic Discovery*, 18 SEDONA CONF. J. 141, 150 (2017).

standards—the importance of the issues at stake in the action, the amount in controversy, and the parties’ respective available resources for discovery—are other factors that may merit consideration by the parties and court.⁷⁸

Even if ephemeral messaging technologies enable the preservation of relevant data, a blanket requirement to create records of ephemeral messaging content—thereby converting such content to non-ephemeral information—while litigation is pending could be too onerous.⁷⁹ This is particularly the case where organizations have implemented ephemeral messaging to advance business imperatives such as data minimization, security, and confidentiality.⁸⁰ Instead, it could be appropriate

78. Compare *Henson v. Turn, Inc.*, No. 15-cv-01497-JSW (LB), 2018 WL 5281629 (N.D. Cal. Oct. 22, 2018) (forbidding unfettered discovery of plaintiffs’ web browsing and related social media history given their privacy interests in certain information) with *In re Mercedes-Benz Emissions Litig.*, No. 16-cv-0881 (KM) (ESK), 2020 WL 487288 (D.N.J. Jan. 30, 2020) (finding that a protective order would adequately protect cross-border privacy interests during discovery in U.S. litigation). See also *Commentary on Proportionality in Electronic Discovery*, *supra* note 77, at 168–73 (explaining that privacy rights should be taken into account when determining the application of proportionality standards); Agnieszka A. McPeak, *Social Media, Smartphones, and Proportional Privacy in Civil Discovery*, 64 U. KAN. L. REV. 235 (2015) (arguing that privacy should be a factor in the proportionality analysis).

79. See *Commentary on Legal Holds, Second Edition*, *supra* note 76, at 395–96 (“Absent a showing of special need, *The Sedona Principles, Third Edition* states that a responding party should not be required to ‘preserve, review, or produce deleted, shadowed, fragmented, or residual [ESI].’”).

80. Notably, preservation of ephemeral messaging data may be unnecessary. Regulatory requirements may already mandate creation and retention of certain business records, and ephemeral communications are unlikely to be used for business records to which other retention requirements already apply. See, e.g., Home Mortgage Disclosure Act of 1975, 12 U.S.C. 2801 (1976) (requiring retention of certain information about

to treat an ephemeral message like a phone call rather than an email and refrain from imposing a duty to create and maintain records of *all* ephemeral messaging data.⁸¹ At the same time, organizations should be cognizant that the adoption and use of ephemeral messaging carries risks both in civil litigation and regulatory investigations.⁸²

If ephemeral messaging data satisfies notions of relevance and proportionality,⁸³ a court may then need to determine whether the data is reasonably accessible.⁸⁴ In connection with its analysis of this issue, a court may examine the nature of the ephemeral messaging applications at issue. For applications that do not have the technical functionality to preserve and in fact do not retain an active version of the data, a court may then consider whether such data is either not reasonably accessible because of undue burden or cost, or completely

mortgage applications for three years); Occupational Safety and Health Standards, 29 C.F.R. pt. 1910 (1993) (applying specific retention periods for payroll records, tax forms, human resource records, and other employee files); Federal Deposit Insurance Corporation Record Retention Requirements, 12 C.F.R. pt. 380.14 (2016) (mandating retention of internal company retention policies); Health Care Portability and Accountability Act, 45 C.F.R. pt. 160 (2007) (requiring maintenance of certain records under the “security rule”).

81. Although there is no duty to create a recording of a phone call, for example, a company that already records conversations for business purposes would have a duty to preserve those recordings. *See E*Trade Secs. LLC v. Deutsche Bank AG*, 230 F.R.D. 582, 590 (D. Minn. 2005).

82. *See* Section IV.B, *supra*.

83. *See* FED. R. CIV. P. 26(b)(1).

84. *See* FED. R. CIV. P. 26(b)(2)(B). The limits under Federal Rule of Civil Procedure 26(b)(2)(C) would also apply, including whether the discovery is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive. FED. R. CIV. P. 26(b)(2)(C)(i)-(iii).

inaccessible. For purely ephemeral messaging applications with automated deletion and E2E encryption that eliminates encryption keys, any remnants of that content will likely be completely inaccessible and beyond recovery. In contrast, data from quasi-ephemeral messaging applications may be recoverable as not-reasonably-accessible data, depending on the nature of an application's storage and encryption features.⁸⁵

85. Although certain ephemeral messaging applications give users the ability to save some data, the mere existence of such settings should not convert ephemeral messages to "reasonably accessible" data given the burden that retention may impose in the face of data protection regulations and security considerations. *See* Section III.A.1, *supra*.