The Sedona Conference Journal®

Volume 20 ❖ 2019

Articles

The Sedona Conference®

Antitrust Law, Complex Litigation, and Intellectual Property Rights

The Sedona Conference Journal®

Volume 20

■

2019

The Sedona Conference Journal® (ISSN 1530-4981) is published on an annual or semi-annual basis, containing selections from the preceding year's conferences and Working Group efforts. The Journal is available on a complimentary basis to courthouses and public law libraries. Additionally, each issue is available for purchase ($45; $30 for Working Group Series members). Send us an email (info@sedonaconference.org) or call (1-602-258-4910) to order or for further information. Check our website for further information about our conferences, Working Groups, and publications: www.thesedonaconference.org.

Comments (strongly encouraged) and requests to reproduce all or portions of this issue should be directed to:
The Sedona Conference,
301 East Bethany Home Road, Suite C-297, Phoenix, AZ 85012 or
info@sedonaconference.org or call 1-602-258-4910.

The Sedona Conference Journal® designed by MargoBDesignLLC at www.margobdesign.com.

Cite items in this volume to "20 Sedona Conf. J. _____ (2019)."

Publisher's Note

Welcome to Volume 20 of *The Sedona Conference Journal* (ISSN 1530-4981), published by The Sedona Conference, a nonprofit 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, and intellectual property rights. The mission of The Sedona Conference is to move the law forward in a reasoned and just way through the creation and publication of nonpartisan consensus commentaries and advanced legal education for the bench and bar.

The various Working Groups in The Sedona Conference Working Group Series (WGS) pursue in-depth study of tipping-point issues, with the goal of producing high-quality, nonpartisan consensus commentaries that provide guidance of immediate and practical benefit to the bench and bar. The Sedona Conference conducts a "regular season" of limited-attendance conferences that are mini-sabbaticals for the nation's leading jurists, lawyers, academics, and experts to examine cutting-edge issues of law and policy. The Sedona Conference also conducts continuing legal education programs under The Sedona Conference Institute (TSCI) banner, an annual International Programme on Cross-Border Data Transfers and Data Protection Laws, and webinars on a variety of topics.

Volume 20 of the *Journal* contains four nonpartisan consensus commentaries from The Sedona Conference Working Group on Electronic Document Retention and Production (WG1) and one nonpartisan consensus commentary from the Working Group on Data Security and Privacy Liability (WG11). Additionally, this issue contains a timely new article addressing the proportionality of privacy concerns in discovery. I hope you find the commentaries and article to be thought-provoking pieces that stimulate further dialogue and ultimately serve to move the law forward.

For more information about The Sedona Conference and its activities, please visit our website at www.thesedonaconference.org.

Craig Weinlein
Executive Director
The Sedona Conference
July 2019

The Sedona Conference gratefully acknowledges the contributions of its Working Group Series annual sponsors, event sponsors, members, and participants whose volunteer efforts and financial support make participation in The Sedona Conference and its activities a thought-provoking and inspiring experience.

Journal Editorial Board

The Sedona Conference Advisory Board

Kevin F. Brady, Esq., Redgrave LLP, Washington, DC

Prof. Stephen Calkins, Esq., Wayne State Univ. Law School, Detroit, MI

Michael V. Ciresi, Esq., Ciresi Conlin LLP, Minneapolis, MN

Hon. John Facciola (ret.), U.S. Magistrate Judge, District of Columbia

Prof. Steven S. Gensler, Univ. of Oklahoma College of Law, Norman, OK

Prof. George A. Hay, Cornell Law School, Ithaca, NY

Ronald J. Hedges, Esq., Dentons US LLP, New York, NY

Allan Kanner, Esq., Kanner & Whiteley, L.L.C., New Orleans, LA

Hon. Paul R. Michel (ret.), U.S. Appellate Judge, Federal Circuit

Dianne M. Nast, Esq., NastLaw LLC, Philadelphia, PA

Hon. Nan R. Nolan (ret.), Redgrave LLP, Minneapolis, MN

Hon. Andrew J. Peck (ret.), DLA Piper, New York, NY

Jonathan M. Redgrave, Esq., Redgrave LLP, Washington, DC

Hon. James M. Rosenbaum (ret.), JAMS, Minneapolis, MN

Prof. Stephen A. Saltzburg, George Washington Univ. Law School, Washington, DC

Hon. Shira A. Scheindlin (ret.), Stroock, Stroock & Lavan LLP, New York, NY

Daniel R. Shulman, Esq., Gray Plant Mooty, Minneapolis, MN

Dennis R. Suplee, Esq., Schnader Harrison Segal & Lewis LLP, Philadelphia, PA

Prof. Jay Tidmarsh, Univ. of Notre Dame Law School, Notre Dame, IN

Barbara E. Tretheway, Esq., HealthPartners, Bloomington, MN

Hon. Thomas I. Vanaskie (ret.), JAMS, Philadelphia, PA

Hon. Ira B. Warshawsky (ret.), Meyer, Suozzi, English & Klein, P.C., Garden City, NY

Judicial Advisory Board

Hon. Jerome B. Abrams, Minnesota District Court Judge, First Judicial District

Hon. Michael M. Baylson, Senior U.S. District Judge, Eastern District of Pennsylvania

Hon. Laurel Beeler, U.S. Magistrate Judge, Northern District of California

Hon. Cathy A. Bencivengo, U.S. District Judge, Southern District of California

Hon. Cathy Bissoon, U.S. District Judge, Western District of Pennsylvania

Hon. Hildy Bowbeer, U.S. Magistrate Judge, District of Minnesota

Hon. Ron Clark, Senior U.S. District Judge, Eastern District of Texas

Hon. Joy Flowers Conti, Chief U.S. Distrct Judge, Western District of Pennsylvania

Hon. Mitchell D. Dembin, U.S. Magistrate Judge, Southern District of California

Hon. James L. Gale, Senior Judge, North Carolina Business Court

Hon. George C. Hanks, U.S. District Judge, Southern District of Texas

Hon. Susan Illston, Senior U.S. District Judge, Northern District of California

Hon. Kent A. Jordan, U.S. Appellate Judge, Third Circuit

Hon. Barbara M.G. Lynn, Chief U.S. District Judge, Northern District of Texas

Hon. Kristen L. Mix, U.S. Magistrate Judge, District of Colorado

Hon. Kathleen McDonald O'Malley, U.S. Appellate Judge, Federal Circuit

Hon. Katherine H. Parker, U.S. Magistrate Judge, Southern District of New York

Hon. Andrew E. Porcelli, U.S. Magistrate Judge, Middle District of Florida

Hon. Xavier Rodriguez, U.S. District Judge, Western District of Texas

Hon. Lee H. Rosenthal, Chief U.S. District Judge, Southern District of Texas

Hon. Elizabeth A. Stafford, U.S. Magistate Judge, Eastern District of Michigan

Hon. Gail J. Standish, U.S. Magistrate Judge, Central District of California

Hon. Patrick J. Walsh, Chief U.S. Magistrate Judge, Central District of California

Hon. Leda Dunn Wettre, U.S. Magistrate Judge, District of New Jersey

Table of Contents

THIS PAGE INTENTIONALLY LEFT BLANK

THE SEDONA CONFERENCE PRIMER ON SOCIAL MEDIA, SECOND EDITION

A Project of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1)

Author:

The Sedona Conference

Drafting Team:

Andrea D'Ambra
Michelle Greer Galloway
Alan C. Geolot
Julie Lewis
Lauren Schwartzreich
Amy E. Sellars

WG1 Steering Committee Liaisons:

Gareth Evans
Annika K. Martin
Ronni D. Solomon

Drafting Team Leaders and Editors-in-Chief:

Alitia Faccone
Philip Favro

Judicial Participant:

Hon. Kristen L. Mix

Staff Editors:

David Lumia
Susan McClain

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 1. 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, *Primer on Social Media, Second Edition,* 20 SEDONA CONF. J. 1 (2019).

PREFACE

Welcome to the final, February 2019, version of The Sedona Conference *Primer on Social Media, Second Edition*, a project of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). 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, and intellectual property rights. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The need for an updated *Primer* was essential given significant advances in social media technology since we published the first edition of The Sedona Conference *Primer on Social Media* in December 2012. The proliferation of messaging technology and its usage—on traditional social media platforms and in mobile messaging applications—have created preservation, production, and evidentiary challenges that counsel should learn to recognize and address. These and other issues led The Sedona Conference to organize a drafting team in 2017 to consider revisions to the 2012 *Primer*. A panel of speakers presented the proposed revisions at the WG1 2017 Midyear Meeting in Minneapolis. After receiving feedback on the proposal from WG1 members, the drafting team developed a first draft that was the subject of dialogue at the WG1 2017 Annual Meeting in Phoenix. The drafting team acted on the various recommendations the membership provided in Phoenix, which resulted in the public comment version of the *Primer* in July 2018. Where appropriate, the comments received during the public comment period have now been incorporated into this final version of the *Primer*.

The Sedona Conference wishes to thank Andrea D'Ambra, Michelle Galloway, Alan Geolot, Julie Lewis, Lauren Schwartzreich, and Amy Sellars for their efforts and commitments in time

and attention to this project. We also thank the Honorable Kristen L. Mix for serving as the Judicial Participant on the *Primer*. Finally, we acknowledge the efforts of Alitia Faccone and Philip Favro for serving as Drafting Team Leaders and Editors-in-Chief, and Gareth Evans, Annika Martin, and Ronni Solomon for their service as the WG1 Steering Committee Liaisons to the drafting team.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG1 and several other Working Groups in the areas of international electronic information management, discovery, and disclosure; patent damages and patent litigation best practices; data security and privacy liability; trade secrets; and other "tipping point" issues in the law. 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
February 2019

TABLE OF CONTENTS

I. INTRODUCTION

Social media is ubiquitous throughout most of the world, with users numbering in the billions irrespective of age, geography, or socioeconomic status. Not only consumers, but also governments and businesses employ social media to communicate with their constituencies and target audiences. With so many individuals and organizations communicating through social media, it is increasingly becoming a subject of discovery in litigation and investigations. Lawyers must understand the different types of social media and the unique discovery issues they present so they can advise and assist their clients in properly preserving, collecting, producing, and requesting such information in discovery.

The Sedona Conference initially addressed these issues when it published the first edition of *The Sedona Conference Primer on Social Media* in December 2012. The first edition described social media as a "fast-developing and fast-changing area of technical, social, and legal development." It also recognized the difficulty of proclaiming "any consensus-based commentary or set of principles" regarding discovery of social media because they "may be doomed to obsolescence as soon as [they are] announced on Twitter." This assessment has proven prescient as rapid change in social media technologies has rendered certain aspects of the first edition *Primer* obsolete.

The first edition of the *Primer* nonetheless has proven to be a useful resource on various information governance and litigation issues as it established a practical approach for addressing the corporate use and management of social media. It provided guidance regarding employee use of social media in the workplace at a time when there was little if any authoritative direction on these issues. The first edition of the *Primer* was also at the forefront of developing fundamental guidance on legal issues at the core mission of Working Group 1—the preservation,

collection, and production of electronically stored information (ESI).

Despite its initial and ongoing value, The Sedona Conference recognized a compelling need to update the *Primer*. Substantial changes in social media technology and its usage, together with the development of new social media jurisprudence, require a revised edition of the *Primer*.[1] In addition, The Sedona Conference has since published multiple commentaries that generally address information governance issues related to social media. In light of these developments, this edition of the *Primer* focuses exclusively on the discovery of social media in civil litigation.

Section II of the *Primer* discusses traditional and emerging social media technologies and the discovery challenges they present. Section III examines relevance and proportionality in the context of social media. It also explores preservation challenges, collection and search obligations, and the impact of the Stored Communications Act ("SCA"), together with review and production considerations. Section IV describes the impact of cross-border issues on social media discovery and Section V explores authentication issues. The *Primer* concludes in Section VI by analyzing ethical issues that lawyers should consider in connection with social media discovery.

1. *See* Agnieszka A. McPeak, *Social Media, Smartphones, and Proportional Privacy in Civil Discovery*, 64 U. KAN. L. REV. 235, 273 (2015) ("[S]ocial media's popularity, functionality, and ubiquity has grown in unprecedented ways since 2006.").

II. SOCIAL MEDIA AND EMERGING TECHNOLOGIES

Social media is a broad term that defies precise definition. Social media ranges from traditional platforms and messaging applications to collaboration tools and applications that stream live video. Formats include a combination of text (messages, status updates, comments, blog posts, etc.), photos, graphics, memes (photos with overlay text), infographics, maps (geographic location information), emojis, audio, video, or links to other content. While social media content varies from one site and application to the next, several consistent concepts continue to emerge: content is shared, interactive, internet-based, professional, or personal. Perhaps most significant for discovery, such content is typically dynamic, i.e., it may be easily modified or destroyed by the user, the recipient, the application provider, or by the technology itself.

As social media has expanded into many different areas, a precise definition has become more elusive, particularly since conceptions of what it is have been blurred. Numerous social and professional networking, collaboration, and communication applications may be considered social media. The Oxford English Dictionary defines "social media" as "websites and applications used for social networking." "Social network," in turn, is defined as "the use of dedicated websites and applications to communicate with each other by posting information, comments, messages, images, *etc*."[2] A common characteristic of all social media is the sharing of information—either personal information or, increasingly, work-related information—in either a targeted or broad fashion. Many social media applications have their own direct and group messaging functions, and

2. *Social Media,* CONCISE OXFORD ENGLISH DICTIONARY (12th ed. 2011) (emphasis in original).

many instant messaging applications have added features that are common to more traditional forms of social media.

Given the variety and fluidity of forms and formats, the *Primer* focuses on the different kinds of social media in the marketplace today, together with their respective discovery challenges. This includes a review of platforms and other traditional forms of social media, various types of messaging applications, live-streaming video applications, location-based social intelligence platforms, and devices using social media applications.[3]

A. Platforms and Other Traditional Forms of Social Media

Discovery of social networking content has generally focused on more traditional platforms, mainly because platform-based social media was the first type of online social networking to be widely embraced and widely used by consumers and organizations.

Although traditional platforms differ from one site to the next, these sites share many similar features. They allow users to post content to bulletin board-type locations. Privacy settings, when enabled, permit users some control over the initial distribution of their content.[4] Platforms also permit users to exchange messages directly with other users, known as "direct messaging." Direct messaging capability reflects responsiveness to consumer demand for a feature of traditional messaging applications.[5]

---

3. Social media data analytics platforms and content distribution portals for posting on social media sites are outside the scope of the *Primer*.

4. *See* Jacquelyn v. Macy's Retail Holdings, Inc., CV416-052, 2016 WL 6246798 (S.D. Ga. Oct. 24, 2016) (discussing the impact of privacy settings on the discoverability of relevant information).

5. *See infra* Section II(B).

Popular social media platforms include Facebook (a social networking site) and Twitter (an electronic bulletin board, social networking, and online news service). Other platforms include LinkedIn (a professional networking site), Instagram (mobile, desktop, and internet-based photo-sharing application and service), Flickr (a photo-sharing site), and YouTube (a site for posting and commenting on video footage). Many of these platforms were initially developed as consumer-based applications funded by advertising. Increasingly, however, businesses, governments, and political campaigns and organizations use these platforms for marketing and communication purposes.

For several years now, requesting parties in litigation have sought to obtain, and responding parties have attempted to preserve and produce, relevant content from social media platforms. Indeed, social media jurisprudence generally reflects discovery of platform-based social media. Some of the more common issues that arise in connection with discovery of platform-based social media include preservation and collection; the nature and scope of a particular request; the role of privacy settings; issues surrounding possession, custody, and control; and the role of the SCA.[6]

B. Messaging Applications

Messaging applications have grown exponentially since the first edition of the *Primer* was published in 2012. Indeed, reports indicate that users of messaging applications now outnumber users of social media platforms.[7] The advent of more advanced mobile device technology and consumer preference are primarily responsible for this phenomenon.

---

6. *See infra* Section III.

7. *See Messaging Apps Are Now Bigger Than Social Networks*, BUS. INSIDER INTELLIGENCE (Sept. 20, 2016), http://uk.businessinsider.com/the-messaging-app-report-2015-11?r=US&IR=T.

Relevant information can often be found on a wide variety of messaging applications. Nevertheless, messaging applications are not a homogenous class of data repositories. On the contrary, features such as communication functionality, user information, and content retention vary widely. The following is a brief overview of some of the more common messaging applications and the discovery challenges they may present.

1. "Over-The-Top" Messaging Applications

"Over-the-top" ("OTT") messaging applications were developed several years ago as an alternative to traditional text messages, i.e., short message service ("SMS") messages. Messages sent through OTT applications go directly through the internet from device to device. Unlike text messages, they do not pass through the message servers belonging to SMS providers (telecommunications companies such as Verizon or AT&T), private enterprises, or governmental entities.

OTT messaging applications generally offer users enhanced functionality at a lower cost than providers of traditional text messaging services.[8] Such functionality includes, among other things, the ability to send images and video, graphic overlay functionality, and the use of emojis and effects. Certain OTT messaging applications offer end-to-end message encryption. OTT applications generally fall into two categories: third-party applications and operating system-specific communication systems.[9]

---

8. *See* Janet Balis, *What an OTT Future Means for Brands*, HARV. BUS. REV. (May 13, 2015), https://hbr.org/2015/05/what-an-ott-future-means-for-brands.

9. *See* James Chavin, Aadil Ginwala & Max Spear, *The future of mobile messaging: Over-the-top competitors threaten SMS*, MCKINSEY & COMPANY, INC. (Sept. 2012), https://www.mckinsey.com/~/media/mckinsey/dotcom/%20client_service/Telecoms/PDFs/Future_mobile_messaging_OTT.ashx.

Third-party OTT messaging applications operate across multiple device platforms. This means that users can access application content on smartphones, tablets, laptops, and other devices. In addition, users can download and communicate with these applications on different operating systems (e.g., the Android and the iOS operating systems). Popular third-party OTT applications include WhatsApp, Snapchat, Signal, LINE, Facebook Messenger, and Kik.

In contrast are operating system-specific OTT messaging applications such as iMessage—offered exclusively by Apple through its iOS operating system. If an iMessage user sends a message from an iOS device to a device that uses the Android operating system, it is transmitted as a traditional SMS text message rather than as an OTT message. As a result, the enhanced features of iMessage will not be available.

2. Anonymous Chat and Messaging Applications

Anonymous chat and messaging applications allow users to communicate without disclosing their identities. They have grown in popularity due to the perceived freedom that anonymity provides. Anonymous applications such as Blind have been deployed in the workplace to encourage workers to provide candid feedback to their employers without fear of recrimination.[10]

Consumer versions of anonymous messaging applications (such as Whisper and Truth) generally appeal to high school and college students. They are group-oriented; any number of users in a specific geographic area can join in a discussion. Consumer-based applications have gained a certain amount of

10. *See* Rosa Trieu, *How Businesses Are Using Anonymous Blind App To Change Work Culture*, FORBES (July 2, 2016), https://www.forbes.com/sites/rosatrieu/2016/07/02/how-businesses-are-using-anonymous-blind-app-to-change-work-culture/#444d6a9eff81.

notoriety due to harassing messages exchanged by application users and other inappropriate conduct.[11]

3. Ephemeral Messaging Applications

Ephemeral messaging applications enable senders of a message to control its deletion, ranging from immediately upon reading the message (or even after reading each word of the message) to several hours, days, or weeks afterwards.[12] 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.[13] Consumer and enterprise-grade versions of these applications, also known as "self-destructing messages" and "disappearing messages," are available from Wickr and Confide. Other applications such as Facebook Messenger, Signal, and iMessage can be configured to include an ephemeral messaging feature.

