The Sedona Conference Draft Guidelines for Addressing Ephemeral Data in Cross-Border Litigation (June 2019)

The Sedona Conference Draft Guidelines for Addressing Ephemeral Data in Cross-Border Litigation

(June 2019)

Drafting Team:

Phil Favro (Drafting Team Leader)

Bennett Arthur

Stacey Blaustein

Oliver Brupbacher

Guillermo Christensen

Andrea D'Ambra

Robert DeCicco

Starr Drum

David Gaston

Alan Geolot

Jennifer Joyce

Agnieszka McPeak

Denise Backhouse (Steering Committee Liaison)

Hon. Anthony Porcelli (Judicial Advisor)

I. INTRODUCTION

Ephemeral data is increasingly used around the globe. And for good reason. With its ability to automate the destruction 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 the enhanced ability to communicate confidentially, may also facilitate compliance with data protection and privacy laws. Indeed, these laws—particularly the European Union ("EU") General Data Protection Regulation ("GDPR"[1])—are a predominant consideration driving organizations toward the use of ephemeral data.

Beyond these factors are matters such as culture, convenience, and ease of use. Users find that ephemeral messaging facilitates keeping communications confidential and enhances their ability to collaborate and communicate without significant IT infrastructure. All of these considerations make ephemeral messaging an attractive communication option for organizations and their employees.

Despite the growing use of ephemeral data, there are obstacles to widespread adoption. Those obstacles include resistance from government regulators such as the U.S. Department of Justice ("U.S. DOJ") and the U.S. Securities & Exchange Commission ("U.S. SEC"). The U.S. DOJ and the U.S. SEC have adopted policies that expressly oppose organizational adoption of ephemeral messaging. While the U.S. DOJ recently modified its policy to arguably soften its position on the issues, the fact remains that government regulators in different parts of the world are against the use of ephemeral messaging.[2]

Other impediments to ephemeral messaging include the legal obligation in common law countries that parties preserve potential evidence for litigation. For example, civil litigation in U.S. federal and state courts generally requires litigants to at least keep information relevant to the claims and defenses in a particular action. Once the common law duty to preserve attaches, continued use of ephemeral messaging may cause relevant data to be destroyed in violation of that duty.

These and similar competing demands spotlight a clear tension. On the one hand, there are laws, organizational practices, and cultural factors driving the use of ephemeral data. At the same time, certain laws, regulations, policies, and legal duties militate against the use of ephemeral data. This tension has created a quandary for organizations wishing to implement ephemeral technologies. Irrespective of the basis for that implementation, organizations need direction on how they should address these competing demands. This is particularly the case for entities seeking to use ephemeral data to comply with data protection directives without violating other legal requirements.

---

[1] The General Data Protection Regulation [hereinafter GDPR] is a single, binding EU-wide regulatory framework (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, text *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN), which became effective on May 25, 2018.

[2] *See*, *e.g.*, Paul Karp, *Coalition's deal with Labor on cracking encrypted messages – what it means for you*, THE GUARDIAN (Dec. 5, 2018), *available at* https://www.theguardian.com/australia-news/2018/dec/05/coalitions-deal-with-labor-on-cracking-encrypted-messages-what-it-means-for-you (discussing the impact of Australia's new encryption cracking law on, among other things, the use of ephemeral messaging).

These conflicting concerns have led The Sedona Conference to prepare a commentary that encompasses a series of guidelines, which provide informed direction to organizations on how they should navigate the landscape of uncertainty surrounding the use of ephemeral data. Section II of the Commentary defines the nature and scope of ephemeral data—particularly ephemeral messaging technologies—for purposes of the guidance memorialized in this paper. In Section III, the Commentary next provides a detailed sketch of the tension and competing demands facing organizations that wish to use ephemeral technologies. Section IV then delineates the respective recommendations that provide guidance on the issues. While the guidance should prove helpful for organizations, it should also assist decision makers such as government regulators and judges in responding to ephemeral data use and addressing conflicting obligations that organizations may confront in using ephemeral technologies.

II. Ephemeral Data—Nature and Scope

Ephemeral is generally defined as "lasting a very short time"[3] and data as "information in digital form that can be transmitted or processed."[4] Leveraging these definitions, ephemeral data may simply be defined *as information in digital form, lasting a very short time, that can be transmitted or processed.*

Ephemeral data is *intended* to be short-lived. It is generally characterized as being dynamic and non-static in nature.[5] Ephemeral data is often defined by the technology that creates this data, specifically the functionality of the technology that enables automatic disposition or expiration of that data. Today, ephemeral data most often refers to communications (written or spoken) that are generated by end-users using an electronic messaging and collaboration platform. These platforms enhance communications in both personal and professional settings and are changing the way in which companies do business.

These platforms offer specialized functionality to delete data automatically or after a pre-defined duration, most often a very short time. The automated destruction feature eliminates data residing on the user's device *and* the devices of those who either sent or received the messages in question. For some technologies, the destruction of such content is instantaneous upon closing the message. For other applications, users can set a period of time—from moments to days or even months—before such information is discarded. They can also modify retention and destruction periods by sender or recipient.

Ephemeral messaging may also offer additional features including message encryption.[6] All of which provide the user with enhanced control over the disposition of messages and enables the technology to supports the messages' ephemeral nature, in that they are intended to last for a brief period of time.

---

[3] https://www.merriam-webster.com/dictionary/ephemeral
[4] https://www.merriam-webster.com/dictionary/data
[5] *See The Sedona Conference Primer on Social Media, Second Edition*, 20 SEDONA CONF. J. 1, 10 (forthcoming 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.")
[6] *See id.* 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.").

A. Ephemeral Data of The Past

Ephemeral data is the opposite of a persistent data structure or a "data structure that always preserves the previous version of itself when it is modified." [7] From an information technology ("IT") perspective, ephemeral data refers to electronic data and files that were generated by a system process, such as a temporary file. For example, when an end-user wanted to print a paper copy of an Microsoft Office document, "Windows creates temporary files on the hard disk… spools the print job to the temporary file and then sends it to the appropriate printer as a background operation."[8] After the document is successfully printed and the end-user closes the Microsoft Office application, "these (temporary) files are closed and deleted by Windows when you quit a Windows session." Generally, these temporary files—"stored in random access memory (RAM) and caches"—are considered "temporary, transient files" which are ultimately "deleted as often as every few hours."[9]

B. The Evolution of Ephemeral Data in Communications

The evolution of ephemeral data mirrors the transition from an analog to a digital world. Traditional telephone calls using land lines, or even mobile calls using cellular towers, were (and still are) routinely considered ephemeral data. As traditional forms of instant messaging technology were introduced, many companies considered instant messages to be ephemeral.

