wgs

The Sedona Conference

Commentary on Ephemeral Messaging

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

January 2021
Public Comment Version
Submit comments by March 28, 2021,
to comments@sedonaconference.org

The Sedona Conference Commentary on Ephemeral Messaging

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

JANUARY PUBLIC COMMENT VERSION

Author: The Sedona Conference

Editor-in-Chief
Philip J. Favro

Contributing Editors
Stacey Blaustein
Oliver Brupbacher
Guillermo Santiago Christensen
Andrea D'Ambra
Robert DeCicco
Starr Turner Drum
David K. Gaston
Alan Geolot
Jennifer L. Joyce
Agnieszka McPeak
Hon. Anthony E. Porcelli

Steering Committee Liaisons
Denise E. Backhouse
Taylor Hoffman
Wayne Matus

Staff Editors
David Lumia
Michael Pomarico

Preface

Welcome to the public comment 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 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 thank Bennett Arthur for his 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 meetings where drafts of this *Commentary* were the subject of the dialogue. On behalf of The Sedona Conference, I thank all of them for their contributions.

Please note that this version of the *Commentary* is open for public comment, and suggestions for improvement are welcome. Please submit comments by March 28, 2021, to comments@sedonaconference.org. The editors will review the public comments and determine what edits are appropriate for the final version.

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
January 2021

Table of Contents

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 factors are considerations 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 considerations make ephemeral messaging an attractive communication option for organizations and their employees.

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

---

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 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.*, 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).

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 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 a company. 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 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 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

---

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).

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

7 *See* Section IV, *infra.*

Also available as part of the eCourse
Discoverability of Mobile Devices, New Technology and Social Media Platforms

First appeared as part of the conference materials for the
2021 E-Discovery Essentials session
"Discoverability of Mobile Devices, New Technology and Social Media Platforms"