4. Cloud-Based Messaging and Collaboration Applications for the Workplace

Cloud-based messaging and collaboration applications are designed to provide users with a more interactive communication platform than traditional enterprise communication tools

---

11. *See* Matt Burns, *After School Is The Latest Anonymous App Resulting In Student Cyberbullying And School Threats*, TECHCRUNCH (Dec. 3, 2014), https://techcrunch.com/2014/12/03/after-school-is-the-latest-anonymous-app-resulting-in-student-cyberbullying-and-school-threats/.

12. *See* Aarian Marshall, *Uber's Not The Only One That Should Be Wary Of Disappearing Messaging Apps*, WIRED (Dec. 17, 2017), https://www.wired.com/story/uber-waymo-wickr-ephemeral-messaging/.

13. *See generally* Agnieszka A. McPeak, *Disappearing Data*, 2018 WIS. L. REV. 17, 32 (2018) (discussing various technological features of ephemeral messaging applications).

such as email. Intended for the workplace, these applications have multifaceted functionality, including discussion lines for larger groups, one-on-one messaging exchanges, and confidential messaging channels to share sensitive information.[14] These applications typically maintain communicated content in cloud-based storage, though they may also be deployed on an enterprise's servers. Slack, Asana, HipChat, Jive, Microsoft Yammer, Salesforce Chatter, and VMware's Socialcast are examples of these applications.

5. Discovery Challenges with Messaging Applications

In addition to the discovery issues relating to social media platforms,[15] there are unique issues relating to discovery of relevant messaging application content, such as identifying the origin of anonymous application content. This process often requires unmasking application user identities, which can be a difficult and lengthy process.[16] Unveiling the identity of a message poster typically hinges on the detail of logs the software provider may maintain on the back end of its application and the duration of time it maintains the logs.

Preserving and collecting relevant messaging application content, particularly from OTT and ephemeral messaging applications, presents an additional challenge. Such content is

14. *See* Philip Favro, Donald Billings, David Horrigan & Adam Kuhn, *The New Information Governance Playbook for Addressing Digital Age Threats*, 3 RICH. J.L. & TECH. ANN. SURVEY ¶10 (2017).

15. *See supra* Section II(A).

16. *See* FAQs, BLIND, https://www.teamblind.com/faqs (last visited Dec. 28, 2018) ("[O]ur . . . infrastructure is set up so that user account and activity information is completely disconnected from the email verification process. This effectively means there is no way to trace back your activity on Blind to an email address, because even we can't do it. . . . [Y]our work emails are encrypted and locked away, forever.").

dynamic. In addition, messaging content is often not backed up or even retained by many application providers and may only be available on the device itself.[17] End-to-end encryption may also prevent access to message content.

C. Live-Streaming Video

Live-streaming video applications are another source that may contain relevant information in discovery. Users of these applications can now share live-streaming content with followers, friends, or others through any number of different applications or platforms, such as Periscope or Facebook Live. Users include organizations that are gravitating toward live video streams because it "is an easy and effective way to interact with people, especially if you use a question and answer style format or another medium that encourages participation."[18]

Discovery of data from live-streaming video applications involves many of the same issues as those involved in discovery of other social media. These issues include preservation and collection; relevance and proportionality; possession, custody, and control; and the SCA.[19]

D. Location-Based Social Intelligence Platforms

Location-based social intelligence platforms enable searching across social media sites for conversations by keywords and geo-fencing. Geo-fencing is a software feature that uses global

---

17. *See* Waymo LLC v. Uber Tech., Inc., No. C 17-00939 WHA, 2018 WL 646701 (Jan. 30, 2018) (holding that plaintiff could present evidence and argument to the jury regarding defendant's use of "ephemeral messaging" to eliminate relevant evidence).

18. Jason DeMers, *The Top 7 Social Media Trends That Dominated 2016*, FORBES (Dec. 7, 2016), https://www.forbes.com/sites/jaysondemers/2016/12/07/the-top-7-social-media-trends-that-dominated-2016/#7ae6d67c726c.

19. *See infra* Section III.

positioning system or radio frequency identification to define geographical boundaries.[20] To date, law enforcement and news reporters are the most prevalent users. Examples of companies developing and distributing the technology include DigitalStakeout, Echosec, Snaptrends, and Media Sonar.

The technology is still nascent and relies on the social media providers to feed data to these platforms through an application programming interface ("API").[21] Mass market adoption of these tools will depend on pricing, availability of data, privacy concerns, and government regulations.

Discovery involving location-based social intelligence platforms will likely focus on issues that are similar to those with other social media. Those issues include preservation and collection; relevance and proportionality; possession, custody, and control; and the SCA.[22]

E. Devices Using Social Media Applications

Devices are not social media sites in and of themselves. Nevertheless, devices in some instances have been designed to work

---

20. *See* Sarah K. White, *What is geofencing? Putting location to work*, CIO (Nov. 1, 2017), https://www.cio.com/article/2383123/mobile/geofencing-explained.html.

21. In March 2017, Facebook updated its policies to prohibit mass surveillance on its platform by explicitly blocking developers from obtaining user data for surveillance purposes. *See* Elizabeth Dwoskin, *Facebook says police can't use its data for 'surveillance,'* WASH. POST (Mar. 13, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/03/13/facebook-says-police-cant-use-its-data-for-surveillance/?utm_term=.ee98e286d96c. Those policy changes were criticized in 2018 after it was revealed that Cambridge Analytica (and likely other companies) circumvented those policies to mine Facebook users' data. *See The Facebook scandal could change politics as well as the internet: Even used legitimately, it is a powerful, intrusive political tool*, ECONOMIST (Mar. 22, 2018).

22. *See infra* Section III.

in conjunction with specific-purpose social media applications. In these circumstances, devices can be considered part of a social media system.

These devices include wearable technologies, which are electronic devices embedded in clothing, jewelry, shoes, or other apparel that transmit or receive data through wireless technology.[23] Users frequently use social media to communicate information found on their wearable technologies.

The data that wearable technologies generate often relates to the users of these technologies. It includes information relating to a user's physical condition and level of exertion (e.g., heart rate, blood pressure, sleep cycles, etc.), together with geolocation information (based on tracking exercise locations for higher-end models).[24] Strava, for instance, is an application that allows users to share publicly or with their authorized followers myriad details regarding their running, cycling, and swimming workouts.[25] Because wearable technologies (such as a smart watch) generally are considered temporary storage endpoints and synchronize with mobile and computer devices, they are likely redundant with traditional sources of information found on those technologies.

Additional examples of these devices may be smartphones or game consoles that are connected to the internet where social elements exist.[26] Whether in a smartphone or a stand-alone

23. *See* Nicole Chauriye, *Wearable Devices As Admissible Evidence: Technology Is Killing Our Opportunities To Lie*, 24 CATH. U. J. L. & TECH. 495, 499 (2014).

24. *See id*. at 500–02.

25. *See* Richard Pérez-Peña & Matthew Rosenberg, *Strava Fitness App Can Reveal Military Sites, Analysts Say*, NEW YORK TIMES (Jan. 29, 2018), https://www.nytimes.com/2018/01/29/world/middleeast/strava-heatmap.html.

26. Social media elements may also be found in social robots such as iPal and in devices that use artificial intelligence. Machine learning, based on

game console, these devices generate data such as user identities or game results that are designed to be shared over social channels. Examples of games played on these devices include Mafia Wars, FarmVille, and Pokémon.

Attempts to discover such data, whether communicated through social media sites or maintained on wearable technology, will encounter issues similar to those posed by platforms and messaging applications. They include preservation and collection; relevance and proportionality; possession, custody, and control; and the SCA.[27]

human behavior, is used to auto-generate code to better customize the social experience. *See* Robin Raskin, *Robots on the Runway*, HUFF POST (June 15, 2016), https://www.huffingtonpost.com/robin-raskin/robots-on-the-runway_b_10460902.html.

27. *See infra* Section III.

III. THRESHOLD DISCOVERY ISSUES

As social media usage becomes more widespread, the challenges of preservation, collection, review, and production of relevant information are receiving more attention. While procedurally social media is generally treated no differently from other requests for production, parties often battle over relevance, proportionality, and burden.[28] Disputes may be avoided or mitigated by considering the following issues when assessing whether to preserve, how to request with specificity, how to search for, and how to produce social media evidence:

- which social media sources are likely to contain relevant information;
- who has possession, custody, or control of the social media data;
- the date range of discoverable social media content;
- what information is likely to be relevant;
- the value of that information relative to the needs of the case;
- the dynamic nature of the social media and user-generated content;
- reasonable preservation and production formats; and

28. *See* United States *ex rel.* Reaster v. Dopps Chiropractic Clinic, LLC, No. 13-1453-EFM-KGG, 2017 WL 957436, at *1–2 (D. Kan. Mar. 13, 2017) ("while information on social networking sites is not entitled to special protection, discovery requests seeking this information should be tailored so as not to constitute the proverbial fishing expedition in the hope that there might be something of relevance in the respondent's social media presence") (quotation and citation omitted).

- confidentiality and privacy concerns related to parties and non-parties.

Some parties may also find it helpful to speak with opposing counsel before or during the meet and confer process regarding the discoverable information that will be sought or should be provided from social media sites.

This section is designed to provide guidance for addressing the most common discovery challenges associated with social media.[29]

A. Relevance and Proportionality

The scope of discovery for social media content is no different from other categories of information.[30] The threshold question remains whether social media evidence is "relevant to any

29. For additional guidance on these issues, see *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1 (2018) [hereinafter *The Sedona Principles, Third Edition*], and The Sedona Conference, *Commentary on Legal Holds, Second Edition: The Trigger & The Process*, 20 SEDONA CONF. J. 341 (2019), *available at* https://thesedonaconference.org/publication/Commentary_on_Legal_Holds.

30. *See* E.E.O.C. v. Simply Storage Mgmt., LLC, 270 F.R.D. 430, 434 (S.D. Ind. 2010) (indicating that discovery of social networking sites "requires the application of basic discovery principles in a novel context," and that the challenge is to "define appropriately broad limits . . . on the discoverability of social communications"); Winchell v. Lopiccolo, 38 Misc. 3d 458, 461 (N.Y. Sup. Ct. 2012) ("Discovery in this area is nonetheless governed by the same legal principles that guide more traditional forms of discovery."); Moore v. Wayne Smith Trucking Inc., No. Civ. A. 14-1919, 2015 WL 6438913, at *2 (E.D. La. Oct. 22, 2015) ("It is settled that information on social media accounts, including Facebook, is discoverable.").

party's claim or defense and proportional to the needs of the case."[31]

Social media evidence may be relevant in several ways, depending on the facts, circumstances, and legal issues in a particular case. It may reflect evidence relevant to a party's physical or mental state, geographic location, identity, or other information.[32] The *Primer* does not identify all types of relevant social media evidence as cases vary and social media sources are constantly evolving. Therefore, counsel should explore what social media their clients and opponents use and assess whether those sources of information may contain evidence relevant to the case. For example, even in a situation where social media evidence does not seem to impact issues of liability, it may be relevant to issues such as standing, damages, or good-faith participation in the judicial process. Because certain types of social media evidence can be readily destroyed (whether intentionally, unintentionally, or by a third party), counsel must take steps early in the case to assess the potential relevance of their client's social media content. Counsel must then help the client take reasonable steps to preserve it once a duty to preserve has been triggered.[33]

Courts generally reject efforts to obtain "all" social media postings or "entire" account data. This is because the entire contents of a social media source are not likely to be relevant in most

---

31. FED. R. CIV. P. 26(b)(1). The scope of discovery may differ in state court. *See, e.g.*, CAL. CIV. PROC. CODE § 2017.010 (permitting discovery that is "relevant to the subject matter").

32. *See* Roberts v. Clark Cty. Sch. Dist., 312 F.R.D. 594, 608 (D. Nev. 2016) (refusing a defendant's broad request for social media postings, but allowing discovery of posts made on the days plaintiff missed work and related to the plaintiff's physical or emotional state, physical condition and activity level, and damages).

33. *See infra* Section III(C).

cases, just as all of a party's emails are not likely to be relevant.[34] As with discovery of other ESI, a party is generally not entitled to inspect or obtain all data from a particular source.[35] The *Gordon v. T.G.R. Logistics* case is illustrative of this issue.

---

34. *See* Ye v. Cliff Veissman, Inc., No. 14-CV-01531, 2016 WL 950948, at *3 (N.D. Ill. Mar. 7, 2016) (denying motion to compel where defendants "have not limited the scope of their request to a relevant time period or to content that is relevant to a claim or defense in the case. Instead, they are asking for unfettered access to the Facebook archives of Plaintiff's decedent and her next of kin."); *Moore*, 2015 WL 6438913, at *2 (observing that parties are generally "no more entitled to such unfettered access to an opponent's social networking communications than . . . to rummage through the desk drawers and closets in his opponent's home"); Ogden v. All-State Career School, 299 F.R.D. 446, 450 (W.D. Pa. 2014) (denying in part defendant's motion to compel and explaining that defendant's request for "complete copies of [plaintiff's] social networking accounts would permit defendant to cast too wide a net and sanction an inquiry into scores of quasi-personal information that would be irrelevant and non-discoverable"); *Winchell*, 38 Misc. 3d at 461 ("digital fishing expeditions are no less objectionable than their analog antecedents.") (internal quotes omitted).

35. *See* Johnson v. PPI Tech. Servs., L.P., No. 11-CV-2773, 2013 WL 4508128 (E.D. La. Aug. 22, 2013) (requiring a threshold showing to avoid "unfettered access" to the opposing party's social media). *See also* Michael Brown, Sr. v. City of Ferguson, No. 4:15-cv-00831 ERW, 2017 WL 386544, at *2 (E.D. Mo. Jan. 27, 2017) (finding that disclosure of social media passwords would constitute unfettered access to those accounts); Farley v. Callais & Sons LLC, No. 14-2550, 2015 WL 4730729, at *8 (E.D. La. Aug. 10, 2015) (rejecting motion to compel login information, passwords, and real-time monitoring of Facebook account); Chauvin v. State Farm Mut. Auto. Ins. Co., No. 2:10-cv-11735-AJT-MKM, 2011 U.S. Dist. LEXIS 121600 (S.D. Mich. Oct. 20, 2011) (affirming an award of sanctions against defendant that filed a motion to compel a Facebook password as "intrusive"). Examples of courts ordering unrestricted production of social media content include where the requesting party presented evidence that the responding party had withheld relevant social media evidence. *See, e.g.*, Glazer v. Fireman's Fund Ins. Co., No. 11-cv-4374(PGG)(FM), 2012 WL 1197167, at *3 (S.D.N.Y. 2012) (ordering unrestricted production after court reviewed excerpts of electronic communications and concluded that "most, if not all, of them contain information that

In *Gordon*, the court curtailed the extent of the defendant's social media discovery request. The defendant had requested the "entire Facebook account history" of the plaintiff, arguing the information was relevant to plaintiff's claims of physical and emotional injury from a motor vehicle accident.[36] Subsequently, the defendant narrowed the request to the period of three years before the accident to the present. Considering the issue of scope, the court explained:

> Social media presents some unique challenges to courts in their efforts to determine the proper scope of discovery or relevant information and maintaining proportionality. While it is conceivable that almost any post to social media will provide some relevant information concerning a person's physical and/or emotional health, it also has the potential to disclose more information than has historically occurred in civil litigation.[37]

Turning to proportionality, the court observed that the request—though not unduly burdensome in terms of cost—was too burdensome given the nature and extent of the social media content it sought.[38] The court limited discovery to the period

---

is relevant"); Bass *ex rel.* Bass v. Miss Porter's School, 3:08-cv-1807, 2009 WL 3724968, at *1 (D. Conn. 2009) (ordering production of all Facebook materials following in camera inspection because "a number of [withheld] communications . . . are clearly relevant to this action").

36. Gordon v. T.G.R. Logistics, Inc., 321 F.R.D. 401 (D. Wyo. 2017).

37. *Id*. at 403.

38. *Id*. ("It's not difficult to imagine a plaintiff being required to explain every statement contained within a lengthy Facebook history in which he or she expressed some degree of angst or emotional distress or discussing life events which could be conceived to cause emotion[al] upset, but which is extremely personal and embarrassing.").

after the accident and to posts "which reference the accident, its aftermath, and any of her physical injuries related thereto."[39]

Counsel is responsible for reasonably investigating client social media content to identify relevant information and provide oversight of the search and production of such information.[40] In *Calvert v. Red Robin International*, a named plaintiff in a class action lawsuit failed to disclose relevant content from a social media account, including communications between the named plaintiff and putative class members regarding participation in the lawsuit.[41] The court rejected the arguments of plaintiffs' counsel that he was unfamiliar with social media technology and that he had no choice but to rely on his client's misrepresentations that all responsive documents had been produced. The court declined to impose sanctions on counsel at that time, waiting instead to determine if similar lapses occurred in the future.

Nevertheless, the court did grant a motion to disqualify the plaintiff as a class representative and awarded monetary sanctions against him. The plaintiff's communications with other putative class members about the case may have impacted any number of issues, including whether the plaintiff was an adequate class representative.

Calvert highlights counsel's duty to conduct a reasonable inquiry regarding a client's social media and to think broadly

---

39. *Id*. at 406.

40. *See e.g.*, FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment ("It is important that counsel become familiar with their clients' information systems and digital data—*including social media*—to address these issues. A party urging that preservation requests are disproportionate may need to provide specifics about these matters in order to enable meaningful discussion of the appropriate preservation regime.") (emphasis added).

41. Calvert v. Red Robin Int'l., Inc., No. C 11-03026, 2012 WL 1668980 (N.D. Cal. May 11, 2012).

about notions of relevance.[42] It also teaches that counsel must be competent (or partner with a competent lawyer) to facilitate appropriate discovery of this information.[43]

As with all discovery, even if social media information may be relevant, efforts to preserve, collect, and produce should still be proportional to the needs of the case. Similarly, requests for social media evidence should be made with specificity and be proportional to the needs of the case.[44]

1. Privacy Considerations

Privacy concerns are not a *per se* bar to discovery of relevant information, regardless of whether it is located in social media or elsewhere. Instead, privacy is more "'germane to the question of whether requested discovery is burdensome or oppressive and whether it has been sought for a proper purpose' rather than to affording a 'basis for shielding those communications from discovery.'"[45] The proportionality limitation on the scope of discovery includes two factors that implicate privacy concerns, i.e., "the importance of the discovery in resolving the

42. *See* FED. R. CIV. P. 26(g)(1).

43. *See infra* Section VI.

44. *See* Mackelprang v. Fid. Nat. Title Agency of Nev., Inc., No. 2:06-cv-00788-JCM-GWF, 2007 WL 119149, at *8 (D. Nev. Jan. 9, 2007) (denying defendant's motion to compel all information in plaintiff's Myspace accounts, because it amounted to a fishing expedition, but permitting "limited requests for production of *relevant* email communications," including social media "private messages that contain information regarding her sexual harassment allegations in this lawsuit or which discuss her alleged emotional distress and the cause(s) thereof").