Instant messaging act as an electronic conversation, mimicking a telephone call through a real-time dialogue between two or more parties. Most "conversations" were not intended to be memorialized, recorded or otherwise maintained since they are dynamic and not considered to have long term value for an organization. In contrast to a telephone or mobile calls, instant messages left a trail of digital artifacts beyond a list of in-bound and out-bound calls. Nevertheless, companies typically let these artifacts expire, be overwritten, or left them otherwise untouched.

By the early to mid-2000s, organizations began using instant messaging as an alternative to email correspondence and telephone calls. [10] This rise in instant messaging as an enterprise communication platform, combined with several regulatory requirements to capture electronic communications, led to a shift in the way companies treated this ephemeral data source.[11] Organizations began to evaluate whether instant messaging needed to be retained to support compliance with regulatory requirements while also considering the discoverability of this data source for legal disputes.

[7] https://www.netlingo.com/word/ephemeral-data.php
[8] https://support.microsoft.com/en-us/help/92635/windows-temporary-files
[9] https://www.netlingo.com/word/ephemeral-data.php. *See generally* Kenneth J. Withers, *"Ephemeral Data" and the Duty to Preserve Discoverable Electronically Stored Information*, 37 UNIV. OF BALTIMORE L. REV. 349 (2008) (discussing the nature and characteristics of ephemeral data).
[10] https://www.vyopta.com/blog/uc-industry/history-unified-communications-retro-tech-included/ ("people were inundated with instant messaging options both in their personal lives as well as at work;" as employees could now see whether their colleagues were online and available, its "usage really skyrocketed for larger businesses.").
[11] *See*, *e.g.*, 17 C.F.R. § 240.17a-4(b)(4); 17 C.F.R. § 275.204-2; FED. R. CIV. P. 34(a).

Technology advances also allowed for the retention of subsets of instant messaging by an employee or department while also providing a mechanism to suspend the automatic expiration of messages in order to preserve it for investigations or litigation.

C. Ephemeral Data of Today

The rise in use of instant messages as an enterprise communications platform gave way to a number of new technologies that provided an alternative to traditional phone calls, email, and instant messages in both personal and professional settings. A single messaging and collaboration platform may be capable of creating several types of ephemeral data including chats, messages, and voice and video recordings. While traditional landline and mobile telephone services did not have the technology available to retain content of calls ("record the conversation") or capture much more than a minimal number of metadata elements (depending on service provider, the availability of metadata such as, for example, inbound and outbound calls or call duration, may vary), these platforms have the technology to do so though they expire data by design.[12]

The ephemeral data of both yesterday and today essentially remain the same: *Information in digital form, lasting a very short time, that can be transmitted or processed*. The systems and applications presently being used to create ephemeral data provide additional functionality to support a variety of information risks and concerns, including data security, data privacy, data minimization, and other information governance best practices. It is this definition—and particularly how it applies to contemporary ephemeral messaging technologies—that provides the scope of the guidelines encapsulated by the instant *Commentary*.

III. TENSIONS ASSOCIATED WITH THE USE OF EPHEMERAL DATA

The use of ephemeral data creates tensions due to competing policies and perspectives. Various legal, security, data governance, technological, and cultural policies and considerations around the globe encourage greater privacy and data controls. The objectives of these collective considerations are, in turn, supported or advanced by ephemeral technologies.

On the other hand, longstanding policies in the U.S. and elsewhere discourage the use of ephemeral data. For these stakeholders, the focus is on the importance of access to relevant data in legal and regulatory proceedings and police investigations. Because ephemeral applications can permanently delete data that may be relevant to a legal or regulatory proceeding or police investigation, organizations may be reluctant to adopt these technologies. Indeed, in various regulated industries, data must be preserved for specified time periods. The use of ephemeral technologies that deletes data before the expiration of those periods would violate those regulatory requirements. As a result, organizations must consider carefully the potential operational, legal, and regulatory risks of adoption of ephemeral data applications.

[12] *See generally* Agnieszka McPeak, *Disappearing Data*, 2018 WIS. L. REV. 17, 32 (2018); Agnieszka McPeak, *Self-Destruct Apps: Spoliation by Design?*, 51 AKRON L. REV. 749 (2017).

This section explores in more depth the policies and perspectives that support and oppose the use of ephemeral data applications.

A. Policies and Factors that Encourage the Use of Ephemeral Data Applications

1. Data Privacy and Control

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 focused more on monetizing the value of customer data instead of protecting it, users have become aware that their online data may not be secure.[13] As a result, interest has grown in possible legislative and regulatory responses that give users more protection and control over their data and allow data minimization to reduce their data footprint.

a. Privacy Laws and Regulations

The EU has taken the strongest steps to address privacy issues with the GDPR. This regulation establishes data protection and privacy requirements for data of individuals within the EU and governs the export of personal data outside the EU. Organizations not established in the EU but that process data in the EU, offer goods or services in the EU, or monitor behavior within the EU, or to which EU law applies due to public international law, are generally subject to its requirements. The GDPR gives individuals rights over their personal data, including rights of transparency, notice, access, rectification of inaccurate or incomplete data, erasure, portability, and the right to restrict processing. Data controllers must ensure that data is maintained securely, that they take data minimization steps in collecting and retaining only data necessary for the purpose for which it was collected, and that they retain such data only for as long as needed. Organizations must have policies in place to respond to requests relating to an individual's data, and violation of GDPR requirements could have severe consequences, as the GDPR provides for penalties of up to 4% of global revenues.[14]

Various other regions and countries have recently enacted or updated data protection laws to enhance privacy safeguards in the digital age. This includes Argentina, Australia, Brazil, Hong Kong, Israel, New Zealand, and Singapore. China, too, has safeguards for data privacy against misuse of personal data by private companies.

In the U.S., most of the movement on data privacy has originated within state governments.[15] In 2016, New York State promulgated cybersecurity regulations requiring financial institutions to

---

[13] *See* Christopher Mele, *Data Breaches Keep Happening. So Why Don't You Do Something*, NEW YORK TIMES (Aug. 1, 2018), *available at* 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), *available at* https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.

[14] *See* Adam Satariano, *Google Is Fined $57 Million Under Europe's Data Privacy Law*, NEW YORK TIMES (Jan. 21, 2019) *available at* 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).

[15] *But see* Federal Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers* , FTC Report (March 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-

develop and implement cybersecurity policies.[16] And California enacted in 2018 the California Consumer Privacy Act to take effect in 2020, which gives individuals more control over their data and creates a private right of action for individuals whose data is breached.[17]

As a result of the GDPR and various national laws and regulations on data privacy, focus on ephemeral data applications that offer features such as data minimization and encryption will likely increase, as such applications minimize data, reduce the volume to be securely maintained and reduce the risks of unauthorized disclosure or breach if the data is encrypted.