45. Reid v. Ingerman Smith LLP, No. 2012-0307, 2012 WL 6720752, at *1 (E.D.N.Y. Dec. 27, 2012) (quoting E.E.O.C. v. Simply Storage Mgmt., 270 F.R.D. 430, 434 (S.D. Ind. 2010)).

issues, and whether the burden . . . of the proposed discovery outweighs its likely benefit."[46]

Privacy concerns should not be confused with discovery exclusions such as legal privileges or doctrines recognized under well-developed case law. Regardless of whether a person has a reasonable expectation of privacy in social media communications, a party may not use privacy expectations as a shield against discovery.[47] Nevertheless, requests for social media evidence should not be designed to harass or embarrass a party; nor should they be used as a tool to increase litigation costs.[48]

---

46. FED. R. CIV. P. 26(b)(1). *See* Henson v. Turn, Inc. No. 15-cv-01497-JSW (LB), 2018 WL 5281629 (N.D. Cal. Oct. 22, 2018) (analyzing the interplay between privacy and proportionality and discussing supporting cases).

47. *See* Forman v. Henkin, 30 N.Y.3d 656, 664 (2018) (holding that a requesting party need not identify relevant information in the "public" portion of a responding party's social-media account before being able to discover the "private" portion of that account); Michael Brown, Sr. v. City of Ferguson, No. 4:15-cv-0831 ERW, 2017 WL 386544, at *1 (E.D. Mo. Jan. 27, 2017) (rejecting a distinction between public content and private messages on Facebook and suggesting the parties seek recourse in a protective order to address remaining privacy concerns); Tompkins v. Detroit Metro. Airport, 278 F.R.D. 387, 388 (E.D. Mich. 2012) (holding that "material posted on a 'private' Facebook page, that is accessible to a selected group of recipients but not available for viewing by the general public, is generally not privileged, nor is it protected by common law or civil law notions of privacy"). *But see Henson*, 2018 WL 5281629 (finding plaintiffs' privacy interests in the information stored on their smartphones and computers outweighed defendant's interest in conducting a forensic examination of those devices to identify relevant information); McPeak, *supra* note 1, at 273 (asserting that privacy should be considered in connection with the proportionality analysis).

48. *See* FED. R. CIV. P. 1 (emphasizing that the Federal Rules of Civil Procedure (FRCP) "should be construed, administered, and employed by the court and the parties to secure the just, speedy, and inexpensive determination of every action"); FED. R. CIV. P. 26(g)(1)(B)(ii) (requiring counsel to certify that document requests are "not interposed for any improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation")

The same considerations regarding privacy apply to discovery of third-party information. While parties may pursue discovery of relevant social media content regarding third parties,[49] they should consider managing the discovery to minimize potential embarrassment to third parties and protect against unnecessary disclosure of their sensitive personal information.[50] Counsel should assess the scope of third-party information, its sensitivity, and whether it is intertwined with discoverable social media content such that it is part of relevant social media information to be produced. If intertwined sensitive third-party information exists, counsel should consider proactively addressing these issues through a good-faith attempt to confer.

---

and (B)(iii) (requiring that the requests are "neither unreasonable nor unduly burdensome or expensive, considering the needs of the case, prior discovery in the case, the amount in controversy, and the importance of the issues at stake in the action."); FED. R. CIV. P. 26(b)(c)(1) ("The court may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense.").

49. *Cf.* Marquez v. Bd. of Cty. Comm'rs Eddy Cty., No. 11-0838 JAP/KBM, 2015 WL 13638613, at *2 (D.N.M. Jan. 13, 2015) ("Plaintiff also contends that disclosure [of posts made to a private Facebook page] would interfere with the privacy of third-parties. Yet there is no expectation of privacy to comments made on another person's post or posts made on another person's page. Additionally, entry of a protective order, to which Defendants agree, would adequately protect third-parties from any potential embarrassment."); Higgins v. Koch Dev. Corp., No. 3:11–cv–81–RLY–WGH, 2013 WL 3366278, at *3 (S.D. Ind. July 5, 2013) ("Rachel and Sarah's claim that Koch's Request violates the privacy of their Facebook friends who have posted on their 'walls' and 'tagged' them in posts or other pictures is similarly unfounded."); Davenport v. State Farm Mut. Auto. Ins. Co., No. 3:11–cv–632–J–JBT, 2012 WL 555759, at *1 (M.D. Fla. Feb. 21, 2012) (ordering production of all relevant Facebook photographs "regardless of who posted the photograph").

50. *See* Carlson v. Jerousek, 68 N.E.3d 520 (Ill. App. 2d 2016) (emphasizing that courts should consider the rights of third parties in connection with a proportionality analysis regarding the discovery of social media).

Parties may seek to limit or set the circumstances for disclosure of sensitive information of third parties contained in social media content by incorporating procedures for producing, transferring, storing, or using such information as evidence. For appropriate redactions, this may include "Confidential Information" or "Attorneys Eyes Only" designations, data security protocols, filing under seal, or other procedures that can be documented via confidentiality agreements or other stipulated protective orders.

2. Requesting Social Media Evidence

The appropriate procedure for requesting and obtaining relevant social media information is, as with all types of ESI, for the requesting party to draft requests with specificity and for the responding party to conduct a reasonable inquiry, assert reasonable objections, and produce relevant, responsive non-privileged information.[51]

The duty of reasonable inquiry regarding relevant social media—as with all relevant evidence—begins with the responding party's compliance with its initial disclosure obligations.[52] The responding party must also conduct a reasonable inquiry once served with properly issued requests for production of documents. A requesting party has no obligation to prove relevant social media evidence exists or is publicly available before a

51. *Cf.* Offenback v. L.M. Bowman, Inc., No. 1:10-CV-1789, 2011 WL 2491371, at *3 (M.D. Pa. June 22, 2011) (stating that the court in a personal injury case questioned why the parties required its assistance when "it would have been . . . substantially more efficient for Plaintiff to have conducted this initial review [of social media content] and then, if he deemed it warranted, to object to disclosure of some or all of the . . . responsive information").

52. *See* FED. R. CIV. P. 26(a)(1)(A)(ii); 26(g)(1).

responding party's duty to conduct a reasonable inquiry is triggered.[53]

Social media evidence is often sought in cases where a party's physical or mental state during a particular period is relevant. In cases where physical ability, mental condition, or quality of life are at issue, social media postings reflecting physical capabilities, state of mind, or changes in a party's circumstances may be relevant and discoverable.[54] Such information has been found to be relevant in employment discrimination, personal injury, and workers compensation cases.[55]

For example, in *E.E.O.C. v. Original Honeybaked Ham*, a sexual harassment class action, the defendant sought social media evidence relating to the class members' damages—emotional and financial—along with their credibility and bias.[56] The defendant showed that one plaintiff had posted photographs of herself on her social media account in which she was wearing a shirt with a pejorative term in large letters across the front, the same term

53. *See* FED. R. CIV. P. 26(g)(1); Giacchetto v. Patchogue-Medford Union Free Sch. Dist., 293 F.R.D. 112, 114 (E.D.N.Y. 2013) ("The Federal Rules of Civil Procedure do not require a party to prove the existence of relevant material before requesting it. Furthermore, [such an] approach improperly shields from discovery the information of Facebook users who do not share any information publicly.").

54. *See* Forman v. Henkin, 30 N.Y.3d 656 (N.Y. Ct. App. Feb. 13, 2018) (finding pre- and post-accident photos privately posted on social media were discoverable); Nucci v. Target Corp., 162 So. 3d 146, 148, 152 (Fla. Dist. Ct. App. 2015) (holding that photographs from plaintiff's Facebook page could be relevant to his claim for personal injury damages).

55. *See* Ledbetter v. Wal-Mart Stores, Inc., No. 06-cv-01958, 2009 WL 1067018, at *1–2 (D. Colo. Apr. 21, 2009) (finding social media content was "relevant to the issues in this case" where plaintiffs sustained injuries while employed by defendant).

56. E.E.O.C. v. Original Honeybaked Ham Co. of Georgia, Inc., No. 11-cv-02560-MSK-MEH, 2012 WL 5430974 (D. Colo. Nov. 7, 2012).

she alleged to be offensive.[57] The defendant also showed that she posted statements on her social media account about her emotional state after the loss of a pet and a broken relationship, her sexual aggressiveness, sexually amorous communications with other class members, financial condition, and employment prospects.[58] The court, in granting the defendant's motion to compel social media information, reasoned as follows:

> I view this content logically as though each class member had a file folder titled "Everything About Me," which they have voluntarily shared with others. If there are documents in this folder that contain information that is relevant . . . to this lawsuit, the presumption is that it should be produced. The fact that it exists in cyberspace on an electronic device is a logistical and, perhaps, financial problem, but not a circumstance that removes the information from accessibility by a party opponent in litigation.[59]

The court acknowledged the potential financial exposure to the defendant in the case, "well into the low-to-mid seven-figure range," and explained that this potential exposure was "important to note when addressing whether the potential cost of producing the discovery is commensurate with the dollar amount at issue."[60]

57. *Id*. at *2.

58. *Id*.

59. *Id*. at *1.

60. *Id*. at *2.

B. Possession, Custody, and Control[61]

Whether relevant social media information is in the responding party's possession, custody, or control is another threshold issue for assessing whether there is a duty to preserve or produce such information.[62] A party who uses social media generally does not host the data and therefore will likely not have "possession" of the data, except to the extent that some of the data may be on the party's devices.[63] That social media technologies are constantly changing their functionality and storage features adds to the complexity of this issue. Courts have not helped to clarify matters as they have adopted inconsistent approaches for determining the meaning of "control" under Federal Rules of Civil Procedure ("FRCP") 34 and 45. Some courts have applied a broad "practical ability" standard, others a narrower "legal right" test, and others a "legal right" test with notification obligation. Accordingly, what constitutes "control" in one jurisdiction may not qualify as "control" in another.[64]

---

61. The concept of possession, custody, or control, as addressed herein, derives from FRCP 34(a)(1), which states "[a] party may serve on any other party a request within the scope of Rule 26(b) to produce and permit the requesting party or its representative to inspect, copy, test, or sample the following items in the responding party's possession, custody, or control." The occasional use of "*and* control" in the *Primer* is intended to address all three factors. It does not replace or diminish the "possession, custody, or control" standard under FRCP 34, which is discussed in this Section.

62. *See* FED. R. CIV. P. 34(a)(1).

63. *See* The Sedona Conference, *Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control*," 17 SEDONA CONF. J. 467, 524 (2016).

64. *See id*. at 483–89 (defining the "legal right" test as "[w]hen a party has the legal right to obtain the Documents and ESI"—followed by the Third, Fifth, Sixth, Seventh, Eighth, Ninth, Tenth, and Eleventh Circuits—and the "practical ability" test as "[w]hen a party does not have the legal right to obtain the Documents and ESI but has the 'practical ability' to do so"—followed by the Second, Fourth, Eight, Tenth, Eleventh, and District of Columbia Circuits).

1. "Control" By Individual Parties

A party generally has possession, custody, or control over its social media content. Other than certain controls implemented by the social media provider, the account user largely controls the content created on the account, the timing of when the content is posted, the deletion of content from the account, the other users who can view content posted to the account, and the like.[65] Thus, while some of the content may be exclusively obtainable from the social media provider's systems, the user still controls the vast majority of information shared via the account and can often take steps to preserve and collect information from the account. Further, the user can do so without violating the service provider's terms of service or state or federal law (such as the SCA).

For example, an individual user may generate content by typing text, uploading files, or live recording video or audio content to a social media account from a mobile device or computer. To the extent the content was uploaded from physical storage on that or another device, the content may still reside on the device and thus likely remains in the user's possession, regardless of whether a second copy may also reside on the servers of the social media provider. Similarly, content created on a smartphone application may be stored in that application on the phone—again, remaining in the user's possession. Thus, locally-

65. *Cf.* Arteria Prop. Pty Ltd. v. Universal Funding V.T.O., Inc., No. 05-4896 (PGS), 2008 WL 4513696, at *5 (D.N.J. Oct. 1, 2008) ("This Court sees no reason to treat [corporate] websites differently than other electronic files. Where, as here, Defendants had control over the content *posted* on its website, then it follows *a fortiori* that it had the power to delete such content. . . . Despite the inevitable presence of an intermediary when posting content on the Web, the Court finds that Defendants still had the *ultimate* authority, and thus control, to add, delete, or modify the website's content.").

stored copies of uploaded content remain in the user's possession, custody, or control.

This distinction does not suggest that posted content to a social media account is not in and of itself a unique piece of discoverable evidence. It may be meaningfully different from a locally-stored copy.

Similarly, evidence that posted content was removed from a social media account, the timing of when the account was updated or deactivated, or other account activity may be relevant to a given case. Records of such account activity are often in the possession of the social media provider.[66] Nevertheless, the user may still exercise "control" over such information and may be able to gain, grant, or deny access pursuant to end-user

66. Account activity log data may include the date and time the account was accessed, IP addresses from where the account was accessed, and reports detailing other aspects of the user's social media account. *Cf*. Crowe v. Marquette Transp. Co. Gulf-Inland, LLC, No. 14-1130, 2015 WL 254633 (E.D. La. Jan. 20, 2015) (explaining that 4,000 pages of plaintiff's "Facebook history" was relevant, including information showing the date on which the account was deactivated, media type and IP address of media used to access account on various dates, date and time of account reactivation, and content of messages exchanged with others).

agreements, social media provider policy,[67] or as a "customer" or "subscriber" of the account pursuant to the SCA.[68]

An account user's "ownership," i.e., legal right, to its social media content may be confirmed by the social media provider's terms of service. Some social media providers specify in their

67. *See, e.g.*, *Facebook Terms of Service*, § 3 , FACEBOOK, https://www.facebook.com/legal/terms/update (last revised Apr. 19, 2018) ("You own the content you create and share on Facebook and the other Facebook Products you use, and nothing in these Terms takes away the rights you have to your own content. You are free to share your content with anyone else, wherever you want."); *Twitter Terms of Service*, § 3, TWITTER, https://twitter.com/en/tos (effective May 25, 2018) ("You retain your rights to any Content you submit, post or display on or through the Services. What's yours is yours—you own your Content (and your incorporated audio, photos and videos are part of the Content)."); *Instagram Privacy and Safety Center, Terms of Use* § 4, INSTAGRAM HELP CTR., https://help.instagram.com/478745558852511 (last revised Apr. 19, 2018) ("We do not claim ownership of your content that you post on or through the Service."); *LinkedIn User Agreement*, § 2.2, LINKEDIN, https://www.linkedin.com/legal/user-agreement (effective May 8, 2018) ("As between you and others (including your employer), your account belongs to you. However, if the Services were purchased by another party for you to use (e.g. Recruiter seat bought by your employer), the party paying for such Service has the right to control access to and get reports on your use of such paid Service; however, they do not have rights to your personal account."); *Snap Inc. Terms of Service, Rights you Grant Us* § 3, SNAP, https://www.snap.com/en-US/terms/ (effective Sept. 26, 2017) ("Many of our Services let you create, upload, post, send, receive, and store content. When you do that, you retain whatever ownership rights in that content you had to begin with."); *Reddit User Agreement*, § 4, REDDIT, https://www.redditinc.com/policies/user-agreement (last revised Sept. 24, 2018) ("You retain any ownership rights you have in Your Content . . . ."); *Tumblr Terms of Service*, § 6, TUMBLR, https://www.tumblr.com/policy/en/terms-of-service (last modified May 15, 2018) ("Subscribers retain ownership and/or other applicable rights in Subscriber Content, and Tumblr and/or third parties retain ownership and/or other applicable rights in all Content other than Subscriber Content. You retain ownership you have of any intellectual property you post to Tumblr.").

68. *See infra* Section III(D).

terms of use that a user maintains control of its own content. Even where the service provider is silent on the issue of control or ownership over the account, the user's valid authorization under the SCA may be required for anyone other than the user to obtain content from the account. In other words, an account user likely has a legal right to obtain its social media information from the service provider because it is a customer or subscriber to the social media service pursuant to the SCA.

Thus far, courts have not expressly applied the practical ability test to an individual's ability to obtain the social media information of another. Nevertheless, a few courts have found control—without specifically invoking the practical ability test—despite the individual not having a legal right to the requested information.[69]

2. "Control" by Organizational Parties

The determination whether an organization has possession, custody, or control of social media content stored on its internal servers and infrastructure is similarly straightforward. A corporation has the "ultimate authority to control, to add, to delete, or modify" content it creates and stores on either its own servers or on those of a third party.[70]

Employers generally do not have control over their employees' personal social media accounts. Personal property of an

69. *See, e.g.*, Meyer v. DG Retail LLC, No. 13-2115-KHV, 2013 WL 5719508 (D. Kan. Oct. 21, 2013) (compelling a plaintiff to produce a job posting she found on a social media site despite the fact that it was not posted by her, nor did it originate from her own Facebook page); *contra* Fox v. Pittsburg State Univ., No. 14-2606-JAR-KGG, 2015 WL 7572301, at *2 (D. Kan. Nov. 24, 2015) (declining to compel the social media postings of the non-party husband of a plaintiff because plaintiff did not have possession, custody, or control over the husband's internet postings).

70. *Arteria Property Pty Ltd.*, 2008 WL 4513696, at *5.

employee is not generally under the "control" of the employer unless the employer has a legal right to obtain the property from its employee.[71]

The *Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control"* explains that (a) corporations do not own or control their employees' personal social media accounts, and (b) an employer's demand for information from such accounts may be viewed as "improper or coercive."[72] It does not appear that courts have held that employers have the "practical ability" to obtain their employees' social media information.[73] Indeed, efforts to compel an organization to produce its employees' information, absent a legal right to do so, would likely run afoul of the SCA. This is because the organization would lack direct access to the requested information and would instead seek it from the social media provider, a practice forbidden by the SCA.[74]

An employer's attempt to solicit social media usernames and passwords from its employees to facilitate social media access and collection by the employer may violate certain state laws.

---

71. *Cf.* Matthew Enter., Inc. v. Chrysler Grp., LLC, No. 13-cv-04236-BLF, 2015 WL 8482256, at *3 (N.D. Cal. Dec. 10, 2015) (holding that employer did not have legal right to personal email accounts used by its employees where the employees could "legally—and without breaching any contract—continue to refuse to turn over such documents"); Cotton v. Costco Wholesale Corp., No. 12-2731-JWL, 2013 WL 3819975, at *6 (D. Kan. July 24, 2013) (referring to personal cell phones of defendant's employees not under defendant's possession, custody, or control).

72. S*upra* note 63; *cf.* Pietrylo v. Hillstone Rest. Grp., No. CIV.06-5754(FSH), 2009 WL 3128420 (D.N.J. Sept. 25, 2009).

73. *But see* Ronnie Van Zant, Inc. v. Pyle, 270 F. Supp. 3d 656, 669 (S.D.N.Y. 2017) (finding defendant had the "practical ability" through its independent contractor film director to preserve relevant text messages and sanctioning defendant for failing to ensure their preservation).

74. *See infra* Section III(D)(8).

Moreover, state and federal regulations may limit an employer's ability to implement policies concerning employees' use of social media. Even if an employee were to leave social media access credentials on an employer-issued computer, the employer would still likely be prohibited from using such credentials to access the account by the SCA.[75] And employers do not have "control" over something that they are prohibited from accessing by state or federal law.

3. "Control" by Third Parties

While certain discoverable information may be visible to a party through its social media account, it may be removed by a third party (who created, posted, and potentially controls that information) or the social media provider. The account holder frequently cannot demand access to the removed content because it was not created by the account holder.

C. Preservation, Collection, and Search Obligations Generally

The popularity of social media, the proliferation of new technologies, and their rapid adoption by the public have made its preservation and collection more complicated than in many areas of discovery. Moreover, the dynamic nature of social media mandates that parties be proactive in addressing preservation.

1. Considerations for Preserving and Collecting Social Media

As with other forms of evidence, the preservation obligation with respect to social media information arises when a party knows or reasonably should know that it is relevant to actual or

75. *See* Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548 (S.D.N.Y. 2008) (awarding damages for violation of the Stored Communications Act where employer used webmail login credentials to access an employee's personal webmail account).

reasonably anticipated litigation.[76] Once the preservation obligation arises, a party should determine what sources of social media within its possession, custody, or control may contain information relevant to the litigation. The existence of an information retention policy that a party consistently observes can be a great aid in this preservation effort.[77]

Social media raises a number of preservation and collection issues that may need to be addressed in connection with a review of a party's preservation obligations. As an initial matter, a party needs to know exactly what social media is to be preserved and collected that is within its possession, custody, or control.[78] For example, a party might need to collect its relevant ESI from a third-party social media provider to avoid its potential loss, particularly if the site could take action to terminate the account and delete content. [79]

A party should also consider the types of social media data that may be obtained, which may go beyond ESI that would

---

76. *See* Nutrition Distrib. LLC v. PEP Research, LLC, 16-cv-02328, 2018 WL 3769162 (S.D. Cal. Aug. 9, 2018), *aff'd in part* 2018 WL 6323082 (S.D. Cal. Dec. 4, 2018) (imposing sanctions on defendant for destroying relevant Facebook posts after a duty to preserve attached).

77. *See* The Sedona Conference, *Commentary on Proportionality in Electronic Discovery*, 18 SEDONA CONF. J. 141, 152 (2017) (observing in Principle 1 that information retention policies, among other protocols, can help a party satisfy preservation duties).

78. *See supra* Section III(B).

79. The dynamic nature of the social media market—in which providers quickly fluctuate from success to failure—often leads to providers going out of business. In such instances, the responding party has to determine if its data is still available and whether it can be retrieved. Where the social media entity simply stops providing service, that entity should inform users whose data it holds accordingly so that arrangements can be made to provide users with their data. If the responding party cannot obtain or access its data due to a provider's insolvency, that data may no longer be in the party's possession, custody, or control.

ordinarily be accessible to a user on a social media platform. Data obtained from the provider could include geographical coordinates from image files or other sources, hashtags, referral links, payment history, lists of friends or followers, along with unusual language abbreviations and purposeful misspellings. It could also encompass other content such as emojis used in text messaging and live or streamed video data. Whether such information needs to be preserved depends on its relevance and proportionality.[80] Features such as encryption and ephemeral messaging can also raise preservation issues that need to be taken into account in any review of social media data.[81]

Next, the party should consider whether it needs the services of a third-party vendor to help preserve or collect relevant social media content. The value of the case and the nature of the issues will likely affect this determination. In addition, a party may need different technologies to collect diverse content types from the variety of social media outlets where discoverable information may reside. Technical sophistication may also be required to load the collected data onto a platform for review. The cost of preservation and collection is also a factor, as the range of services available differs for various services and budgets.[82]

A party should additionally consider whether the dynamic nature of a social media site requires that it perform more than one collection from that site. If the social media content as of a particular point in time is relevant to a matter, then it may be advisable to seek to extract the social media data at that time. In other instances, it may be appropriate to make collections at periodic intervals.

---

80. *See supra* Section III(A).

81. *See supra* Section II(B)(3).

82. *See Commentary on Proportionality in Electronic Discovery*, *supra* note 77, at 174–75 (discussing in Principle 6 that parties should have the discretion to select technologies that address their discovery needs).

Finally, the party must also consider the evidentiary aspects of preservation and collection, as authentication of social media evidence has been an ongoing issue over the years.[83]

2. The Role of Cooperation

Parties should consider working with litigation adversaries to develop reasonable steps for identifying and handling difficult social media preservation and collection issues.[84] Such discussions will ideally take place as early as possible and should be raised prior to or during the FRCP 26(f) discovery conference. The relevance and proportionality principles of FRCP 26(b)(1) should guide those discussions, with parties seeking to reach a resolution that satisfies their respective needs. This obligation may include mutual steps to preserve social media ESI, consideration of other ESI sources addressing the same issues that would obviate the need to preserve the social media, or the use of other evidentiary tools (e.g., stipulations or phased discovery to determine what is available from other sources).

Even if discussions between counsel are ultimately unsuccessful at this stage, the parties have at least framed the issues for further consideration and possible resolution by the court at the FRCP 16 scheduling conference.[85] There will undoubtedly be instances where such cooperation may not be possible (as when opposing counsel has not been identified after the duty to

83. *See infra* Section V.

84. *See The Sedona Conference Cooperation Proclamation*, 10 SEDONA CONF. J. 331 (2009 Supp.); *The Sedona Principles, Third Editio*n, *supra* note 29, at Cmt. 3, 71–79.

85. *See Commentary on Proportionality in Electronic Discovery*, *supra* note 77, at 155–59 (explaining in Principle 2 the roles of cooperation and phased discovery in advancing the aims of proportional discovery).

preserve is triggered) or practicable (when an adversary is unreasonable).[86]

3. The Interplay Between Reasonable Steps and Social Media

The touchstones of relevance and proportionality inform both the scope and nature of preservation of social media, with questions regarding the adequacy of a party's preservation efforts being a fact-based inquiry. FRCP 37(e) provides that sanctions for failures to preserve relevant ESI cannot issue where a party has taken "reasonable steps" to preserve that information.[87]

The "reasonable steps" standard calls for a good-faith assessment of what data may be relevant to the claims or defenses in the litigation. In the context of social media, "reasonable steps" should be examined through the additional lens of unique social media discovery challenges. Those challenges include that social media is often hosted remotely, may include data that is difficult to access, is dynamic and collaborative by nature, can include several data types, often involves privacy issues, and frequently must be accessed through unique interfaces. Any subsequent court review of the reasonableness of a party's preservation actions should use as its frame of reference the

86. *See* The Sedona Conference, *Commentary on Preservation, Management and Identification of Sources of Information that are Not Reasonably Accessible*, 10 SEDONA CONF. J. 281 (2009).

87. FED. R. CIV. P. 37(e). *See The Sedona Principles, Third Edition, supra* note 29, at Cmt. 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.").

party's knowledge at the time preservation decisions were made.[88]

In considering preservation issues, it may be that some social media and information sources are more difficult or more expensive to preserve than others. If a party can conduct an inventory of the relevant information in its possession, custody, or control, then it may be in a position to determine if certain ESI is duplicative and, if so, which sources it should focus on preserving. In any such exercise, cost is a legitimate consideration.[89]

Documenting the preservation process, including identifying relevant social media information and a party's decisions, can be helpful in establishing a defensible process. This is particularly the case as spoliation disputes may arise years after the original preservation efforts. Such a document should be updated as circumstances change, identifying, for example, the changed conditions and new actions taken.

4. Means of Preservation and Collection of Social Media

The available tools for preserving and collecting social media are becoming more sophisticated, more varied, and continue to evolve with changing technology. Thorough documentation and verification of the process and results will help ensure that evidence supporting the decisions and actions taken during the

88. *See Commentary on Proportionality in Electronic Discovery*, *supra* note 77, at 151; FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment ("A variety of events may alert a party to the prospect of litigation. Often these events provide only limited information about that prospective litigation . . . It is important not to be blindsided to this reality by hindsight arising from familiarity with an action as it is actually filed.").

89. *See* FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment (observing that a party "may act reasonably by choosing a less costly form of information preservation, if it is substantially as effective as more costly forms").

process is available to rebut spoliation claims that may arise in long-running litigation.

a. Static Images

Some practitioners resort to capturing static images of social media data (i.e., screen shots and PDF images) as a means of preservation, with courts often permitting the use of such evidence at trial.[90] Printing out social media data has its evidentiary limitations, as a static image does not capture the metadata of the image, other than whatever information may be viewable as part of the screen shot. As a result, static images may result in an incomplete and inaccurate data capture that is hard to authenticate, except on the basis of the personal knowledge of a witness.[91] Social media may also contain data and content, such as video, that cannot be properly collected in the form of static images.[92] In addition, social media outlets use different

90. *See infra* Section V; Michigan v. Liceaga, No. 280726, 2009 WL 186229, at *3–4 (Mich. Ct. App. Jan. 27, 2009) (indicating that the photograph from defendant's Myspace site depicting him holding the gun used to shoot a murder victim and "'throwing' a gang sign" was properly used for the purpose of establishing state of mind and intent and also showed his familiarity with weapons); United States v. Ebersole, 263 F. App'x. 251 (3d Cir. Feb. 6, 2008) (admitting a Myspace page at revocation hearing to provide context for threatening email sent to stalking victim's sister).

91. *See* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 538, 542–43 (D. Md. 2007); Hon. Paul Grimm, Gregory Joseph & Daniel Capra, *Best Practices for Authenticating Digital Evidence*, WEST ACAD. PUB. (2016) (discussing circumstances in which static evidence of social media can be authenticated). *See also* United States v. Vayner, 769 F.3d 125 (2d Cir. 2014) (vacating conviction based on lack of proper authentication for profile page from Russian social network site); Griffin v. State, 419 Md. 343, 19 A.3d 415 (2011) (holding that the trial court's admission of inadequately authenticated Myspace printout was reversible error).

92. Depending on the specific type of information that needs to be preserved or collected, videoing/interactive demonstration software that creates

interfaces to display content, further complicating efforts to create standardized snapshots.[93] Any such collection will most likely be a visual representation that does not include metadata, logging data, or other information that would allow the content to be easily navigated and used.[94]

While recognizing these limitations of static images as a means of preservation, their use may be appropriate in situations in which the visual representation of certain data is essential or sufficient (e.g., capturing a photograph or certain text) and the collection of metadata is of lesser importance.[95]

b. Self-Collection Based on Social Media Processes

Various social media platforms have established means by which a user can download social media data. Platforms also have procedures for carrying out a download, which differ in the form and appearance of data that they provide to the subscriber.

Facebook, for example, requires a username and password to process a download request, and as a result, this process must

---

a record of the experience of navigating a site may more accurately represent the dynamic nature of the information, including capturing dynamic and non-text postings such as audio and video materials.

93. For example, Facebook uses algorithms based on a subscriber's prior usage to determine how to array the web content.

94. Circumstantial evidence may enhance authentication, including the presence of photographs, email addresses, and posting dates. *See*, *e.g.*, *In re* T.T., 228 S.W.3d 312, 322–23 (Tex. App.—Houston [14th Dist.] 2007). Related data obtained from other sources, including email notifications of posting activity and computer and account usage logs, may provide additional context to aid authentication.

95. *See* Spencer v. Lunada Bay Boys, No. 16-cv-02129 (C.D. Cal. Dec. 13, 2017), *aff'd* 2018 WL 839862 (C.D. Cal. Feb. 12, 2018) (holding that a defendant should have taken screenshots (among other preservation measures) to preserve relevant text messages instead of allowing them to be destroyed).

generally be carried out by the account user (or someone to whom the user has provided login credentials).[96] The download includes various categories of information, including advertisements on which the user has clicked and communications exchanged on Facebook Messenger. It is provided in HyperText Markup Language (HTML) plain text files. Although the information from the Facebook download can perhaps be used as evidence in particular situations, it may be preferable to have a vendor obtain the data with the appropriate tools for accessing and then reviewing the information in a manner that includes available metadata.

Twitter offers a "request your archive" service. This request goes to Twitter, which provides the user with a download link to a ZIP file sent to the confirmed account email address.[97] This download gives the user copies of all the user's tweets since the account's creation. Non-public information from an individual's Twitter account—including direct messages—must be requested separately via email to Twitter, which then provides additional information about how to obtain such data.[98]

LinkedIn offers a download option from the user's account. The process involves two steps: first, using the privacy settings to request an archive of the user's data, which provides within minutes the ability to download information regarding

96. *See Accessing & Downloading Your Information,* FACEBOOK HELP CTR., https://www.facebook.com/help/1701730696756992/?helpref=hc_fnav (last visited Dec. 12, 2018).

97. *How to Download Your Twitter Archive,* TWITTER HELP CTR., https://help.twitter.com/en/managing-your-account/how-to-download-your-twitter-archive (last visited Dec.12, 2018).

98. Margaret (Molly) DiBianca, *Discovery and Preservation of Social Media Evidence,* BUS. L. TODAY (Jan. 2, 2014), https://www.americanbar.org/content/dam/aba/publications/blt/2014/01/social-media-evidence-201401.authcheckdam.pdf.

messages, connections, and contacts. Within 24 hours, LinkedIn provides an email link that allows the user to obtain a full archive of the user's data, including activity and account history.[99]

Reliance on provider-controlled export tools, such as those described above, may raise preservation and collection issues. These tools are often modified or updated by the service provider, without necessarily making the user aware of those changes. For example, Facebook's tool may cap the number of Messenger messages exported, potentially omitting responsive messages from the exported data. Although self-collection may be an easier option for some subscribers as a means of preservation, the frequent changes to the export tools pose some risk that counsel should consider.

c. Use of an Application Programming Interface Offered by the Social Media Provider

A number of social media providers have created utilities that allow third parties to access the social media provider's application and exchange information with that application. These utilities, using an API, allow eDiscovery vendors to access the social media platform and import selected data in a machine-readable format that captures both content and various metadata associated with the content.

Vendors may capture individual items on the platform with metadata attached in a manner that permits search and review of the content. These tools collect metadata that can help with corroboration and potential authentication of the underlying

99. *Accessing Your Account Data,* LINKEDIN HELP, https://www.linkedin.com/help/linkedin/answer/50191/accessing-your-account-data?lang=en (last visited Dec. 12, 2018).

content and may generate a message-digest hash for verification of the extracted data.[100]

Facebook, Twitter, Flickr, and Tumblr, among others, have APIs that allow access to their web content. These APIs all have different operating formats, but vendors have developed their own programs to download the data made available by the social media provider's API.[101] Among messaging applications, Slack also has an API that may allow access to vendors.[102]

Social media providers set the standards on web content that may be downloaded. In 2015, Facebook changed its prior policy of giving access through its API to almost all public-facing information to a more restrictive policy that does not permit collection of data on user timelines or personal profiles, and allows access only to public pages that could be liked or followed.[103]

---

100. For example, a "tweet" generated on Twitter or an individual Facebook post contains over 20 specific metadata items. *See* John Patzakis, *Key Facebook Metadata Fields Lawyers and eDiscovery Professionals Need to be Aware of,* EDISCOVERY L. & TECH BLOG (Oct. 11, 2011), http://blog.x1discovery.com/2011/10/11/key-facebook-metadata-fields-lawyers-and-ediscovery-professionals-need-to-be-aware-of.

101. One of the popular social media discovery collection tools is X1 Social Discovery, which has API collection tools for Facebook, Twitter, YouTube, Instagram, and Tumblr, along with the capability to collect webpages and email from other providers. *See Social Media and Internet-Based Data Collection*, X1, https://www.x1.com/products/x1_social_discovery/ (last visited Dec. 12, 2018).

102. *See e.g., Guide to Slack import and export tools,* SLACK HELP CTR., https://get.slack.help/hc/en-us/articles/204897248-Guide-to-Slack-import-and-export-tools (last visited Dec. 12, 2018).

103. *See Terms of Service,* FACEBOOK, https://www.facebook.com/terms.php?ref=p (last visited Dec. 12, 2018); *see also What Type of Web Data Can You Collect From Facebook?*, BRIGHT PLANET (June 17, 2016), https://brightplanet.com/2016/06/type-web-data-can-collect-facebook/.

Twitter provides information through its API on individual users and their tweets.[104]

The API process cannot produce a forensic image of the captured web content because it changes and transforms the original context and format of the underlying content. There is also a chance that the content will not be rendered in an identical manner to the way it appeared on the service provider's site. Despite these issues, content produced using a social media provider's API has routinely been admitted into evidence at trial and is considered a best practice.

d. Native or Near-Native File of the Web Content

With the International Organization for Standardization (ISO) 28500 Web ARChive (WARC) standard, it is possible to get a native or near-native file of the collected content of a social media site. This standard, established by the International Internet Preservation Consortium, uses a WARC file as a container or image for accessed web resources and metadata.[105] A web crawler or similar program captures the data, stores the data in a WARC file, and generates relevant metadata about the capture to confirm that the data has been obtained and that its integrity has been preserved. The captured data has working links, graphics, and other dynamic content, along with an audit trail tracing back to the original social media site.[106]

---

104. *See Twitter Terms of Service,* TWITTER, https://twitter.com/en/tos (last visited Dec. 12, 2018); *see also What Type of Data Can You Get from Twitter*, BRIGHT PLANET (Mar. 15, 2016), https://brightplanet.com/2016/03/what-type-of-data-you-can-get-from-twitter/.

105. *ISO 28500:2017 Information and documentation—WARC file format.*, ISO, https://www.iso.org/standard/68004.html (last visited Dec. 12, 2018).

106. *WARC this way,* DELOITTE, https://www2.deloitte.com/us/en/pages/advisory/articles/warc-this-way.html (last visited Dec. 12, 2018).

With the native or near-native file capture, the data can be viewed as the content appeared on the original page of the social media site, although it may not be possible to view all of the linked content. The data can be searched, reviewed for metadata, and exported to an eDiscovery platform for further review.[107]

To carry out this imaging of the web content, it would be necessary to have the consent of the user, and with such consent, vendors could access the user's account.

e. Other Vendor Services, Including Dynamic Capture

Vendors have developed technology to allow certain content to be collected in a way that preserves the content and captures various metadata fields associated with social media data. Properly captured, these metadata fields can assist with establishing the chain of custody and authentication. They can also help to facilitate more accurate and efficient data processing and review.

Dynamic capture can assist with the preservation and collection of social media. This process captures and analyzes the resulting digital materials based on specific business rules. This analysis allows a party to draw conclusions about the data set based on the rules applied to the data, without corrupting the data.

In litigation, dynamic capture processes can be applied to interactive content in cloud-based collaboration sites that needs to be preserved and reviewed. It may also apply to situations involving large amounts of user data on a social media site.

---

107. Hanzo is one of the providers offering a WARC native file copy of web content with its Preserve service. *See eDiscovery and Litigation Archiving with Hanzo Preserve™*, HANZO, https://www.hanzo.co/ediscovery-software (last visited October 17, 2018).

Dynamic capture allows a vendor to identify relevant data in the collaboration site or capture interactive data on the social media site. It then creates data sets that can be reviewed and searched to identify relevant data for litigation without altering it.