2. Data Management

With the massive increase in the volume of data generated by organizations, data management practices have evolved to adjust to new technologies and the shift from manufacturing to service and information industries. These changes include the adoption of management policies that favor the use of ephemeral data applications to address the new data management realities. Those realities include global organizations with worldwide operations; heightened risk of data breach; data available throughout an organization and therefore easier to access, but harder to track and store securely. Encryption and privacy by design are examples of such policies and principles where ephemeral data applications can play a role.

a. Encryption

Encryption involves the use of cryptography to take a plain text and, through use of keys and algorithms, transform that plain text into coded text that cannot be read. At the other end, the process is reversed to 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. It is the central component of ephemeral messaging applications that safeguard communicated data by making it unintelligible in the absence of the algorithm and keys.

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. Depending on the level of security required, it may be necessary to use encryption in conjunction with other ephemeral

commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (calling in the report for enhanced focus on privacy, data security, and data minimization of consumer personal data).

[16] New York Dept. of Financial Services, Cybersecurity Regulations, 23 NYCRR 500 (2016). These regulations required covered financial institutions to design a cybersecurity policy, establish reporting procedures and submit an annual report, and develop a full-scale cybersecurity program that also covers third party service providers.

[17] California Consumer Privacy Act, AB-375, California Civil Code § 1798.100 et seq.(signed into law June 28, 2018) allows California citizens 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. Companies that are victims of a data security breach can be subject to a civil lawsuit and be ordered to pay California residents statutory damages of $100-$750 per resident, or actual damages, unless the California Attorney General decides to prosecute the company instead of permitting civil suits. There are still a number of issues to be clarified about the law, and further revisions are anticipated.

data management methods. Encryption can, however, be a powerful tool to ensure that data does not fall into the hands of unintended recipients.

b. Privacy by Design

Privacy by design is an increasingly popular data management approach that 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 requires end-to-end security for the data at issue and directs operators to keep privacy as the default to ensure that data is automatically protected at all stages of its existence.[18] This emphasis on privacy encourages corporate adoption of ephemeral technologies to address privacy issues.

Indeed, the GDPR has adopted privacy by design as party of its regulatory framework, and use of ephemeral tools can facilitate GDPR compliance. In the case of a data breach, for example, Article 34(3)(a) of the GDPR states that a breach notification is not required to the data subject if a company has "implemented appropriate technical measures [that] render the personal data unintelligible to any person who is not authorised to access it, such as encryption."[19]

c. Information Governance

In light of the enormous growth of information, organizations have adopted policies that seek to manage the life cycle of data. Their focus is both on retention of data with ongoing business value and early identification and action to discard data without such value. Ephemeral data 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 data, offering any number benefits to the organization.

d. Data Security

Organizations may actively seek to use ephemeral data in situations where data security is paramount. For example, senior officials in pre-merger negotiations or similar situations requiring confidentiality may rely on ephemeral messaging to better ensure the communications are secure and reduce the likelihood they are subject to interception. Minimizing the amount of data vulnerable to compromise is one of the most effective means of ensuring data security and ephemeral tools may prevent hackers from gaining access to important data. Even if a mobile device is lost or otherwise compromised, for example, the automatic deletion of data provides more protection against loss.

e. Productivity

Large organizations are also taking advantage of ephemeral data to facilitate collaboration among employees in different locales. Certain tools allow personnel to work on a collaborative basis and establish data minimization processes that govern data retention on a platform and provides end-to-

[18] Ann Cavoukian, *Privacy by Design: The Seven Foundational Principles*, IAPP *available at* https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/.
[19] GDPR, Article 34(3)(a).

end encryption of data, which limits access to authorized users. These applications can enable compliance with the GDPR and enhance the ability of workers spread across the globe to work together on projects.[20]

3. Cultural Factors

Certain ephemeral technologies have been widely adopted on a worldwide basis. For example, WhatsApp, a messaging application offering end-to-end encryption, is estimated to have over 1.5 billion users in 180 countries, with the largest WhatsApp country markets being India (200 million users) and Brazil (120 million users). In some markets, including the Netherlands, Spain and Italy, WhatsApp has achieved penetration of over 80%.[21] Another popular messenger service, Snapchat, which features deletion of messages after review, reports that it has approximately 190 million daily active users, with approximately 79 million North American active users and 60 million European active users. Its services appear to be particularly popular with the young, reaching 90% of those between the ages of 13-24, and 75% of all 13-34 year old users in the U.S.[22] Ephemeral tools have become popular in part because of the control they provide to users in disseminating and deleting data as they choose.[23] Wide scale acceptance of these applications makes it likely that ephemeral data will continue to be popular into the foreseeable future.

B. Factors that Discourage Use of Ephemeral Data Applications

Ephemeral data applications create substantial challenges for an organization's information retention practices. In practice, prudent retention policies balance the usefulness of an organization's data against the risks of data destruction. Traditionally, these polices have been designed for tools that centrally organize and collect data and allow time for decision-making and adjustment. Ephemeral data disrupts this approach. These tools feature automatic destruction capabilities that force records management decisions to occur at the beginning of the data lifecycle. This shift removes the safety net that traditional retention policies offer. Where data can be destroyed immediately after creation or consumption, organizations have little opportunity to adjust their retention policies to reflect changed needs or new threats. Accordingly, the risks and consequences of improper data destruction are amplified and must be considered before an ephemeral data application is deployed.

The risks of improper data destruction impact an organization in three key ways. First, data destroyed may retain an operational business value for an organization. When operational data is destroyed prematurely, critical data such as financial records, contracts, key communications, or

[20] Wickr materials.
[21] WhatsApp Revenue and Usage Statistics (2019), available at http://www.businessofapps.com.
[22] Snapchat Company Profile (Apr. 23, 2019).
[23] Ephemeral data 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.

work product may be lost before the business use of the asset has expired, creating losses in the form of additional costs to remediate lost data.

Second, the consequences of improper data destruction in a legal context can be substantial. Organizations face obligations to retain information important for legal matters that may arrive unexpectedly and extend for years. Non-compliance with legal retention requirements may impact the organization's ability to assert or defend its claims, run afoul of discovery obligations, or invite further scrutiny into its affairs. These outcomes are costly to resolve and enhance the risk of improper data destruction.

Finally, government regulatory requirements can compel regulated organizations to retain certain classes of information with robust penalties in place for non-compliance. For organizations impacted by these regulations (data management regulations may be found in various sectors including technology services, finance, health care, and government), ephemeral data requires considerations beyond operational and legal risks to avoid additional scrutiny and costs.

Each risk (operational, legal, and regulatory) applies where ephemeral data applications are deployed in an organization, especially where a functional understanding of a tool's ability to control and create data is neglected before adoption. Further, many ephemeral data applications are dynamic platforms – features may be removed, changed, or added without the knowledge or consent of the organization, thereby adding unpredictability to data resources that are volatile by design. These factors may persuade a decision-maker to reject calls to adopt ephemeral data applications, creating conflict with those who advocate for the business advantages these tools can offer.