Technology to preserve, collect, and review social media continues to adapt to new services and social media offerings. Similar to early generation email review, where slow and relatively simple technologies were rapidly supplanted by a variety of sophisticated email review options, eDiscovery tools addressing social media will undoubtedly grow in capacity and capabilities and should in the future be able to handle more of the challenges that social media poses.

D. Preservation and Collection Guidance in Light of the Stored Communications Act

An organization under a preservation duty may lack possession, custody, or control over relevant social media content stored on external websites.[108] Under these circumstances, a litigant may seek discovery directly from the social media service provider, but could be thwarted by the sweeping provisions of the SCA.[109] The following discussion of the SCA provides guidance on how parties can navigate through the statutory framework to accomplish preservation, collection, or production of relevant social media.

---

108. *See* Section III(B), *supra*.

109. The SCA is part of the Electronic Communications Privacy Act (ECPA) that Congress passed in 1986. *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 971 (C.D. Cal. 2010).

1. Restrictions on Electronic Communication Service Providers

The SCA imposes different levels of restrictions and protections, depending on whether the service provider is providing an "electronic communication service" ("ECS") or a "remote computing service" ("RCS").

An ECS refers to "any service which provides to users thereof the ability to send or receive wire or electronic communications."[110] The SCA generally prohibits "a person or entity providing an electronic communication service to the public" from "knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service."[111]

For this restriction to apply, the communication must be in "electronic storage." Plainly stated, this section of the SCA prohibits an ECS from divulging the contents of communications that either are: (a) in temporary storage (such as messages waiting to be delivered); or (b) kept for purposes of backup protection.

2. Restrictions on Remote Computing Service Providers

The SCA separately prohibits unauthorized disclosure of communications by those providing "remote computing services" to the public. Under the Act, an RCS refers to a service

---

110. 18 U.S.C. § 2510(15).

111. 18 U.S.C. § 2702(a)(1). *See* Facebook, Inc. v. Wint, No. 18-CO-958, 2019 WL 81113 (D.C. App. 2019) (holding that "the SCA prohibits providers from disclosing covered communications in response to criminal . . . subpoenas"). One obvious exception is that the service provider may disclose the communication to the sender or the intended recipient. 18 U.S.C. § 2702(b)(3).

offering the public "computer storage or processing services by means of an electronic communications system."[112]

Compared to ECS providers, the restrictions on RCS providers are broader and are not limited to communications that are in temporary storage or kept for purposes of backup protection.

3. Determining the Type of Service Involved

Whether a service provider is providing an ECS or an RCS depends in large part on the type of information or data at issue and its current state. The distinction is not trivial and can sometimes result in liability under the SCA.[113] Moreover, an entity may qualify as providing both types of service, even for a single type of communication.[114]

For private messages, such as those exchanged through Facebook Messenger, that have not yet been delivered or read, the service provider typically is considered an ECS provider, and the messages are subject to the SCA because the communication is in temporary intermediate storage pending delivery.[115]

For messages that have already been delivered and read, there is a split of authority. If a copy remains on the service

112. 18 U.S.C. § 2711(2).

113. Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 900 (9th Cir. 2008) (agreeing that "if Arch Wireless is an [electronic communication service provider], it is liable as a matter of law, and that if it is [a remote computing service provider], it is not liable"), *rev'd on other grounds*, City of Ontario, Cal. v. Quon, 560 U.S. 746 (2010).

114. *See Crispin*, 717 F. Supp. 2d at 987–90 (holding among other things that Facebook was both an ECS and an RCS in context of facilitating and hosting the private messages exchanged on its platform).

115. *See id*. at 987 and cases addressed therein. A number of courts have concluded that once an email has been opened by the recipient it is no longer in "temporary, intermediate storage." *See, e.g.*, Levin v. ImpactOffice LLC, No. 8:16-cv-02790-TDC, 2017 WL 2937938 (D. Md. July 10, 2017); Murphy v. Spring, 58 F. Supp. 3d 1241, 1270 (N.D. Okla. 2014).

provider's server, a court may decide the provider remains an ECS provider and the communication is subject to the SCA because it is kept for backup purposes.[116] Other courts have reached a different conclusion, holding instead that retrieved email messages (even if kept on the internet service provider's (ISP) server) are not retained for backup purposes and therefore not covered by the SCA.[117] Courts may also conclude that service providers that retain delivered and read email messages are actually RCS providers, thus eliminating the "electronic storage" issue altogether.[118]

4. Protections Limited to Contents of Communications

The SCA prohibits disclosure of the "contents of communications," such as the substance of the message conveyed.[119] However, it does not apply to other aspects of the communication, such as the date, time, or originating and receiving telephone number for phone calls and text messages, or the

116. *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004). *See also Levin*, 2017 WL 2937938, at *4–5 (discussing cases and "find[ing] the reasoning of *Theofel* persuasive"); Cheng v. Romo, No. 11-10007-DJC, 2013 WL 6814691 (D. Mass. Dec. 20, 2013); Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548 (S.D.N.Y. 2008).

117. *See, e.g.*, Lazette v. Kulmatycki, 949 F. Supp. 2d 748 (N.D. Ohio 2013); Anzaluda v. Northeast Ambulance and Fire Prot. Dist., 793 F. 3d 822, 840–42 (8th Cir. 2015) (disagreeing with reasoning of *Theofel*); Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001), *aff'd in part* 352 F.3d 107, 114–15 (3d Cir. 2003) (holding that retrieval of message from post-transmission storage did not violate the SCA).

118. United States v. Weaver, 636 F. Supp. 2d 769, 772 (C.D. Ill. 2009) (finding Microsoft to be a remote computing service provider and holding that web-based email messages were covered by the SCA).

119. 18 U.S.C. § 2702(c)(6).

personally identifying information of a service subscriber.[120] Thus, a requesting party can obtain such account information from the social media provider regarding both the sender and recipient of a communication at issue, together with the internet protocol (IP) address used to access the account.[121]

5. Public vs. Private Issues

The prohibitions in the SCA apply only to those that provide services to the public.[122] Additionally, SCA protections apply only to private communications and not those readily accessible to the public.[123] For example, the SCA does not apply where a user's privacy setting for Facebook is such that the public can view wall posts or comments.[124] Similarly, the SCA does not

120. *See* Williams v. AT&T Corp., No. 15-cv-3543, 2016 WL 915361 (E.D. La. Mar. 9, 2016) (holding that defendant did not violate the SCA by revealing "customer information such as the date, time, originating and receiving telephone number for phone calls and text messages."); *In re* Zynga Privacy Litig., 750 F.3d 1098, 1107 (9th Cir. 2014) (holding that disclosure of Facebook header information, which included a Facebook user's identification number, did not violate the SCA).

121. *See* Sines v. Kessler, No. 18-mc-80080, 2018 WL 3730434 (N.D. Cal. Aug. 6, 2018) (enforcing subpoena seeking account information of parties sending messages in advance of 2017 Charlottesville disturbance but quashing request for substance of communications); Obodai v. Indeed, Inc., No. 13-cv-80027, 2013 WL 1191267, at *3–4 (N.D. Cal. Mar. 21, 2013) (holding that the SCA permits subpoenaing parties to obtain relevant subscriber information including plaintiff's email address, the IP addresses used to access plaintiff's email, and the dates and times of such access).

122. *See* Andersen Consulting LLP v. UOP, 991 F. Supp. 1041, 1042–43 (N.D. Ill. 1998) (holding that the SCA did not apply to companies that provide email service to their employees).

123. 18 U.S.C. § 2511(2)(g).

124. *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010).

apply to an internet bulletin board where the public could gain access simply by signing up.[125]

6. Enforcement of the Prohibition Against Divulging Communications

There are some exceptions that allow service providers to disclose communications,[126] but no exception exists under the SCA for civil subpoenas.[127] The SCA provides a civil cause of action against service providers that violate the Act.[128] The aggrieved party may sue for both equitable relief and damages.[129] The minimum that can be awarded is $1,000; damages can include actual harm suffered by the plaintiff, any profits made by

125. *See* Snow v. DirecTV, Inc., 450 F.3d 1314, 1321–22 (11th Cir. 2006) (stating that "[i]n order to be protected by the SCA, an Internet website must be configured in some way so as to limit ready access by the general public"); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002) (holding that the SCA applies to internet bulletin boards that limit public access); Viacom Int'l Inc. v. YouTube Inc., 253 F.R.D. 256, 264 (S.D.N.Y. 2008) (finding the SCA protects from discovery videos marked "private" by a YouTube user).

126. *See* 18 U.S.C. § 2702(b). The *Primer* does not address the exception that allows government entities to compel ECS providers to disclose communications, including those stored with social media sites, pursuant to a warrant issued in accordance with the procedures set forth in the Federal Rules of Criminal Procedure by a court of competent jurisdiction for communications that are in electronic storage for less than 180 days. 18 U.S.C. §2703(a).

127. *See* Chasten v. Franklin, No. 10-cv-80205 MISC JW (HRL), 2010 WL 4065606, at *2 (N.D. Cal. Oct. 14, 2010); *Crispin*, 717 F. Supp. 2d at 975; *Viacom Int'l*, 253 F.R.D. at 264; *In re* Subpoena Duces Tecum to AOL, LLC, 550 F. Supp. 2d 606, 611 (E.D. Va. 2008).

128. 18 U.S.C. § 2707. *See also* Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892 (9th Cir. 2008) (holding that a provider of text messaging services violated the SCA by releasing transcripts of text messages).

129. 18 U.S.C. § 2707(b).

the violator as a result of the violation, punitive damages for willful or intentional violations, and attorney fees and costs.[130]

7. The Prohibition Against Access by Unauthorized Persons

In addition to prohibiting service providers from divulging the contents of communications, the SCA also bars third parties from improperly accessing an electronic communication maintained by an ECS provider. Further, any exception under the SCA for conduct authorized by the ECS provider does not protect the attorneys who issued the subpoenas to the ISP.[131] This prohibition applies to attorneys who, through improper means, gain access to protected content.[132]

8. Seeking to Obtain Information Without Violating the SCA

Given the SCA's prohibitions and the possibility of criminal or civil liability, attorneys must take care when seeking discovery of communications protected by the SCA. One way to lawfully obtain communications protected by the SCA would be to subpoena or otherwise obtain them directly from the user or subscriber.[133] Alternatively, the requesting party could obtain

130. 18 U.S.C. § 2707(c).

131. 18 U.S.C. § 2701(a) (prohibiting improper access); 18 U.S.C. § 2701(b) (establishing criminal penalties); 18 U.S.C. § 2707(a) (providing a private right of action).

132. *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1074 (9th Cir. 2004) (sanctioning counsel and reasoning that the aggrieved parties could bring claims against counsel under the SCA for issuing subpoenas to the parties' ISP to obtain their email).

133. The *Primer* sets forth various means by which a user or subscriber can (on its own or with the assistance of a third-party vendor) download or otherwise obtain content stored on the user's social media website and produce relevant information to a requesting party. *See supra* Section III(C)(4).

the consent of the user or subscriber of the service to receive protected communications directly from the service provider.[134]

If subscriber consent is not given, the requesting party may seek relief from the court in the form of an order compelling the user or subscriber to undertake the necessary review to provide the requested social media information. In some instances, however, parties have sought to obtain login credentials to a social media account that would allow the requesting party to access the social media content directly without the user. Several problems could arise if a responding party is compelled to disclose its login credentials:

- Doing so may violate the social media provider's terms of use.[135]
- Users may have the same login credentials for multiple social media accounts, which could permit an adversary to access content from other accounts without user consent.
- Some social media providers have adopted "two factor authentication" protocols, which can block account access if users try to access their accounts from a different device.[136]

---

134. *See* 18 U.S.C. § 2702(b)(3).

135. *See, e.g., Terms of Service*, §3, ¶1, FACEBOOK, http://www.facebook.com/legal/terms (last visited Apr. 19, 2018) (providing that as a Facebook user "you must . . . [n]ot share your password, give access to your Facebook account to others, or transfer your account to anyone else (without our permission)"); *Snap Inc. Terms of Service*, *Safety* § 8, SNAP, https://www.snap.com/en-US/terms/ (effective Sept. 26, 2017) (proscribing users from seeking the "login credentials from another user").

136. *See, e.g., Staying in Control of Your Facebook Logins*, FACEBOOK, https://www.facebook.com/notes/facebook/staying-in-control-of-your-facebook-logins/389991097130/ (last visited Dec. 12, 2018) (providing that

- Requiring users to disclose login credentials could create a presumption that all content from a social media account is discoverable and lead to the disclosure of irrelevant, confidential, or privileged information.
- Divulging login credentials could lead to spoliation without an audit trail of what information was deleted or created by the requesting party.

Courts have reached conflicting results regarding this issue. Cases prohibiting the practice have cited overbreadth and privacy concerns.[137] In cases granting such requests, different means have been adopted to permit discovery of social media content. But such cases generally present additional problems and roadblocks such that direct access by a requesting party to a responding party's social media accounts may be allowed only in special circumstances and upon a showing of good cause with the entry of an appropriate protective order.[138]

Significantly, during the period that the parties are negotiating over issues of consent or litigating in court over discovery of

---

Facebook will block "suspicious logins," which include attempts to login from "an unusual device").

137. *See, e.g.*, Chauvin v. State Farm Mut. Ins. Co., No. 10-cv-11735, 2011 U.S. Dist. LEXIS 121600 (S.D. Mich. Oct. 20, 2011) (rejecting request for login information and imposing sanctions against defendant as the requested discovery was available "through less intrusive, less annoying and less speculative means"). *But see* Connolly v. Alderman, No. 17-cv-0079, 2018 WL 4462368, at *6 (D. Ver. Sept. 18, 2018) (requiring plaintiff to produce relevant information from his social media accounts or alternatively "provide Defendants with passwords and more unrestricted access to Plaintiff's social media accounts"). Issues regarding the scope of access to a party's social media accounts and privacy issues associated therewith are discussed at Section III(A)(1), *supra*.

138. *The Sedona Principles, Third Edition*, *supra* note 29, at cmt. 10.e.

social media, information may be lost.[139] If there is a risk that evidence may be lost, a requesting party could place a social media service provider on notice that the requesting party will seek consent, whether voluntary or compelled, to obtain the sought-after information.

If the court has jurisdiction over the third party, another approach would be to seek permission to issue a preservation subpoena to the service provider early in the litigation.[140] At least one court has recognized that "[i]t may be necessary to issue a preservation subpoena to a non-party when the non-party does not have actual notice of the litigation or when the non-party is a corporate entity which typically destroys electronic information by 'performing routine backup procedures.'"[141] A preservation subpoena would not compel the service provider to divulge the contents of any stored communications, but would instead merely order them to be preserved.[142]

E. Review and Production

1. Review

The way in which social media data will generally be reviewed for discovery purposes is driven by how the data was preserved and collected and by what is feasible under the

---

139. *See* Gatto v. United Air Lines, Inc., No. 10-cv-1090-ES-SCM, 2013 WL 1285285 (D.N.J. Mar. 25, 2013) (issuing an adverse inference where plaintiff deleted his Facebook account while negotiating with defendants over terms of their access to his account).

140. *See* Johnson v. U.S. Bank Nat. Ass'n., Case No. 1:09-CV-492, 2009 WL 4682668 (S.D. Ohio, Dec. 3, 2009) (permitting issuance of a preservation subpoena to third parties prior to FRCP 26(f) conference).

141. *In re* Nat'l Century Fin. Enter., 347 F. Supp. 2d 538, 542 (S.D. Ohio 2004).

142. The only mention in the SCA of preservation by a service provider is in the context of certain government subpoenas. 18 U.S.C. § 2704.

circumstances. Selecting the proper approach for review may involve a number of factors, including whether there is a need to review the data interactively as it appeared on the social media site or to see how the content changed over time. Other factors may include the volume of the data to be reviewed, whether metadata was collected and is relevant, and the ability of the review software to facilitate coding and to support litigation processing and management needs. Those needs may include, among other things, search, sampling, Bates stamping, redaction, and export. A final factor is whether to allow the requesting party to inspect and copy relevant content from the social media accounts at issue.[143]

a. Small Data Volumes

It may be preferable to review social media content using the native or near-native file or the API used for collection when the data volume is small. These methods are also useful if a responding party needs to review the social media data interactively, as it was originally displayed on the site, or over a certain period of time.[144] Available social media ISO 28500 WARC and API products can collect an entire site or a single page with its associated content, such as links to other sites and multimedia files, making the review experience similar to the experience the user had when uploading or posting content. This functionality

143. FED. R. CIV. P. 34(a). Such a course may be preferable for some parties who might consider a review to be unduly burdensome. *See* McDonald v. Escape the Room Experience, LLC, No. 15-cv-7101 RAK NF, 2016 WL 5793992, at *1 (S.D.N.Y. Sept. 21, 2016) (rejecting plaintiff's argument that it would be "unduly burdensome" to produce her Facebook postings).

144. When an individual party's own social media content on a third-party site is relevant to litigation, it can undertake the review directly in its account on the third-party site to determine whether it contains relevant information. *See* Offenback v. L.M. Bowman, Inc., No. 1:10-CV-1789, 2011 WL 2491371 (M.D. Pa. June 22, 2011).

could be important in a trademark or trade dress infringement case, for example, where the way the allegedly infringing mark is displayed throughout a site or sites and over time is critical. Similarly, interactive access may be helpful to understand the emotional or mental state of claimants in a sexual harassment suit.[145]

Parties might alternatively consider obtaining archival downloads of user information from social media sites,[146] although such downloads have their limitations. With Facebook and Twitter, users may only download the entirety of their accounts and cannot limit the download to relevant content. In addition, an archival download may not include all relevant data.[147] Information may also be difficult to review.[148] Moreover, the content and format of provider-created archives may be periodically changed or updated by the service provider, rendering the archives unreliable for preservation purposes.

b. Large Data Volumes

When large volumes of social media data are involved, it may be preferable to use early case assessment and review tools to filter the content and accomplish the review. Selecting a review tool for social media may be particularly useful when the

145. *See* EEOC v. Simply Storage Mgmt., LLC, 270 F.R.D. 430 (S.D. Ind. May 11, 2010).

146. Instagram does not offer an archival download, but some third-party applications support archiving of social media posts.

147. Archived information may not provide context surrounding certain user comments. More sophisticated tools may be required to capture a snapshot in time of the social media interface on which comments were made. In addition, the Twitter archive does not include messages exchanged with other users through the platform messaging interface.

148. Posts and photos in a Facebook archive download into different folders, and the posting list renders as a crudely formatted list in an HTML file. Tweets download to a comma separated value (CSV) file format in Excel.

case team is most concerned with the text from social media sites as opposed to the way data was originally displayed. Reviewing social media content in a review tool is also practical when the content was preserved and collected in a manner that rendered it more like other types of ESI, enabling reviewers to use features such as threading and bulk tagging.

Data clustering and near duplicate identification technologies may also be helpful in identifying content from social media data that is similar to and can be grouped with other ESI such as email and loose files. Extended social media communication often takes place over several different types of media. For example, such a communication may begin with messaging, move to phone, then to text, and end with video. Technology that allows these different forms of communication—all residing in different services and saved in different file types—to be reviewed together can be useful for understanding the full context and content of such communication. Such capability also provides better context and prevents social media data from being reviewed in isolation. This functionality is optimized when social media metadata is available.[149]

If the social media content is loaded into a review platform, it will be important to consider how the content will be organized as "documents" within the platform. A "document," for instance, could reflect a page, a site, a user homepage, an email, a blog post, or a picture. Content may need to be parsed and reconstructed to make it manageable for review as well as to give context.