C. Understanding the Risks of Ephemeral Data

The risks of ephemeral data applications draw from specific operational, legal, and regulatory guidelines and standards and will be discussed below.

1. Regulatory Risks

Regulatory risks pose a significant risk for organizations where information governance must adhere to regulatory controls. Some industries (e.g., financial and health) have stricter retention requirements than others, including various reporting and audit requirements. The risk strategy for these organizations requires a robust retention policy that may require preservation of records unrelated to an assessment of operational and legal risk. The strategy must also be flexible as regulatory authorities can change the scope of what must be preserved with limited notice and grave consequences for violative conduct. Moreover, the use of ephemeral data tools requires measures to affirmatively indicate to regulatory authorities that the tools are not being used to obscure or destroy information required for preservation.

There is not a single standard to predict successful compliance; however, there are several prevailing sources of guidance for the use of ephemeral data. One example comes from the U.S. DOJ for organizations seeking to demonstrate cooperation in Foreign Corrupt Practices Act ("FCPA") investigations. 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."[24] Nevertheless, this guidance should be construed in the context of the U.S. DOJ's historical antipathy toward the use of ephemeral data.[25]

Similarly, 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.[26]" Taken together, organizations should expect close attention to their use of ephemeral data applications from regulatory and investigative authorities as this technology becomes more prevalent. The costs of modeling data retention policies to emerging regulatory standards, and the outcomes of failure, are risks that should be considered carefully for any regulated organization considering ephemeral data applications.

2. Legal Risks

There are clear legal risks in the adoption of ephemeral data applications. For organizations subject to common law jurisdiction, a primary consideration is compliance with the duty to preserve information pertinent to potential or active litigation.[27] Failure to comply with this duty exposes an organization to legal consequences that can significantly add to the time and costs required to litigate a matter. As a result, the duty to preserve creates a separate and distinct set of risks that may engage records beyond those normally retained for operational utility. Navigating these risks requires practices and policies that anticipate challenges to what was automatically destroyed—as well as what was preserved—using ephemeral data applications. As noted previously, certain ephemeral technologies could remove the safety net of traditional information management practices, such as an organization's ability to suspend the elimination of information routinely destroyed by ephemeral data. Ephemeral tools can also present a separate evidence spoliation risk: as information must be preserved for an organization's claims *or defenses*, it is feasible that an organization could unwittingly destroy exculpatory evidence or records otherwise favorable to its position in the regular use of ephemeral data.

3. Operational Risks

As the operational needs of an organization are case-by-case and tailored to disparate business interests, few factors are generally applicable to all organizations. However, key questions can be

[24] *See United States Department of Justice: Justice Manual* 9-47.120(3)(c) – FCPA Corporate Enforcement Policy (2018), *available at* https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977 (last visited May 29, 2019).
[25] *See* 9-47.120(3)(c) – FCPA Corporate Enforcement Policy (Nov. 29, 2017), *available at* https://www.justice.gov/criminal-fraud/file/838416/download (last visited Mar. 28, 2019) ("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.").
[26] *See National Exam Program Risk Alert*, OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS (Dec. 14, 2018), *available at* https://www.sec.gov/files/OCIE%20Risk%20Alert%20%20Electronic%20Messaging.pdf (last visited Mar. 28, 2019).
[27] *See* Arthur Andersen LLP v. United States, 544 U.S. 696, 704 (2005); Micron Tech., Inc. v. Rambus Inc., 645 F.3d 1311, 1322 (Fed. Cir. 2011).

anticipated as an organization weighs the risks of adopting an ephemeral data platform. The questions are especially complex for multinational organizations.

First, an organization must decide what records fall within and outside the scope of "business records or communications."[28] Targeting the universe of records with ongoing business value defines where the risks of data destruction are costliest. These potential costs must be balanced against the advantages that ephemeral data applications offer. In some cases, the risk of destruction may be too catastrophic to chance tools that automatically destroy data without a second review. Conversely, identifying records with operational value separates business records from data assets with only incidental or casual applicability to the organization's work. For these records, prudent removal by ephemeral technologies may reduce the organization's overall risk and decrease operational costs.

Next, an organization must evaluate the actors creating organizational data. Ephemeral data applications are, ultimately, only effective if an organization's employees understand and correctly use these tools. Any deviation from the tool's intended use introduces risks and costs that may only be discovered years after a tool's deployment. To understand if ephemeral data would reduce or enhance an organization's' risk profile, the organization must engage in a realistic evaluation of its actors with questions such as the following: Can the organization successfully prohibit or restrict methods of communication that their employees are already using widely? Can the organization enforce ephemeral communications among a workforce unaccustomed to ephemeral data applications? Can an organization's employees be trusted to correctly classify the retention period of their own communications? Can each decision be defended if challenged?

Finally, an organization must constantly consider the controls ephemeral data applications offer for retention. There is no clear line yet between ephemeral and non-ephemeral data. At the same time, ephemeral communication models are constantly and rapidly evolving. Because there is no distinct guidance for ephemeral data applications, retention decisions must be revisited whenever controls are added (or removed) from a tool to appropriately calibrate risk. Organizations should reevaluate where ephemeral tools rank in their overall data retention strategy: as the needs of an organization change, ephemeral data applications in use may require greater (or fewer) retention controls to maintain a defensible retention policy.

IV. GUIDELINES

A. Corporate Information Governance Programs Should Actively Manage Ephemeral Data Applications

1. *It should be recognized in principle by all stakeholders (in litigation and legal actions, investigations, regulatory matters, etc.) that non-static and ephemeral data represents a data source of increasing significance that meets real communication needs and may be used for legitimate reasons.*

This guidance is premised on the understanding that automatic message deletion, as burn-on-read or with only very short-term data retention, and end-to-end encryption, as typically offered by

[28] *See United States Department of Justice: Justice Manual* 9-47.120(3)(c) – FCPA Corporate Enforcement Policy (2018), *available at* https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977 (last visited May 29, 2019).

ephemeral messaging applications, can serve legitimate interests and offer significant business benefits.

Such benefits come in the form of *confidentiality and security* for sensitive electronic information in the face of increasing cybersecurity and other threats of inadvertent disclosure.[29] *Data minimization* likewise embraces those benefits given the explosion in data volumes and in satisfying laws and regulations such at the GDPR. Limiting the retention of organization data that has no business value is recognized both as a good information governance practice and a key component of privacy by design.[30] As such, ephemeral data is becoming more common as a fundamental design feature of new IT applications.