Despite the benefits of review platforms, they are generally not programmed to mimic the interactive experience of a social media site. The difficulty in collecting metadata associated with the social media content, combined with other issues such as the

149. *See The Sedona Principles, Third Edition*, *supra* note 29 at 169–71.

tendency of social media sites to incorporate content from external sites, can make using a conventional platform to review social media content difficult or inefficient.

2. Production

The same analysis that guides the selection of an appropriate review platform also applies to the production of social media data. The issue turns on the importance to the case for the requesting party to be able to review the social media data interactively and as it appeared on the social media platform. When interactive review is not important, it may be sufficient to produce the social media content in a reasonably usable and searchable format with or without metadata. Where messaging, texts, or similar text-based content are the primary data being produced, they can usually be handled in the same manner as traditional text-based content such as email.

In cases involving small amounts of social media data, static images or hard-copy printouts are often used for review and production.[150] Doing so, however, may run afoul of the requesting party's production requests or FRCP 34's mandate to produce in a reasonably usable format.[151] The complexities

150. *See*, *e.g.*, Bass *ex. el.* Bass v. Miss Porter's School, 3:08-cv-1807, 2009 WL 3724968 (D. Conn. 2009) (producing relevant pages of Facebook in hard copy).

151. *See In re* Cook Med., Inc., IVC Filters Mktg., Sales Practices & Prods. Liab. Litig., No. 1:14-ml-2570-RLY-TAB, 2017 WL 4099209 at *3-4 (S.D. Ind. Sept. 15, 2017) (requiring that plaintiff, who initially produced a PDF of social media data in response to a defendant's request for native production, provide native files with metadata where defendant demonstrated relevance and clearly identified the requested data); German v. Micro Elecs., Inc., No. 2:12-cv-292, 2013 WL 143377, at *9 (S.D. Ohio Jan. 11, 2013) (ordering production of blog posts as a static PDF or tagged image file format (TIFF) since the screenshots of plaintiff's blog posts were not "'a reasonably usable form'

surrounding social media production emphasize the need for dialogue and cooperation between requesting and responding parties.

It will sometimes be important to produce the relevant social media data in an interactive format that imitates the way it appeared on the site. Production in this manner would be consistent with the concept that a reasonably usable production format is typically one that allows the receiving party to make use of data in the same or similar way as the responding party ordinarily maintained the content.[152]

There are different potential responses to this request. One strategy is to give the requesting party access to a copy of the native or near-native file or to certain portions of the API used for collection. Other approaches involve giving access to the user's social media account to allow the requesting party to make similar use of the content within the meaning of FRCP 34(b)(2)(E)(ii). Another strategy is for the responding party to produce static images of the pertinent sites, so the requesting party may observe how they appeared. At the same time, the responding party may grant the requesting party access, who can then review the site's content interactively.[153] To be sure,

---

given that [the] production method strips the entries of their original and complete text, formatting, images, and likely the source.").

152. *The Sedona Principles, Third Edition*, *supra* note 29, at 171–72.

153. With the cooperation of the court, another approach is for the responding party to "friend" the judge, who then performs an in camera review and makes available any relevant content; though this approach does not allow the requesting party to view the site interactively. *See* Offenback v. L.M. Bowman, Inc., No. 1:10-CV-1789, 2011 WL 2491371 (M.D. Pa. June 22, 2011) (court obtained plaintiff's login information for Facebook and conducted in camera review to determine if the site contained relevant information); Barnes v. CUS Nashville, LLC, No. 3:09-cv-00764, 2010 WL 2265668 (M.D. Tenn. 2010) (discussing whether the court should set up a Facebook account and "friend"

providing adversaries with direct access to a responding party's social media account should be a last resort, if done at all, e.g., when there is no other way to accomplish production and when it is critical that opponents have interactive and similar use of the content.[154]

Depending on whether the cost is proportional to the needs of the case, engaging a neutral vendor may be helpful to assist with challenges in social media production. In one case, a vendor collected the defendant's devices, and the defendant granted the vendor access to his social media accounts, which contained millions of pages of data.[155] The vendor then ran search terms agreed to by the parties and provided only responsive material to the plaintiff.[156]

---

friends and witnesses of the plaintiff in order to facilitate in camera inspection and expedite discovery).

154. *See supra* Section III(D)(8).

155. Pre-Paid Legal Servs., Inc. v. Cahill, No. 6:2012-cv-0346, 2016 WL 8673142, at *1 (Sept. 30, 2016).

156. *Id*.

IV. CROSS BORDER DISCOVERY ISSUES

Parties who seek discovery of information from persons outside the United States or social media information located in a foreign country may face significant challenges. Parties seeking social media information within the United States may consult a patchwork of federal and state laws focused on specific industries or circumstances where personal data is protected.[157] In contrast, personal data may be protected more broadly by treaty[158] or applicable foreign law outside U.S. borders. In Europe, parties should determine not whether there is a law that *precludes* the processing, transfer, or production of social media information, but whether the law *permits* such activities.

A. Europe

Members of the European Union (EU) define "personal data" broadly to include any information relating to an identifiable individual. The EU views privacy of "personal data" as a "fundamental human right."[159] An even stricter standard of protection applies to sensitive personal information such as racial

157. Most notably the ECPA, 18 U.S.C. § 2510; Fair Debt Collections Practices Act (FDCPA), 15 U.S.C. §§ 1692–92p; Financial Services Modernization Act (GLBA), 15 U.S.C. § 6801; Health Insurance Portability and Accountability Act (HIPAA), Pub. L. No. 104-191, 110 Stat. 1938 (1996).

158. *See* Charter of Fundamental Rights of the European Union (EU), 2000 O.J. (C 364) 1, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1544731399799&uri=CELEX:32000X1218(01) [hereinafter Charter of European Union]. In addition, the African Union Convention on Cyber Security and Personal Data was adopted on June 27, 2014, and requires the creation of an independent administrative authority tasked with protecting personal data. However, as of February 2018, only one state, Senegal, has ratified the treaty. *See* African Union Convention on Cyber Security and Personal Data Protection, June 27, 2014, EX.CL/846(XXV), *available at* https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

159. Charter of European Union, *supra* note 158, at art. 8.

or ethnic origin, religious beliefs, and political opinions.[160] This benchmark stands in contrast to the United States, which provides limited protection of personally identifiable information and focuses more narrowly on personal data such as financial information,[161] social security numbers,[162] and medical records.[163]

EU member states also broadly define the "processing" of data and have proscribed the processing of personal data unless an exception applies. Processing includes "collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."[164] A party's actions in preserving or collecting social media content will likely be considered "processing." Unless an exception such as consent (obtained from a data subject) applies or where processing is "necessary for compliance with a legal obligation to which the controller is subject,"[165] such processing could violate EU or member nations' laws.

---

160. 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. (L119) 1, at art. 9, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679#PP3Contents [hereinafter GDPR] (prohibiting the processing of such personal information barring narrow, delineated exceptions).

161. *See* FDCPA, 15 U.S.C. §§ 1692–92p; GLBA, 15 U.S.C. § 6801.

162. However, regulation of social security numbers in the United States is largely limited to the public sector. *See* The Privacy Act of 1974, 5 U.S.C. § 552a note.

163. *See* HIPAA Privacy Rule, 45 C.F.R. pts. 160, 164(A), (E).

164. GDPR, *supra* note 160 at art. 4.

165. *Id.* at art. 6.

Transferring data to the United States may also run afoul of the General Data Protection Regulation (GDPR), which is now the basis of EU data protection law. The GDPR includes the new Article 48 which provides:

> Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.[166]

The Hague Convention is such an international agreement, but in practice the Convention may not be a viable means of complying with European data protection laws. In 1987, the U.S. Supreme Court in *Société Nationale Industrielle Aérospatiale v. U.S. District Court for the Southern District of Iowa* held that a requesting party was not required to use the Hague Convention in cross-border discovery.[167] Should a conflict exist between domestic and foreign law, the *Aérospatiale* Court instructed courts to conduct a comity analysis to determine whether requesting parties should be required to perform discovery under the FRCP or through a treaty such as the Hague Convention. Listing five factors[168] for courts to consider when conducting this

166. *Id.* at art. 48.

167. Société Nationale Industrielle Aérospatiale v. U.S. District Court for the Southern District of Iowa, 482 U.S. 522 (1987).

168. *Id.* at 543–44 ("[T]he concept of international comity requires in this context a more particularized analysis of the respective interests of the foreign nation and the requesting nation. . . .") (page numbers omitted).

analysis, the Court stressed that courts must balance the competing interests of the forum state and the foreign state in complying with the Hague Convention.[169]

Following *Aérospatiale*, however, courts have largely disfavored conducting discovery under the Hague Convention.[170] Responding parties may be placed in the position of either refusing to comply with U.S. discovery or potentially violating foreign law on cross-border transfer of personal data. Parties in this position should seek a stipulation or court order to protect social media data in a manner consistent with applicable data protection laws.[171] This may include producing data in an anonymized or redacted format, or agreeing to phased productions that prioritize reviewing social media information of U.S. custodians before that of custodians outside the U.S.[172]

Even parties who successfully use the Hague Convention may find, however, that it provides little relief. Not all European member states are parties to the Convention. Nor have they all

---

169. *See id.* at 544, n.28 (listing comity factors) (quoting RESTATEMENT (REVISED) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 437(1)(c) (AM. LAW. INST., Tentative Draft No. 7, 1986) (approved May 14, 1986)).

170. *See* Geoffrey Sant, *Court-Ordered Law Breaking: U.S. Courts Increasingly Order the Violation of Foreign Law*, 81 BROOK. L. REV. 181, 237 (2015) (conducting a statistical analysis of the application of the *Aérospatiale* five-factor test in U.S. courts and concluding that "there is overwhelming evidence of pro-forum bias").

171. *See* The Sedona Conference, *International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition)*, Principle 4, THE SEDONA CONFERENCE (Jan. 2017), https://thesedonaconference.org/publication/International_Litigation_Principles ("Where a conflict exists between Data Protection Laws and preservation, disclosure, or discovery obligations, a stipulation or court order should be employed to protect Protected Data and minimize the conflict.").

172. *See* The Sedona Conference, *Practical In-House Approaches for Cross-Border Discovery & Data Protection*, Practice Point #7, 17 SEDONA CONF. J. 397, 423–26 (2016).

agreed to comply with pretrial discovery requests from treaty signatories.[173] As a result, cross-border discovery requests for social media content may be rejected even if those requests are reasonable and proportional.[174]

Alternatively, Article 49 of the GDPR provides that transfers of personal data to a third country may take place outside of additional methods delineated in Article 45 and 46,[175] under one of several special circumstances, including if "the transfer is necessary for the establishment, exercise or defence of legal claims."[176] This language mirrors the prior governing Directive 95/46/EC, which allowed such transfers only if the transfer involved a "single transfer of all relevant information" and did

---

173. For additional information regarding Article 48, see David J. Kessler, Jamie Nowak & Sumera Khan, *The Potential Impact of Article 48 of the General Data Protection Regulation on Cross Border Discovery From the United States*, 17 SEDONA CONF. J. 575 (2016).

174. *See*, *e.g.*, *In re* Baycol Products Litig., 348 F. Supp. 2d 1058, 1059 (2004) (issuing order permitting the service of letters rogatory in Italy despite evidence of Italy's "complete refusal to execute Letter Requests for pretrial discovery pursuant to the [Hague] Convention"). The Italian courts rejected the request to conduct pretrial discovery, citing the state's reservation under Article 23 of the Hague Convention. *See In re* Baycol Products Litig., 01-md-01431-MJD-SER, ECF No. 4052-14 (D. Minn. Nov. 29, 2005) ("[N]essun dubio, pertanto . . . che la richiesta assolva una finalità puramenta esplorativa, incompatibile con la lettera or lo spirito della riserva. In conclusione, la richiesta non può essere accolta.").

175. GDPR, *supra* note 160, at art. 45 (providing that transfers may take place where the EU Commission has decided that the third country "ensures an adequate level of protection"); *Id.* at art. 46 (allowing transfers subject to appropriate safeguards such as binding corporate rules).

176. *Id.* at art. 49(1)(e); Article 29 Data Protection Working Party, WP 158, 00339/09/EN (Feb. 11 2009), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp158_en.pdf. The Working Party recognizes the need for pretrial discovery with safeguards such as proportionality deployed to protect parties responding to discovery requests or third-party subpoenas. *Id*.

not involve the transfer of "a significant amount of data."[177] Article 49 of the GDPR should also be read in conjunction with Recital 115 of the GDPR, which states that transfers that "are not based on an international agreement . . . should only be allowed where the conditions of this Regulation for a transfer to third countries are met."

Because the United States lacks the type of data protection that the EU considers "adequate," a provision was created to permit companies to transfer EU personal data when companies agreed to comply with EU data protection standards. However, that provision—the "U.S.-EU Safe Harbor Framework"—was invalidated in 2015.[178] It was replaced by the "EU-U.S. Privacy Shield Framework" in 2016.[179] The Privacy Shield provides participating companies with a legal mechanism for the transfer of personal data from the EU to the United States.[180] Companies must be subject to the jurisdiction of the Federal Trade Commission or the Department of Transportation to be eligible.

Parties seeking cross-border discovery of social media from participating companies must satisfy the Privacy Shield or otherwise reach an acceptable data transfer agreement that incorporates standard contractual clauses providing for the protection of personal data. Individuals may elect to opt out of allowing their personal information to be disclosed to third

---

177. *Id.* at 9–10 (referring to art. 26(1)(d) of the Directive).

178. *See* Case C-362/14, Maximillian Schrems v. Data Prot. Comm'n, 2015 E.C.R. I-1-35 (Oct. 6, 2015).

179. Commission Implementing Decision 2016/1250, of July 12, 2016, 2016 O.J. (L 207) (EU), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG.

180. For more information regarding the Privacy Shield, see Doron S. Goldstein, Megan Hardiman, Matthew R. Baker & Joshua A. Druckerman, *Understanding The EU-US "Privacy Shield" Data Transfer Framework*, 20 No. 5 J. INTERNET L. 1 (2016).

parties, however, potentially limiting discovery efforts. The General Court of the EU recently dismissed an action seeking to annul the Privacy Shield, but the Privacy Shield may face another challenge from the Article 29 Working Party if U.S. authorities do not address outstanding concerns, including additional guidance on onward transfers.[181] Moreover, the continued vitality of the standard contractual clauses has also been called into question. This issue will remain unsettled until the Court of Justice of the European Union delivers a definite ruling.

Finally, European laws governing the relationship between employers and employees also change the nature of data collection and transfer. Increasingly, employees are formally or informally using personal social media accounts for business purposes or on business devices. There is a steeper burden in the EU to obtaining sensitive personal information through U.S. discovery.[182] European nations generally extend an employee's expectation of privacy to workplace communications. Employers must obtain *written* informed consent from employees in advance of preserving, collecting, or producing social media content reflecting personal data. To ensure that consent is informed, employees must be aware who the data controller is and each purpose for which their personal data will be used. Employee consent is viewed with suspicion in the EU and will not be regarded as truly voluntary or "freely given" where the employee

181. Article 29 Data Protection Working Party, EU-U.S. Privacy Shield—First Annual Joint Review, WP 255, 17/EN (Nov. 28, 2017), https://iapp.org/media/pdf/resource_center/Privacy_Shield_Report-WP29pdf.pdf.

182. GDPR, *supra* note 160, at art. 9; *cf*. *In re* Xarelto (Rivaroxaban) Prod. Liab. Litig., No. MDL 2592, 2016 WL 3923873, at *19–20 (E.D. La. July 21, 2016) (ordering production of privilege log detailing extent of "sensitive employee information" in personnel files to determine which categories of personal data should be redacted in compliance with Germany's data protection law).

had no "genuine or free choice" or is unable to refuse or withdraw consent without consequence.[183]

B. Asia

The Asia-Pacific Economic Cooperation (APEC) is a forum for twenty-one member-nations. The APEC Privacy Framework sets out nine guiding principles related to privacy.[184] Similar to the EU, the APEC Privacy Framework takes a broader view of privacy and more stringent protections than in the United States. The APEC Cross-Border Transfer Guidelines ("CBTG") provide a framework for the transfer of personal data by participating companies.[185] It is similar to the EU-U.S. Privacy Shield.[186] The United States has joined the CBTG. Parties seeking cross-border discovery of social media must satisfy the CBTG or otherwise reach an acceptable data transfer agreement that provides for the protection of personal data.

A more thorough analysis of treaties, laws, and regulations affecting cross-border discovery of social media is beyond the scope of the *Primer*. The Sedona Conference's *Practical In-House Approaches for Cross-Border Discovery & Data Protection*[187] and *International Principles on Discovery, Disclosure & Data Protection in*

183. *Recital 42 Burden of Proof and Requirements for Consent*, INTERSOFT CONSULTING, https://gdpr-info.eu/recitals/no-42/ (last visited Dec. 17, 2018).

184. *See APEC Privacy Framework*, APEC (2005), https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework.

185. *Cross Border Privacy Rules System*, CBPRS, http://www.cbprs.org/ (last visited Dec. 17, 2018).

186. *See* M. James Daley, Jason Priebe & Patrick Zeller, *The Impact of Emerging Asia-Pacific Data Protection And Data Residency Requirements On Transnational Information Governance And Cross-Border Discovery*, 16 SEDONA CONF. J. 201 (2015).

187. 17 SEDONA CONF. J. 397 (2016).

Civil Litigation (Transitional Edition)[188] provide additional information, as well as guidance and best practices regarding the interplay between cross-border laws and regulations and the U.S. discovery process.

188. *See* The Sedona Conference, *International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition)*, *supra* note 171.

V. AUTHENTICATION OF SOCIAL MEDIA EVIDENCE

Authenticity is a key issue that a court must consider in determining the admissibility of social media evidence. In determining admissibility, a court may consider a number of issues, including relevance, hearsay, the original writing rule, probative value, and authenticity—i.e., is the evidence what its proponent purports it to be?[189] Commentators have observed that "[w]hile there are multiple evidentiary issues that affect the admissibility of any electronic evidence, the greatest challenge is how to authenticate digital evidence."[190] That observation has proven to be particularly true regarding social media evidence.

A. General Authentication Requirements

As with other forms of evidence, a party seeking admission of social media content must authenticate it by providing proof "sufficient to support a finding that the item is what the proponent claims it is."[191] Federal Rule of Evidence ("FRE") 901(b) sets out various examples of evidence that satisfy the authentication requirement, the most common example being testimony of a witness with knowledge that the item is what it is claimed to be.[192]

---

189. *See* Lorraine v. Markel Am. Ins. Co., 241 F.R.D. 534, 538-54 (D. Md. 2007) (discussing the issues that a court may need to consider in determining the admissibility of ESI).

190. Paul W. Grimm, Lisa Yurwit Bergstrom & Melissa M. O'Toole-Loureiro, *Authentication of Social Media Evidence,* 36 AM. J. TRIAL ADVOC. 433, 439 (2013).