It is important to recognize these benefits because they help answer concerns about ephemeral data that mainly arise in four areas: recordkeeping, data preservation, regulatory scrutiny, and cross-border data transfers.[31] These concerns can impact a party's legal interests as well as its reputation as the use of ephemeral data has, in some cases, been viewed as an attempt to hide bad behavior.[32] This view, however, is evolving as regulators and other interested parties better understand the legitimate business purposes ephemeral data addresses. Indeed, most recently the U.S. DOJ's 2019 FCPA Corporate Enforcement Policy abandoned its former bright-line prohibition for organizations seeking cooperation credit to use software that generates, but does not appropriately retain, business records or communications, and instead now grants organizations more latitude to adopt software and record retention policies that meet their legitimate needs. This change seems to recognize that ephemeral messaging in business environments is growing and that stakeholders should increasingly stop short of concluding—barring special circumstances—that a party is seeking to eliminate evidence for some nefarious purpose whenever it elects to use an ephemeral system for communicating.

2. *Where the use of ephemeral data may appear to conflict with legal or regulatory requirements, such requirements should be drafted and interpreted in a way that allows for the use of ephemeral data unless or until there is an overriding need to retain information for legal or regulatory compliance purposes.*

The nature of ephemeral data and messaging may conflict with *recordkeeping* requirements that exist in corporate laws and in standards set by regulatory authorities. By definition, the use of ephemeral data makes it (near) impossible to keep records. Ephemeral data is the opposite of a "record" in that

[29] 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).
[30] Cf. Internet of Things. Privacy & Security in a Connected World (FTC Staff Report, January 2015), at 33 et seq.; article 1(c) GDPR.
[31] *See* Section IV.A.2, *infra.*
[32] Most recently, the Report On The Investigation Into Russian Interference In The 2016 Presidential Election by the Special Counsel Robert S. Mueller, III (at 10) held that "some of the individuals were interviewed or whose conduct we investigated – including some associated with the Trump Campaign – 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. In such cases, the Office was not able to corroborate witness statements through comparison to contemporaneous communications or fully question witnesses about statements that appeared inconsistent with other known facts. Accordingly, ... the Office cannot rule out the possibility that the unavailable information would shed additional light on (or cast in a new light) the events described in the report."

it is not (or should not be) a "communication with continuing business value." This fundamental tension can only be resolved by controlling the uses and content of ephemeral messaging, e.g., through the application of respective policies.[33]

Second, the use of ephemeral data may conflict with *preservation* obligations in the context of litigation or investigations. As with other types of data, preservation obligations for ephemeral data arise once a party reasonably anticipates litigation.[34]

The concern with ephemeral messaging is that, even then, the design of most ephemeral data applications does not allow for a suspension of routine document destruction. To the extent that ephemeral data is truly not "stored in any medium from which information can be obtained," such data should not qualify as "electronically stored information" for the purposes of discovery.[35]

Ephemeral data that is temporarily stored, even briefly, is considered ESI,[36] but at least for information created before the duty to preserve is triggered, ephemeral data is not available anymore because it was automatically and irrevocably deleted immediately or shortly after its creation. ESI that does not exist at the time the duty to preserve is triggered is not subject to preservation obligations. Thus, to the extent a preservation obligation relates to only retrospective data (i.e. data created before the duty is triggered), there is likely to be no ephemeral data available for preservation. This is because ephemeral messaging applications ordinarily delete the messages either upon reading or after a minimal period of time from the sender's and the recipient's device as well as from the provider's server, meaning that the data cannot be restored from anywhere.[37]

It should also be noted that with respect to prospective preservation obligations (i.e. where the duty to preserve includes any newly created information), preservation of relevant ephemeral data may be required, though it may be limited by proportionality and other considerations of reasonableness. For example, there is inevitably a lag between when a party reasonably anticipates litigation and when it is reasonably able to implement preservation holds. It is generally recognized that the preservation obligation requires reasonable good faith efforts as opposed to perfection.[38]

---

[33] *See* Section IV.A.3, *infra*.
[34] *See*, *e.g.*, FED. R. CIV. P. 37(e), 2015 committee note ("court decisions hold that potential litigants have a duty to preserve relevant information when litigation is reasonably foreseeable").
[35] FED. R. CIV. P. 34(a)(1)(A).
[36] See, *Columbia v. Bunnell*, 245 F.R.D. 443, 446 (C.D. Cal. 2007) (holding that temporarily stored information is electronically stored information under Rule 34).
[37] *See* Section II, *supra*.
[38] *See* FED. R. CIV. P. 26(b)(1); The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production, Vol. 19, No. 1 (2018) Comment 5.e ("The preservation obligation for ESI does not impose heroic or unduly burdensome requirements on parties. Rather, the obligation to preserve normally requires reasonable and good faith efforts.") and Comment 5.g ("A party's preservation obligation does not require "freezing" of all ESI, including all email. Parties need not preserve "every shred of paper, every e-mail or electronic document, and every backup tape," nor do they have to go to extraordinary measures to preserve "all" potentially relevant ESI.")(internal citations omitted).

Ephemeral data may not fall within the definition of ESI under Rule 34.[39] For these types of ephemeral communication, parties may want to implement policies and procedures to limit ephemeral messaging to non-substantive communication once the duty to preserve attaches.[40]

As with all preservation obligations, parties need to consider proportionality factors.[41] Factors that may be considered include the accessibility of the information, the relative burdens and costs of the preservation effort, and the probative value of the information.[42] Depending on the IT application used, ephemeral data is either not preservable at all, or requires significant efforts to preserve. In particular, where the potential value of the information is expected to be low, such as where ephemeral messaging is used for non-substantive communication,[43] the burdens and cost of preservation are likely disproportionate. Accordingly, absent reasonable technological solutions or a showing of special need to the court, a party should not be required to preserve, review, or produce ephemeral data even where such data would be available.[44]

Consideration should also be given to the nature and degree of personal information that is potentially subject to discovery. Privacy considerations are a proportionality factor and may outweigh discovery interests, particularly where requests to preserve and produce such information are unreasonably overbroad.[45]

Where ephemeral data comes within the scope of *regulatory scrutiny*, it is proposed that authorities should follow the example of the U.S. DOJ's 2019 FCPA Corporate Enforcement Policy refraining from any bright-line prohibition of ephemeral messaging, unless business records are implicated. Instead, government regulators should focus on the existence and implementation of guidance and controls on the use of ephemeral messaging platforms. Accordingly, the advice for organizations should be to have appropriate policies in place.

Conflicts with legal or regulatory requirements may arise where ephemeral messaging serves to fulfill applicable requirements in one jurisdiction, but by so doing potentially conflicts with obligations in another jurisdiction. This is the case with *cross-border data transfers*, in particular where the understanding and roles of discovery, retention, and data privacy differ between legal regimes—such

---

[39] *See* Section II, *supra*.
[40] *See* Section IV.A.3, *infra*.
[41] *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* (Public Comment Version, December 2018), Guideline 6: "Fulfilling the duty to preserve involves reasonable and good-faith efforts ... applied proportionately."
[42] The Sedona Conference *Commentary on Legal Holds*, *supra* Note 33, Guideline 7. See also The Sedona Conference *Commentary on Preservation, Management and Identification of Sources of Information That Are Not Reasonably Accessible*, 10 SEDONA CONF. J. 281, 291 (2009); The Sedona Conference *Commentary on Proportionality in Electronic Discovery*, 18 SEDONA CONF. J. 141, 150 (2017).
[43] *See* Section IV.A.3, *infra*.
[44] The Sedona Conference, *Commentary on Legal Holds*, *supra* note 33, at 27.
[45] *See* Henson v. Turn, Inc., No. 15-cv-01497-JSW (LB), 2018 WL 5281629 (N.D. Cal. Oct. 22, 2018) (forbidding discovery of plaintiffs' web browsing and related social media history given their privacy interests in such information). *See also* 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).

as between common law and civil law proceedings—and where, accordingly, conflicts may arise between data retention and data minimization requirements. In such cases, international comity requires due regard to the statutory requirements of the jurisdiction where the data originated when assessing the required level of data retention with respect to local data minimization rules.

3. *Organizations should consider addressing concerns about the use of ephemeral data by implementing an appropriate information governance and monitoring advances in technology.*

Adopting ephemeral technologies and monitoring compliance with a policy governing an organization's use of ephemeral data may address some of the aforementioned conflicts by demonstrating reasonableness and good faith. A defined policy and evidence of compliance should provide strong support if an organization is called upon to demonstrate the reasonableness of its use of ephemeral data.[46] Ephemeral technologies may be addressed in a mobile device policy, an acceptable use policy, or a larger corporate information governance policy.

Such a policy may limit the use of ephemeral messaging to non-substantive communications, thereby helping ephemeral communication to steer clear of what would otherwise constitute a business record or other information of continuing business value. The policy may also require users to select non-ephemeral methods of communication regarding matters that could be relevant to pending or reasonably anticipated litigation or investigations. Exceptions may be granted where ephemeral data is used for one-way communication from the organization to recipients only and where, at the same time, a backend system is available that stores the substance and metadata of the communication. This may be the case with informational or promotional material that is checked internally for compliance with professional practices and other policies before distribution to external recipients.

Organizations should also closely follow the advances of technology and actively select the ephemeral tools they wish to permit for use. Where possible, applications may be chosen that offer enterprise versions and, hence, a structured use of ephemeral messaging. This stands in contrast to individual, unstructured, one-off use by employees of their personal applications for business purposes. Such enterprise versions may allow organizations to proactively administer the application and information generated therein. Organizations can then, for example, set their own retention times for information and metadata (such as distribution lists for the communications) that may be different from the provider's. They may also offer certain discovery (including preservation and collection) functions on the back end, obviating the need to access an employee's device. Finally, some enterprise versions of ephemeral messaging allow for a separation between business and private information, the commingling of which may otherwise limit an organization's ability, under certain applicable data privacy laws, to access or otherwise process the ephemeral data.

B. Adopting a Fair and Balanced Approach to Defining Retention and Preservation Duties for Ephemeral Data

1. Cross-Border Litigation

[46] The Sedona Conference *Commentary on Legal Holds*, Guideline 2, at 18.

In cross-border litigation, the differing requirements concerning discovery, retention, and privacy must be taken into account when evaluating the use or limitations on the use of ephemeral data, as parties may find themselves with competing, inconsistent obligations.[47] Where ephemeral data is potentially subject to preservation requirements in a common law legal proceeding and subject to protection under international data protection laws, courts and parties should consider competing requirements and make appropriate accommodations accordingly. If a conflict is found, the parties—and if needed, the court—should endeavor to define the appropriate scope of preservation 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 proportionality considerations.

Parties seeking to exclude ephemeral data from the scope of preservation should be prepared to thoroughly explain their rationale to litigation adversaries and to the court, understanding that there may be a lack of familiarity with, or recognition of, data protection laws that contravene the scope of discovery. Parties seeking to include such data within an adversary's preservation scope should be prepared to recognize that where ephemeral data is used in good faith for purposes of satisfying the data minimization principles of cross-border data protection laws or other legitimate business objectives, the analysis will likely weigh against preserving that ephemeral data for U.S. civil litigation.

To minimize potential cross border discovery disputes, organizations can implement ephemeral data in ways that diminish the conflicting risks involved with common law preservation requirements and international data protection laws. Companies evaluating these tensions should consider and compare the potential consequences for violating those preservation obligations versus international data protection requirements. For example, while sanctions arising from preservation failures should generally be "no greater than necessary" to cure any resulting prejudice, the regulatory consequences for violating a data minimization or pseudonymization principle or failing to obtain required consent for the disclosure of personal information could be far greater.[48] To address the preservation and data minimization conflicts, organizations should evaluate whether to deploy ephemeral solutions in limited geographic regions, specific company divisions or whether to implement ephemeral solutions offering mechanisms that allow for preservation in circumstances where the duty is triggered.

2. Judicial Treatment of Ephemeral Data

Courts should adopt a fair and balanced approach to discovery and preservation of ephemeral data to allow for the benefits of data minimization while avoiding prejudice to organizations that have adopted ephemeral technologies to comply with privacy norms or otherwise advance legitimate corporate objectives.

---

[47] *See generally* The Sedona Conference International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition), *available at* https://thesedonaconference.org/download-publication?fid=573 (2017) (describing tension between U.S. discovery and preservation obligations and non-U.S. data protection laws). *See also* French Penal Law No. 80-538 (blocking statute prohibiting the transfer of data for the purpose of discovery in foreign litigation); *In re Advocat "Christopher X,"* Cour de cassation Paris, crim., Dec. 12, 2007 No. 7168 (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).
[48] *See* GDPR art. 83.5; China Telecommunication Regulations, Article 66 ("The content of telecommunications shall not be examined for any reason by any organisations or individuals . . . Without prior permission, Telecommunication service providers and their employees shall not provide the contents transmitted by the users through the networks to others.").

Some ephemeral applications store no data and lack the technical ability to save content in any meaningful way. Applications that provide for digital communications with no record retention capacity may fall outside the definition of "electronically stored information" altogether.[49]

To the extent data from ephemeral technologies exists, it is not exempt from the general scope of discovery, as long as it is non-privileged, relevant information. Notably, ephemeral data discovery is still subject to proportionality and other limits.[50]

For ephemeral tools that retain some sort of data, any ESI within these applications may be inaccessible. If discovery poses an undue burden or cost, it may only be discoverable subject to a showing of good cause by the party seeking discovery and other limits imposed by courts, like cost-shifting. [51]

More likely, however, the substance of ephemeral data may no longer exist at all by the time discovery is sought. Instead, litigants may need to rely on application metadata, witness testimony, or other sources of evidence.[52]

The fact that ephemeral applications retain little, if any, records raises concerns regarding preservation in common law countries. Preservation duties may apply once litigation is anticipated or pending. But courts have noted that litigants do not have a duty to *create* a record where one otherwise does not exist.[53] In particular, spoken word conversations like telephone calls generally do not need to be recorded even if a litigant possesses the technical capability to do so.[54] Similarly, ephemeral technologies that create no records at all should not necessarily fall within a duty to preserve.