191. FED. R. EVID. 901(a).

192. FED. R. EVID. 901(b)(1). Requests for Admission offer an alternative method for authenticating social media evidence. *See* FED. R. CIV. P. 36(a)(1)(B) ("A party may serve on any other party a written request to admit, for purposes of the pending action only, the truth of any matters within the scope of Rule 26(b)(1) relating to . . . the genuineness of any described documents.").

A document or ESI also can be authenticated by "distinctive characteristics" of the document itself, such as its appearance, contents, substance, internal patterns, or other distinctive characteristics, "taken together with all the circumstances."[193] Evidence "describing a process or system and showing that it produces an accurate result" can also be used to authenticate documents or ESI.[194] Additionally, "ancient" documents or data compilations—those 20 years or older at the time they are proffered, according to the rule—may be authenticated by evidence that they are in a condition that creates no suspicion about their authenticity and they were in a place where, if authentic, they would likely be.[195] Significantly, however, the 2017 amendments to the FRE included an amendment to FRE 803(16) that imposes a cutoff date, limiting the hearsay rule's "ancient records" exception to documents (and ESI) created before 1998.[196]

The Advisory Committee's note states that these are "not intended as an exclusive enumeration of allowable methods but are meant to guide and suggest, leaving room for growth and development in this area of the law."[197] The trial judge is ordinarily responsible for making preliminary determinations with respect to the admissibility of evidence, including whether the evidence is authentic.[198] If there is a genuine dispute of fact

193. *See* FED. R. EVID. 901(b)(4).

194. *See* FED. R. EVID. 901(b)(9).

195. *See* FED. R. EVID. 901(b)(8).

196. FED. R. EVID. 803(16) advisory committee's note to 2017 amendment. The note sets forth the rationale for the amendment: "Given the exponential development and growth of electronic information since 1998, the hearsay exception for ancient documents has now become a possible open door for large amounts of unreliable ESI, as no showing of reliability needs to be made to qualify under the exception." *Id*.

197. *See* FED. R. EVID. 901(b) advisory committee's note on proposed rules.

198. *See* FED. R. EVID. 104(a).

regarding authenticity, however, the ultimate trier of fact (the jury in non-bench trials) may have the responsibility of resolving the factual dispute.[199]

B. Self-Authentication

Self-authentication may be important for authenticating social media evidence, particularly where the author is unavailable or denies having made a social media post. FRE 902 provides that certain evidence is "self-authenticating" and, therefore, does not require the live testimony of a foundational witness. For example, information satisfying the business records exception to the hearsay rule may be authenticated through the certification—or declaration—under oath of the custodian or other qualified person.[200] Reasonable advance written notice and access to the certification and record must be given to the adverse party, who can then challenge its authenticity.[201]

In December 2017, the Federal Rules of Evidence were amended to add two new subdivisions to FRE 902 that may apply to social media evidence. The first provision, FRE 902(13), allows self-authentication of machine-generated information (i.e., a "record generated by an electronic process or system that produces an accurate result") upon submission of a certification prepared by a qualified person.[202] The second provision, FRE

199. *See* FED. R. EVID. 104(b) and advisory committee's note. *See also* Grimm, Bergstrom & O'Toole-Loureiro, *supra* note 190, at 440, 458–61 (stating that the conditional relevance rule applies and the jury determines the facts in the "comparatively less frequent case where the proponent of the evidence proves facts sufficient to justify a jury's conclusion that the evidence is authentic, and the opponent proves facts that also would justify a reasonable jury in reaching the opposite conclusion").

200. FED. R. EVID. 902(11), 902(12).

201. *See id*.

202. FED. R. EVID. 902(13).

902(14), allows a similar certification procedure for data "copied from an electronic device, storage medium or file, if authenticated by a process of digital identification," for example its hash value.[203] The committee note states that "[t]his amendment allows self-authentication by a certification of a qualified person that she checked the hash value of the proffered item and that it was identical to the original."[204]

The Advisory Committee wrote that "[a]s with the provisions on business records in Rules 902(11) and (12), the Committee has found that the expense and inconvenience of producing a witness to authenticate an item of electronic evidence is often unnecessary."[205] A party often goes to the expense of producing an authentication witness "and then the adversary either stipulates authenticity before the witness is called or fails to challenge the authentication testimony once it is presented."[206] The addition of FRE 902(13) and (14) therefore provide "a procedure under which the parties can determine in advance of trial whether a real challenge to authenticity will be made, and can then plan accordingly."[207]

The self-authentication procedures of FRE 902(13) and (14) have the effect of shifting to the adverse party the burden of raising any issues with the authenticity of the proffered digital evidence. They do not, however, shift the burden of *proof* of

---

203. FED. R. EVID. 902(14).

204. FED. R. EVID. 902(14) advisory committee's note to 2017 amendment. The committee note also states that "[t]he rule is flexible enough to allow certifications through processes other than comparison of hash value, including by other reliable means of identification provided by future technology." *Id.*

205. *Id*.

206. *Id*.

207. *Id*.

demonstrating authenticity. The proffering party still has the burden of proving that the evidence is what it claims it to be.[208]

C. Judicial Interpretations

Courts have wrestled with authentication of social media evidence out of concern that the data can be easily manipulated—for example, that "someone other than the alleged author may have accessed the account and posted the message in question" or that the alleged author did not even create the account.[209] Consequently, early cases addressing authenticity of social media in some jurisdictions required "greater scrutiny" and particular methods of authentication for social media compared to other forms of evidence (sometimes effectively requiring a showing that the social media account or post was *not* hacked or manipulated).[210] In other jurisdictions, by contrast, a

---

208. *See, e.g.*, *id.* ("If the certification provides information that would be insufficient to authenticate the record if the certifying person testified, then authenticity is not established under this Rule.").

209. *See* Griffin v. State, 419 Md. 343, 357–64 (2011) (overturning murder conviction when State failed to supply the additional extrinsic evidence necessary to properly attribute Myspace profile and postings to the alleged author; the court held that simply confirming that the profile photo, nickname, and birthday were the author's was insufficient because "anyone can create a fictitious account and masquerade under another person's name or can gain access to another's account by obtaining the user's username and password").

210. *See, e.g.*, *id.*; State v. Eleck, 23 A.3d 818, 822–25 (Conn. App. Ct. 2011) (holding that a printout of an instant message from defendant's Facebook page was not properly authenticated where there was no assurance that defendant's account was not hacked); Commonwealth v. Williams, 456 Mass. 857 (Mass. 2010) (finding that a message was not properly authenticated, even though it came from purported sender's Myspace page, because "there is no testimony (from [the recipient] or another) regarding how secure such a Web page is, who can access a MySpace Web page, whether codes are needed for such access, etc.;" nor was there testimony that circumstantially

proponent could authenticate social media evidence using any type of evidence so long as the proponent demonstrated to the trial judge that a jury could reasonably find that the social media evidence was authentic.[211]

These divergent approaches were at one time described as the "Maryland approach" and the "Texas approach,"[212] although the courts in Maryland have since changed course and adopted the lower threshold and more flexible evidentiary showing requirements of the Texas approach.

Under the Maryland approach, the Maryland Court of Appeals previously required the proffering party to submit sufficient evidence to convince the trial court that a social media post was *not* falsified or created by another user.[213] Methods for doing so, according to the court, included the testimony of the purported creator of the post, forensic examination of the internet history or hard drive of the purported creator's computer, or information obtained directly from the social media site.[214]

By contrast, under the Texas approach, the Texas Court of Criminal Appeals stated that "the best or most appropriate method for authenticating electronic evidence will often depend upon the nature of the evidence and the circumstances of the

---

"identif[ied] the person who actually sent the communication"); People v. Mills, III, No. 293378, 2011 WL 1086559, at *13 (Mich. Ct. App. Mar. 24, 2011) (finding photographs from a Myspace page were not properly authenticated, in part because the proponent of the evidence "ha[d] no way of knowing if the photos were altered in any way").

211. *See, e.g.*, Tienda v. State, 358 S.W.3d 633 (Tex. Crim. App. 2012).

212. *See* Parker v. State, 85 A.3d 682, 684 (Del. 2014) (describing the two approaches and finding that the Texas approach "better conforms to the requirements . . . of the Delaware Rules of Evidence").

213. *See id*.

214. *Id.*; *Griffin*, 419 Md. at 357–64.

particular case."[215] This could include "direct testimony from a witness with personal knowledge, . . . comparison with other authenticated evidence, or . . . circumstantial evidence."[216] Rather than imposing a requirement that the proponent prove the social media evidence was not fraudulent, the Texas court explained that the standard for determining admissibility is whether "a jury could reasonably find [the] proffered evidence authentic."[217]

The trend has moved away from the Maryland approach, which required greater scrutiny and particular evidence for authenticating social media, and towards the Texas approach, with most courts applying the same authentication standard that would apply to other forms of evidence—i.e., whether there is proof from which a reasonable juror could find that the evidence is what the proponent claims it to be.

In *United States v. Vayner*, for example, with respect to authenticating social media evidence, the Second Circuit articulated the standard as whether "sufficient proof has been introduced so that a reasonable juror could find in favor of authenticity or identification."[218] The court stated that FRE 901 ''does not definitively establish the nature or quantum of proof that is required preliminarily to authenticate an item of evidence."[219] The court also stated that "the bar for authentication of evidence is not particularly high."[220]

---

215. *Tienda*, 358 S.W.3d at 639.

216. *Id.* at 638.

217. *Id.* Other courts following the Texas approach include: State v. Assi, 2012 WL 3580488, at *3 (Ariz. Ct. App. Aug. 21, 2012); People v. Valdez, 201 Cal. App. 4th 1429 (2011); People v. Clevenstine, 891 N.Y.S.2d 511, 514 (N.Y. App. Div. 2009).

218. United States v. Vayner, 769 F.3d 125, 129–30 (2d Cir. 2014).

219. *Id.* (internal quotes and citation omitted).

220. *Id.* (internal quotes and citation omitted).

In 2015, the Court of Appeals of Maryland in *Sublet v. State* itself changed course away from the "greater scrutiny" standard and "embrace[d]" the Second Circuit's articulation of the standard in *Vayner*. *Sublet* held that "to authenticate evidence derived from a social networking website, the trial judge must determine that there is proof from which a reasonable juror could find that the evidence is what the proponent claims it to be."[221] The court stated that the preliminary determination of authentication made by the trial judge is a "context-specific determination" based on proof that "may be direct or circumstantial."[222] It noted that "[t]he standard articulated in *Vayner* . . . is utilized by other federal and State courts addressing authenticity of social media communications and postings."[223]

Although the bar for authentication may not be "particularly high," courts have nevertheless required reliable evidence that the social media content being proffered is what the party presenting it purports it to be. In *Vayner*, for example, the Second Circuit held that the trial court had abused its discretion in authenticating evidence based on a profile page from a Russian

---

221. Sublet v. State, 113 A.3d 695, 698, 718, 722 (Md. 2015) (citing *Vayner*, 769 F.3d 125).

222. *Id.* at 715 (citing *Vayner*, 769 F.3d at 129–30).

223. *Id.* at 718 (citing United States v. Hassan, 742 F.3d 104, 133 (4th Cir. 2014); Parker v. State, 85 A.3d 682, 688 (Del. 2014) ("Thus, the trial judge as the gatekeeper of evidence may admit the social media post when there is evidence sufficient to support a finding by a reasonable juror that the proffered evidence is what its proponent claims it to be." (internal quotations marks and footnote omitted)) ("a proponent can authenticate social media evidence using any type of evidence so long as he or she can demonstrate to the trial judge that a jury could reasonably find that the proffered evidence is authentic"); Tienda v. State, 358 S.W.3d 633, 638 (Tex. Crim. App. 2012) ("The preliminary question for the trial court to decide is simply whether the proponent of the evidence has supplied facts that are sufficient to support a reasonable jury determination that the evidence he has proffered is authentic.").

social networking site. The profile page included a variation of defendant's name, a photo of defendant, two places of employment where defendant had allegedly worked in the past, and a Skype moniker that matched the moniker contained in the email address alleged to have been used to transfer a false document.[224]

The Second Circuit found that "the government presented insufficient evidence that the page was what the government claimed it to be—that is, [defendant's] profile page, as opposed to a profile page on the Internet that [defendant] did not create or control."[225] The court compared the profile page to "a flyer found on the street that contained [defendant's] Skype address and was purportedly written or authorized by him," and reasoned "the district court surely would have required some evidence that the flyer did, in fact, emanate from [defendant]."[226]

Finally, while authentication is by its nature very fact-specific to the evidence and context, courts generally seem to agree that the mere testimony of the person who downloaded or printed out social media content, without more, is insufficient to establish its authenticity.[227] Accordingly, parties proffering

224. *Vayner*, 769 F.3d at 127–28.

225. *Id.* at 127.

226. *Id.* at 132. *Cf. Tienda*, 358 S.W.3d at 645–46.

227. *See, e.g.*, Moroccanoil, Inc. v. Marc Anthony Cosmetics, Inc., 57 F. Supp. 3d 1203 n.5 (C.D. Cal. Sept. 16, 2014) ("Defendant's argument, that [Facebook screenshots] could be 'authenticated' by the person who went to the website and printed out the home page, is unavailing. It is now well recognized that 'Anyone can put anything on the internet.' [citations omitted] No website is monitored for accuracy."); Linscheid v. Natus Med. Inc., No. 3:12-cv-76-TCB, 2015 WL 1470122, at *5–6 (N.D. Ga. Mar. 30, 2015) (finding LinkedIn profile page not authenticated by declaration from individual who printed the page from the internet); Monet v. Bank of America, N.A., No. H039832, 2015 WL 1775219, at *8 (Cal. Ct. App. Apr. 16, 2015) (finding that a "memorandum by

social media content should make sure they develop and present foundational evidence beyond simply printing or downloading the content from the internet.

an unnamed person about representations others made on Facebook is at least double hearsay" and not authenticated).

VI. ETHICAL ISSUES RELATED TO SOCIAL MEDIA AS POTENTIAL EVIDENCE

Social media discovery implicates various ethics rules for counsel. These rules involve the preservation and production of such information and the equally significant issue of attorney use of social media.

A. Attorney Duty of Competence

Ethics rules require lawyers to understand the impact and consequences of social media use by clients and counsel. The duty of competence, for example,[228] requires that counsel must render competent representation by providing "the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation."[229] Legal knowledge and skill include keeping current with "the benefits and risks associated with relevant technology."[230]

B. Attorney Advice Related to Client Use of Social Media

To remain current and thereby understand the benefits and risks of technology, counsel should be able to competently use social media or to employ other counsel with such

228. *See also* Jan L. Jacobowitz and Danielle Singer, *The Social Media Frontier: Exploring a New Mandate for Competence in the Practice of Law*, 68 U. MIAMI L. REV. 445 (2014).

229. MODEL RULES OF PROF'L CONDUCT R. 1.1 (Am. Bar Ass'n 1980) ("ABA Model Rules").

230. *Id.* at R. 1.1 cmt. 8. More than 27 states have adopted a duty of competence in technology. *See* Robert Ambrogi, *Another State Adopts Duty to Technology Competence and Canada May Also,* LAWSITES (Mar. 8, 2017), https://www.lawsitesblog.com/2017/03/another-state-adopts-duty-technology-competence-canada-may-also.html.

competence.[231] When attorneys are able to use social media themselves, they may be able to advise clients more effectively concerning their duties regarding social media in discovery.[232]

1. Advising Clients on Social Media Preservation

Several states have issued ethics opinions or guidelines relating to attorneys counseling clients regarding their use of social media. Those opinions generally provide that attorneys may advise clients regarding changing privacy settings or removing content, as long as they also satisfy preservation obligations and do not obstruct another party's access to evidence.[233] In other words, "[u]nless an appropriate record of the social media content is preserved, a party or nonparty may not delete information from a social media account that is subject to a duty to preserve."[234]

For example, an attorney may advise a client regarding changing privacy or security settings to limit access to the client's social media outside of the formal discovery context.[235]

---

231. *See* MODEL RULES OF PROF'L CONDUCT R. 1.1, cmt. 6. *But see* The State Bar of California Standing Committee on Professional Responsibility and Conduct, Formal Op. No. 2015-193 (2015) (providing that a lawyer "lacking the required competence for e-discovery issues" may choose to "associate with or consult technical consultants or competent counsel").

232. *See* N.Y. Cnty. Lawyers' Ass'n., Ethics Op. 745, at 3 (2013) (observing that competent representation could require counsel to advise clients regarding the impact of their social media use on their claims).

233. *See* MODEL RULES OF PROF'L CONDUCT R. 3.4.

234. *See Social Media Ethics Guidelines of the Commercial and Federal Litigation of the New York State Bar Association,* Guideline 5.A, NYSBA, https://www.nysba.org/socialmediaguidelines17/ (updated May 11, 2017).

235. *See id.* ("A lawyer may advise a client as to what content may be maintained or made non-public on her social media account, including advising on changing her privacy and/or security settings." (footnotes omitted)). *See also* N.C. State Bar Ass'n, Formal Ethics Op. 5 (2014); Pa. Bar Ass'n., Formal

Similarly, an attorney may advise a client to "take down" or remove content, as long as it is does not violate substantive law or the duty to preserve.[236]

Both the substantive legal consequences for a party and ethical consequences for the attorney are illustrated in *Lester v. Allied Concrete Company*.[237] *Lester* was a wrongful death case in which the defense learned that the plaintiff's Facebook page might have relevant photos, including a photo of the plaintiff surrounded by women, with a beer in hand, wearing a t-shirt reading "I [heart] hot moms." The defendant served requests for production seeking pages from the plaintiff's Facebook page. Because those images could have undermined his claim for loss of consortium, plaintiff's counsel instructed his paralegal to have the plaintiff "clean up" his Facebook page. In an email to the client, the paralegal instructed the plaintiff "[w]e do NOT want blow ups of other pics at trial so please, please clean up your facebook and myspace!" The plaintiff told the paralegal he had deleted his Facebook page, and only then did his attorney respond to the discovery request by stating, "I do not have a Facebook page on the date this is signed." Following a motion to compel, forensics experts identified sixteen photos deleted from the account.

Op. 2014-300 (2014) ("[A] competent lawyer should advise clients about the content that they post publicly online and how it can affect a case or other legal dispute."); Fla. Bar Ass'n, Ethics Op. 14-1 (2015); N.Y. Cnty. Lawyers' Ass'n., Ethics Op. 745 (2013).

236. *See Social Media Ethics Guidelines, supra* note 234; D.C. Bar Ass'n, Ethics Op. 371 (2016) ("Before any lawyer-counseled or lawyer-assisted removal or change in content of client social media [occurs], at a minimum, an accurate copy of such social media should be made and preserved, consistent with Rule 3.4(a)."); N.C. State Bar Ass'n, Formal Ethics Op. 5 (2014); W. Va. Office of Disciplinary Counsel, Legal Ethic Op. No. 2015-02; Fla. Bar Ass'n, Ethics Op. 14-1 (2015); N.Y. Cnty. Lawyers' Ass'n., Ethics Op. 745 (2013).