Even if an ephemeral tool contains features that allow users to save some data, a blanket requirement to create records of ephemeral information—thereby converting ephemeral data to

---

[49] *See, e.g.*, Columbia Pictures Indus. v. Bunnell, No. CV 06-1093FMCJCX, 2007 WL 2080419, at *3 (C.D. Cal. May 29, 2007) (server log data temporarily kept within computer's random access memory is "electronically stored information" within the scope of discovery)

[50] *See* Section IV.A.2, *supra*.

[51] ESI discovery is potentially limited when it is "not reasonably accessible because of undue burden or cost." FED. R. CIV. P. 26(b)(2)(B). In such instances, the party seeking discovery may need to make a showing of good cause before being granted discovery and the court may craft limits or use cost-shifting to modify discovery. *See id.* Notably, companies do not have a duty to store data in an accessible format. *See, e.g., Quinby v. WestLB AG*, No. 04Civ. 7406(WBP)(HBP), 2005 WL 3453908, at *8 n.10 (S.D.N.Y. 2005).

[52] *See, e.g.*, L.Z. v. K.Q., No. A-4776-14T3, 2016 WL 3865840, at *5 (N.J. Super. Ct. App. Div. July 18 2016) (accepting plaintiffs' testimony as to deleted Snapchat video's content to support Final Restraining Order).

[53] Alexander v. F.B.I., 194 F.R.D. 305, 310 (D.D.C. 2000) (noting that parties cannot be forced to create a list of names when such a list is not already in their possession, custody, or control); Secs. and Exchange Com'n v. Canadian Javelin Ltd., 64 F.R.D. 648 (S.D.N.Y. 1974) (no duty to create a deposition transcript); Soetaert v. Kansas City Coca Cola Bottling Co., 16 F.R.D. 1, 2 (W.D. Mo. 1954) (holding that Rule 34 only allows for discovery of things already in existence).

[54] *See Malletier v. Dooney & Bourke, Inc.*, No. 04 Civ. 5316 RMB MHD, 2006 WL 3851151, at *2 (S.D.N.Y. Dec. 22, 2006) (rejecting the spoliation argument and observing that the chatroom information likely contained little relevant content given the timeline of events).

non-ephemeral materials—while litigation is pending is too onerous in light of the positive reasons to use such applications. Instead, in most cases ephemeral data should be viewed more akin to a phone call than to email, and courts ordinarily should not impose a default duty to create and maintain records of all ephemeral data.[55]

Organizations should maintain information governance programs that also consider ephemeral technologies. To the extent an ephemeral application allows for saving content, the organization's policy should strike a balance between the benefits of ephemeral data and the need to keep certain records. But use of an ephemeral tool, without retention, may be reasonable for some information and should not be presumed to be nefarious or improper.[56]

Notably, preservation of ephemeral data may be unnecessary. Regulatory requirements may already mandate creation and retention of certain business records,[57] and ephemeral communications are unlikely to be used for business records to which other retention requirements already apply. In exceptional cases in which a party demonstrates a particular need for specific content, imposing a duty to preserve certain ephemeral communications may be reasonable.[58] Additionally, parties should consider whether preservation of ephemeral application metadata may suffice to meet the particular needs of a case.[59]

The mere use of ephemeral applications should not be viewed as spoliation of evidence. Spoliation may occur when a party fails to take reasonable steps to preserve data that cannot be restored or recovered through discovery.[60] Ephemeral application use, by itself, should not be viewed as prejudicial or as intentional spoliation. Instead, a more particularized showing should be required.[61]

---

[55] 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).

[56] *See generally* Arthur Andersen LLP v. United States, 544 U.S. 696, 704 (2005); Micron Tech., Inc. v. Rambus Inc., 645 F.3d 1311, 1322 (Fed. Cir. 2011); *see* Phillip M. Adams & Assoc., L.L.C. v. Dell, Inc., 621 F. Supp. 2d 1173, 1193 (D. Utah 2009).

[57] *See*, *e.g.*, Home Mortgage Disclosure Act of 1975, 12 U.S.C. 2801 (1976) (requiring retention of certain information about 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 (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"). *See also* Section III.C.3, *supra*.

[58] Cases that have required preservation of instant messages seem to note the business purpose of the particular record at issue and its relevance to the litigation. *See* Day v. LSI Corp., No. CIV 11-186-TUC-CKJ, 2012 WL 6674434, at *12 (D. Ariz. Dec. 20, 2012) (finding that instant messages should have been preserved because personnel decisions were made using the instant-message feature); Mikhlyn v. Bove, No. 08-CV-3367 (ARR)(RER), 2011 WL 4529613, at *6 (E.D.N.Y. Sept. 28, 2011) (imposing sanctions for failure to preserve Skype chats given their relevance).

[59] *See generally* The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production (2018), Principle 12.b.

[60] FED. R. CIV. P. 37(e) (addressing spoliation of electronically stored content).

[61] For example, spoliation sanctions may be proper if party decides to employ ephemeral communications after litigation is anticipated with an intent to deprive an adversary in litigation of relevant evidence. *See* Fed. R. Civ. P. 37(e). By contrast, a reasoned retention policy consistently employed before and during litigation helps support a party's reasonable and legitimate use of ephemeral applications. *See* Stevenson v. Union Pacific R. Co., 354 F.3d 739, 746 (8th Cir. 2004) (explaining that an adverse inference instruction may be improper when a company employed a reasonable document retention policy that "was not instituted in bad faith."); ClearOne Commc'ns, Inc. v. Chiang, No. 2:07 CV 37

C. Active Organizational Management of Ephemeral Data Sources

Understanding the purpose of each of the available ephemeral data technologies and the compliance or eDiscovery functionalities offered will help an organization make a more informed choice regarding which technology to select to best address regulatory, litigation and business needs.

As detailed more fully in the Appendix, the purpose of specific applications can range from social interaction to business collaboration and file sharing. Likewise, some technologies emphasize the immediate destruction of data, while others offer enterprise options with legal hold functionality that can be integrated with existing archiving solutions.

Among currently used applications Snapchat, for example, is designed for image-heavy social interaction, with messages deleted as soon as (or even before) the recipient closes the message.Vaporstream, at the other end of the spectrum, is a messaging and file sharing tool marketed solely to businesses, with compliance options that include admin consoles, archiving in client repositories, and audit controls that record all user activity.

The most important factors to consider when choosing an ephemeral data tool is whether the technology offers legal hold capabilities and the available retention periods. Wickr, for example, currently offers multiple plans ranging from a basic model with data retention limited to 30 days to an Enterprise plan with eDiscovery functionality and unlimited data retention. Slack, likewise, currently offers an eDiscovery API that allows messages and files to be exported to third party applications for archival and search purposes.

The various purposes and retention capabilities of the available technologies make possible a wide range of preservations options depending on an organization's industry, size, global presence, litigation profile, and appetite for destruction.

Some companies preferring to keep data for longer periods may value the security features of ephemeral messaging more than the opportunities for data minimization. They will therefore choose a technology with longer retention periods and the ability to effect legal hold functionality when the need arises. Others may prioritize minimizing the volume of data retained and may choose instead a technology with shorter retention periods, disabling the application entirely once litigation comes into play. Alternatively, companies may select a middle ground, allowing employees to communicate with ephemeral messaging until a legal hold obligation arises, at which time use of the application may be prohibited for any communications related to the matter.

The failure to create a policy covering preservation and retention of all forms of communication may lead to negative inferences and increased risk of sanctions. To address this, companies should consider creating a comprehensive written policy addressing ephemeral data regardless of which technologies are chosen.

TC, 2008 WL 704228, at *4 (D. Utah Mar. 10, 2008) (declining to impose sanctions where an email was deleted by the routine operation of a company's system).

The first step in this process is to create a committee of appropriate stakeholders, including officers from legal, IT, information security, and other departments with oversight over document management, in order to outline the acceptable and unacceptable uses of each technology.

Again, depending on the organization's specific needs and the type of technology adopted, the company may decide that acceptable uses should be limited to logistical communications (e.g., scheduling calls or meetings) or a slightly broader category of non-substantive communications. Alternatively, acceptable uses may include specific categories of business communications (e.g., discussions relating to internal investigations, sensitive financial information, or pre-merger discussions) or special circumstances (such as when there is a risk of unauthorized state access or when connection to the corporate VPN is not possible).

A company may also choose to adopt more than one technology in order to maximize the possible number of acceptable uses. For example, one application could be permitted for all employees but limited to logistical communications, while another could be permitted for specific departments for limited types of communications.

Once implemented, the ephemeral messaging data policy should be followed by comprehensive employee training and periodic auditing to ensure compliance. In order to provide even greater protection against sanctions or negative inferences from possible information loss, the company should consider performing a data mapping exercise to identify the specific employees who use ephemeral data, which technologies they use, and the subject matter they are permitted to discuss with those applications.

With sufficient documentation of acceptable uses, proactive mapping of data locations, and selection of appropriate technologies tailored to the organization's requirements, organizations can assess and manage risk in taking advantage of the benefits of ephemeral messaging.

D. Best Practices for Addressing Improper Uses of Ephemeral Data within the Enterprise

1. Ephemeral Technologies May Be Abused

Communication channels that leave few traces may be favored by those engaging in secretive activity possibly for nefarious or illicit purposes. In the U.S., a Washington insiders' adage states that one should never send an email when a phone call suffices, and never make a call when an in-person meeting is possible, and never say something when a nod can get the point across. Similarly, Goldman Sachs traders once coined the abbreviation "LDL" (let's discuss live) as a way to take an email discussion into a phone conversation to avoid creating a potentially incriminating trail.[62]

The potential for misuse of ephemeral data is that it can both facilitate more communication than would be possible by phone or in-person means by allowing the sharing of documents or other data. In addition, it may allow for the very existence of the communication to disappear, which may not

[62] Virginia Heffernan, *The Trouble With E-Mail*, THE NEW YORK TIMES (May 29, 2011), *available at* https://opinionator.blogs.nytimes.com/2011/05/29/the-trouble-with-e-mail/.

be possible with a telephone call or even an in-person meeting, especially with the myriad means of tracking phones.

For purposes of this commentary, the term "improper uses" of ephemeral data implies an intent to circumvent the law or perpetrate an action for an improper purpose using a platform or specific application where the data disappears, leaving no trace that a communication transpired.

Individuals, businesses, enterprises, and government officials communicate using a multitude of ephemeral communications applications such as Instagram, Confide, Wickr, Telegram Messenger, Tiger Text/Tiger Connect, Lynx and many others, where the information sent disappears after it is read by the recipient. No metadata remains such communications.

With the current trend toward proliferating privacy rights and data protection regimes, ephemeral messages with encryption functionality provide some reduction of the risk of a data breach and provide security of information that warrants protection. Using ephemeral data to satisfy those objectives is laudable and in line with security and privacy best practices in many situations. Nevertheless, there is the corresponding challenge for governments and companies to consider whether to permit or regulate the use of such applications, particularly in business or government settings that may involve regulations that require data retention. The nefarious uses of ephemeral data may be a consequence of an otherwise acceptable practice. For example, the common use of WhatsApp in many developing countries that lack reliable email communications can become "nefarious" if the intent of the users is to conceal evidence of wrongdoing.

The following discussion sets forth some examples of uses of ephemeral messaging to circumvent what should have otherwise been a preserved communication due to a legal duty to preserve; or were used in the course of business intentionally to evade having a record of what transpired so that no end-to-end data exists on the subject at issue. We do not address nefarious uses of ephemeral messaging (and end-to-end encryption) that are clearly on the wrong side of the law, such as terrorism, in this paper, although the considerations that arise in that context have an impact on the debate here. As is usually the case, the technology is not itself inherently good or bad – which makes the application and the use more challenging to regulate.

2. Best Practices

Ephemeral data is a valuable component for organizations where privacy has risen to the top of the list of individual rights and concerns. Nevertheless, specific policies must be created to clearly outline the valid operational reasons for using ephemeral technology, controlling its use, setting the appropriate retention duties to address use issues within the enterprise.

An organization's data preservation policy and communications, including any data retention directive, should address the use of ephemeral data and clearly extend the duty to preserve to records generated by said application. Otherwise, consideration should be given to prohibiting the use of ephemeral communications on these applications once a data retention order is instituted if the application does not allow for a default setting to save the communications. Some companies

may be unable to use or permit the use of ephemeral applications given regulatory requirements to preserve record traffic and this should be a key factor to be taken into account for any policy.

The technological limitations that are inherent with ephemeral data must also be factored in. The most widely used ephemeral technologies allow the user to set whether messages will be destroyed after a certain time or after being read. Others, aimed at enterprise level applications, provide a more centralized control. Companies that are aware of the use of ephemeral data by employees should consider this technological aspect when they develop their approach to a policy. A policy that cannot be implemented because the technology cannot be configured in the right way would not be likely to be treated with respect by a government regulator or judicial body.

Once a document retention order has been issued, the organization should have a specific contact or department that can deactivate the automatic deletion setting. It should also have a system implemented to audit and confirm with a record that the setting has been changed to archive communications and to make sure the deletion component of the tool remains inactive.

Clear instructions should be provided as to the usage functions of ephemeral data and that compliance by those who use the applications is assured and continued.