237. Allied Concrete Co. v. Lester, 285 Va. 295, 736 S.E.2d 699 (2013).

As a result of the misconduct, the trial court issued adverse inference instructions and sanctions of $542,000 against plaintiff's counsel and $180,000 against plaintiff to cover attorney fees and costs associated with the spoliation. The sanctions were affirmed on appeal. In response to disciplinary action initiated by the Virginia state bar, plaintiff's counsel agreed to a five-year suspension of his law license.[238]

Lester is instructive on the need for counsel to follow ABA Model Rule 3.4 and not advise clients to destroy or neglect to preserve relevant social media content.[239] To ensure compliance with Rule 3.4, counsel should work with clients to issue timely litigation holds and take other reasonable steps to preserve relevant social media evidence.[240]

A client's use of ephemeral messaging for relevant communications after a duty to preserve has arisen may be particularly problematic, as it would have the potential to deprive adversaries and the court of relevant evidence.[241] Counsel should be

---

238. *In re* Matthew B. Murray, VSB Docket Nos. 11-070-088405, 11-070-088422 (July 17, 2013).

239. *See* Painter v. Atwood, No. 2:12–cv–01215–JCM–RJJ, 2014 WL 1089694 (D. Nev. Mar. 18, 2014), *aff'd* 2014 WL 3611636 (D. Nev. July 21, 2014) (imposing an adverse inference on plaintiff and observing that plaintiff's counsel should have advised her to have preserved relevant social media images and comments).

240. *See supra* Section III(C). *See also* The Sedona Conference, *Commentary on Legal Holds, Second Edition: The Trigger & The Process*, *supra* note 29 (providing substantive guidance and best practices for satisfying preservation obligations).

241. *See supra* Section II(B)(3). *See also* Waymo LLC v. Uber Tech., Inc., No. C 17-00939 WHA, 2018 WL 646701 (Jan. 30, 2018) (holding that plaintiff could present evidence and argument to the jury regarding defendant's use of "ephemeral messaging" to destroy evidence regarding trade secret theft); Philip J. Favro & Keith A. Call, *A New Frontier in eDiscovery Ethics: Self-Destructing Messaging Applications*, 31 UTAH BAR J. 40 (2018).

aware of the risks of ephemeral messaging and advise their clients accordingly.

2. Attorney Use of Social Media for Discovery

Counsel must remember the rules of professional conduct when seeking social media content through informal methods or through the formal discovery process. Either scenario can present ethical traps.

Counsel may informally seek messages, posts, or other social media content, as the rules of professional conduct do not impose a blanket prohibition on such discovery. This occurs when social media content is available on sites, applications, or the internet without restrictions. In contrast, when relevant content is not readily available without obtaining formal permission from the social media user, ethical violations can occur.

A quintessential example of this type of professional misconduct occurs when counsel seeks a connection on social media with a person who is or may become a party, witness, or juror in a lawsuit. These requests have the potential to violate ABA Model Rule 4.2 or 4.3. Rule 4.2 generally forbids a lawyer from making contact with a person who is represented by counsel.[242] Rule 4.3 governs a lawyer's behavior in making contact with unrepresented persons.[243]

Even if that person is not represented by counsel, a lawyer's connection request may violate ABA Model Rule 8.4(c). Rule 8.4(c) prohibits "conduct involving dishonesty, fraud, deceit or misrepresentation." Unless counsel fully discloses the nature and purpose of the friend request, i.e., to obtain information in

242. *See* MODEL RULES OF PROF'L CONDUCT R. 4.2; *see also* Yvette Ostolaza & Ricardo Pellafone, *Applying Model Rule 4.2 to Web 2.0: The Problem of Social Networking Sites*, 11 J. HIGH TECH. L. 56 (2010).

243. *See* MODEL RULES OF PROF'L CONDUCT R. 4.3.

connection with a particular lawsuit, it may be deemed deceptive or dishonest, thereby violating Rule 8.4(c).[244]

If there is any doubt regarding the propriety of counsel's method for seeking social media evidence, the more prudent course is to use the formal discovery process.

Formal discovery does not eliminate the potential for ethical challenges. Social media accounts are often a dossier of private or sensitive information including correspondence with intimates, notations that are the equivalent of journal entries, and photographs. Discovery requests that demand the entirety of a person's social media account without reasonable limitations on time or scope may be considered harassing, burdensome, or otherwise improper. Such "frivolous" requests may thus violate the proportionality certification of FRCP 26(g)[245] and could also be grounds for discovery sanctions.[246]

---

244. *See also* San Diego County Bar Ass'n, Legal Ethics Op. 2011-2 ("We have further concluded that the attorney's duty not to deceive prohibits him from making a friend request even of unrepresented witnesses without disclosing the purpose of the request."); Agnieszka McPeak, *Social Media Snooping and its Ethical Bounds*, 46 ARIZ. ST. L.J. 845, 886 (2014) ("Any lawyer seeking private access to an unrepresented person's social media page for the purposes of gathering information to use in litigation should assume the target misunderstands the lawyer's intent, purpose, and role.").

245. FED. R. CIV. P. 26(g)(1).

246. FED. R. CIV. P. 26(g)(3). *See also* MODEL RULES OF PROF'L CONDUCT R. 3.4(d) ("A lawyer shall not: (d) in pretrial procedure, make a frivolous discovery request . . . .").

VII. CONCLUSION

While the *Primer* offers insightful guidance on social media discovery issues as they stand in 2019, social media will almost certainly remain a dynamic area for technological development. As innovations continue to change the social media landscape, court decisions and other laws will likely advance to address new technological challenges. Counsel should therefore stay abreast of ongoing technological and legal developments to ensure continued understanding of the issues surrounding discovery of social media.

THE SEDONA CONFERENCE COMMENTARY ON INFORMATION GOVERNANCE, SECOND EDITION

A Project of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1)

Author:

The Sedona Conference

Drafting Team:

Michael Burg
Abigail Dodd
Thad Gelsinger
Ronald J. Hedges
Courtney Jones Kieffer
Mollie Nichols
Robb Snow
Joe Treese

Drafting Team Leader:

Cheryl Strom

Editors-in-Chief & WG1 Steering Committee Liaisons:

Dean Kuckelman
Kevin F. Brady
Heather Kolasinsky

Staff Editors:

David Lumia
Susan McClain

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 1. 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 Information Governance, Second Edition,* 20 SEDONA CONF. J. 95 (2019).

PREFACE

Welcome to the final, April 2019, version of The Sedona Conference *Commentary on Information Governance, Second Edition*, a project of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). 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, and intellectual property rights. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

In 2014, The Sedona Conference published its first edition of the *Commentary on Information Governance,* which recommended a top-down, overarching framework guided by the requirements and goals of all stakeholders that enables an organization to make decisions about information for the good of the overall organization and consistent with senior management's strategic directions. This Second Edition of the *Commentary on Information Governance* ("Second Edition") accounts for the changes and advances in technology and law over the past four years; underscores the role of IG as part of and complimentary to the business, rather than something separate that adds overhead; and emphasizes the costs of eDiscovery that should drive organizations to focus on IG on the front end, resulting in eDiscovery that is more efficient, less painful, and which allows the organization to reap additional benefits from a business perspective. Additionally, this Second Edition incorporates the knowledge and guidance embodied in the new and updated Sedona commentaries since 2014 such as *The Sedona Principles, Third Edition* and The Sedona Conference *Principles and Commentary on Defensible Disposition*. This Second Edition was first published for public comment in October 2018. Where appropriate, the comments received during the public comment period have now

been incorporated into this final version of the *Commentary on Information Governance, Second Edition*.

The Sedona Conference acknowledges the efforts of Drafting Team Leader Cheryl Strom, who was invaluable in driving this project forward. We also thank drafting team members Michael Burg, Abigail Dodd, Thad Gelsinger, Ron Hedges, Courtney Kieffer, Molly Nichols, Robb Snow, and Joe Treese for their efforts and commitments in time and attention to this project. Finally, we thank Dean Kuckelman, Kevin Brady, and Heather Kolasinsky, who served as both the Editors-in-Chief and WG1 Steering Committee Liaisons to the drafting team.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG1 and several other Working Groups in the areas of international electronic information management, discovery, and disclosure; patent damages and patent litigation best practices; data security and privacy liability; trade secrets; and other "tipping point" issues in the law. 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
April 2019

TABLE OF CONTENTS

THE SEDONA CONFERENCE PRINCIPLES OF INFORMATION GOVERNANCE

1. Organizations should consider implementing an Information Governance program to make coordinated, proactive decisions about information for the benefit of the overall organization that address information-related requirements and manage risks while optimizing value.
2. An Information Governance program should maintain sufficient independence from any particular department or division to ensure that decisions are made for the benefit of the overall organization.
3. All stakeholders' views/needs should be represented in an organization's Information Governance program.
4. The strategic objectives of an organization's Information Governance program should be based upon a comprehensive assessment of information-related practices, requirements, risks, and opportunities.
5. An Information Governance program should be established with the structure, direction, resources, and accountability to provide reasonable assurance that the program's objectives will be achieved.
6. The effective, timely, and consistent disposal of physical and electronic information that no longer needs to be retained should be a core component of any Information Governance program.
7. When Information Governance decisions require an organization to reconcile conflicting laws or obligations, the organization should act in good faith and give due respect to considerations such as data privacy, data protection, data security, records and

information management (RIM), risk management, and sound business practices.

8. If an organization has acted in good faith in its attempt to reconcile conflicting laws and obligations, a court or other authority reviewing the organization's actions should do so under a standard of reasonableness according to the circumstances at the time such actions were taken.
9. An organization should consider reasonable measures to maintain the integrity and availability of long-term information assets throughout their intended useful life.
10. An organization should consider leveraging the power of new technologies in its Information Governance program.
11. An organization should periodically review and update its Information Governance program to ensure that it continues to meet the organization's needs as they evolve.

I. INTRODUCTION

Information is one of modern businesses' most important assets. Like any asset, information can have great value but also pose great risk, and its governance should not be an incidental consideration. Despite these realities, there is no generally-accepted framework, template, or methodology to help organizations make decisions about information for the benefit of the organization rather than any individual department or function.

"Information Governance" as used in this commentary means an organization's coordinated, inter-disciplinary approach to satisfying information compliance requirements and managing information risks while optimizing information value. As such, Information Governance encompasses and reconciles the various legal and compliance requirements and risks faced by different information-focused disciplines, such as Records and Information Management (RIM),[1] data privacy,[2]

1. **RIM** is the standardized process to create, distribute, use, maintain, and dispose of records and information, regardless of media, format, or storage location, in a manner consistent with an organization's business priorities and applicable legal and regulatory requirements. RIM principles also provide for the temporary suspension of policies or processes that might result in the deletion of records or information subject to a legal hold.

2. **Data privacy** is the right to control the collection, sharing, and destruction of information that can be traced to a specific individual. In general, data privacy is more comprehensively protected outside of the United States, particularly in the European Union member states, where the Data Protection Directive provides significant restrictions on the processing and transfer of personal data, and other countries, including Argentina, Canada, Israel, Switzerland, and Uruguay. *See* Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 On the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=EN; 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

information security,[3] and electronic discovery (eDiscovery).[4] Understanding the objectives of these disciplines allows

---

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) 59, *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN [hereinafter GDPR] ("[A] data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation."). In the United States, the approach to data privacy is generally contractual and does not enjoy the same level of generic legal protections. Disparate laws in the United States do, however, mandate protections for specific types of data or target different groups. Examples include patient records under the Health Insurance Portability and Accountability Act (HIPAA), financial information under the Graham-Leach-Bliley Act (GLBA), and prohibitions on the collection of information about children younger than 13 years old under the Children's Online Privacy Protection Act (COPPA).

3. **Information security** is the process of protecting the confidentiality, integrity, and availability of information and assets, enabling only an approved level of access by authorized persons, and properly disposing of such information and assets when required or when eligible. Information security often focuses on limiting access to certain types of information that is important to the organization through various controls, including physical safeguards, technical access controls (e.g., permissions to read, write, modify, delete, browse, add, and rename), authorization challenges (e.g., usernames and passwords), and encryption technologies. Security requirements can be mandated by law (e.g., HIPAA Security Rule), contract, industry requirements (e.g., Payment Card Industry (PCI)), or company requirements and best practices.

4. **eDiscovery** is the process of identifying, preserving, collecting, preparing, analyzing, reviewing, and producing electronically stored information (ESI) relevant to pending or anticipated litigation or investigation or requested in government inquiries, after the application of any privileges or protections to the ESI.

functional overlap to be leveraged (if synergistic); coordinated (if operating in parallel); or reconciled (if in conflict).[5]

The position of The Sedona Conference is that Information Governance should involve a top-down, overarching framework guided by the requirements and goals of all stakeholders that enable an organization to make decisions about information for the good of the overall organization and consistent with senior management's strategic directions.

This paper explains the need for a comprehensive approach to Information Governance. The paper addresses the following:

- why traditional, siloed approaches to managing information have prevented adequate consideration of information value, risk, and compliance for the organization as a whole;
- how hard costs, soft costs, opportunity costs, and risk accumulate for organizations lacking adequate control of information;
- the definition of Information Governance, its fundamental elements, and the resulting benefits to the organization, which include the efficient and effective use of—and accessibility to—information; and
- the crucial role of executive sponsorship and ongoing commitment.

5. *See* Appendix A for additional discussion of the intersections of these disciplines.

II. THE INFORMATION GOVERNANCE IMPERATIVE

We live and work in an information age that is continually—and inexorably—transforming how we communicate and conduct business. Regardless of an organization's size, mission, marketplace, or industry, information is a crucial asset for all organizations. However, retaining extensive volumes of unneeded information will eventually dilute the value of the information that is vital to an organization.

Also, if inadequately controlled, an organization's information can be a dangerous source of risk and liability. For example, an organization's failure to dispose of information that no longer adds value can increase the costs and risks of complying with discovery obligations.[6]

In addition, information control lapses can have significant repercussions, some of which can be highly public:

- Data privacy and security breaches, such as a nationwide credit-reporting agency that compromised sensitive personal information of up to 147 million Americans (about half of the country) in 2017.[7]
- A non-economic impact related to data privacy, such as a major retailer that contacted a frequent customer whose recent purchases suggested that she might be pregnant. When

6. *See* The Sedona Conference, *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1, 60 (2018) [hereinafter *The Sedona Principles, Third Edition*] ("There is often a direct correlation between an organization's IG program and the ease with which it can search for, identify, and produce information.").

7. Sara Ashley O'Brien, *Giant Equifax Data Breach: 143 Million People Could be Affected*, CNN BUSINESS, https://money.cnn.com/2017/09/07/technology/business/equifax-data-breach/index.html (Sept. 8, 2017).

the retailer sent special offers to the "expectant mother" (a teenaged girl), her parents intercepted the mailing and discovered their daughter's pregnancy. The ensuing publicity suffered by the retailer illustrates the potential risk inherent in poor Information Governance controls around a fundamental data mining process.[8]

- Recordkeeping compliance penalties, such as a national clothing retailer fined over $1 million by the U.S. Immigration and Customs Enforcement Agency for information compliance deficiencies in its I-9 employment verification system, and a retail pharmacy chain reaching an $11 million settlement with the U.S. Department of Justice for record-keeping violations under the Controlled Substances Act.[9]

Behind the headlines, however, is a more pervasive problem—the commonly unmeasured aggregation of hard costs, soft costs, opportunity costs, and risk borne by organizations that fail to effectively control their information.

---

8. Hon. John Facciola, Technology and e-Discovery Competence: Enhancing Your Career, Speech to University of Florida Levin School of Law (Oct. 6, 2014), *available at* https://www.youtube.com/watch?v=nNwn-Bqd_OwY.

9. Press Release, Immigration and Customs Enforcement, Department of Homeland Security, Abercrombie & Fitch Fined after I-9 Audit (Sept. 28, 2010), *available at* https://www.aila.org/infonet/ice-abercrombie-fitch-fined-after-i-9-audit; Press Release, Drug Enforcement Administration, Department of Justice, CVS to Pay $11 Million to Settle Civil Penalty Claims Involving Violations of Controlled Substances Act (April 3, 2013), *available at* https://www.dea.gov/press-releases/2013/04/03/cvs-pay-11-million-settle-civil-penalty-claims-involving-violations-0.

Knowingly or not, organizations face a fundamental choice: they can control their information, or, by default, they can allow their information to control them.

A. Siloed Approaches Fail to Govern Information

Many organizations have traditionally used siloed approaches when managing information, resulting in decisions being made without sufficient consideration of information value, risk, or compliance for the organization as a whole. Examples of these silos include the various departments or administrative functions within the organization that deal with the organization's information, such as Information Technology (IT), Legal, Compliance, RIM, Human Resources (HR), Finance, Data Governance, and the organization's various business units. Each business unit or administrative function commonly has its own goals and priorities, and, accordingly, its own Information Governance policies and procedures, as well as disparate data systems and applications.

Another type of information silo consists of those disciplines that deal with specialized categories of information issues, such as data privacy and security (focused on protection of regulated classes of information), eDiscovery (focused on preservation and production of information in litigation), and data governance[10] (focused on information reliability and efficiency). Over

10. We recognize that various definitions of "information governance" have been advanced (*see, e.g.*, Charles R. Ragan, *Information Governance: It's a Duty and It's Smart Business*, 19 RICH. J.L. & TECH. 12, 30–33 (2013), *available at* http://jolt.richmond.edu/jolt-archive/v19i4/article12.pdf), and that there is an emerging discipline called "data governance," and submit that data governance is a subset of our Information Governance concept. The Data Governance Institute, self-described as a mission-based and vendor-neutral authority on essential practices for data strategy and governance, defines "data governance" as "a system of decision rights and accountabilities for information-related processes, executed according to agreed-upon models which

time, these disciplines have developed their own terminologies and frameworks for identifying issues and addressing specific information challenges. The core shortcoming of the siloed approach to governing information is that those within particular silos are constrained by the culture, knowledge, and short-term goals of their business unit, administrative function, or discipline. They perceive information-related issues from the vantage point of what is familiar and important specifically to them. They often have no knowledge of gaps and overlaps in technology or information in relation to other silos within the organization. There is no overall governance or coordination for managing information as an asset, and there is no roadmap for the current and future use of information technology. Siloed decisions concerning information often have unintended consequences for the organization as a whole, with significant cost and risk repercussions, such as the following:

- An organization's individual business units independently make decisions about implementing information technology tools and systems, separate from the other business units. This results in duplication of technology and unneeded expense, and it prevents the efficient sharing of information, a valuable asset, across the organization.
- The IT Department establishes email account volume limits to relieve operational stress on

describe who can take what actions with what information, and when, under what circumstances, using what methods." *Definitions of Data Governance*, THE DATA GOVERNANCE INST., http://www.datagovernance.com/adg_data_governance_definition/ (last visited Feb. 4, 2019). So viewed, "data governance" does not address "why" an organization chooses to do certain things with its data and other information. The critical role of Information Governance is ensuring that actions that users take with information-related assets are consistent with organizational strategy.

an organization's email system. This results in personnel moving email to storage on local drives and devices, exacerbating both data security risks and difficulties in finding and preserving such email for litigation or business purposes.

- The IT Department enables enterprise information technology platforms absent any consideration of incorporating proper governance.
- Legal counsel issues overbroad litigation holds to avoid even a remote possibility of spoliation sanctions. This results in excessive costs in pending and future litigation and the unnecessary retention of data.
- Personnel conduct an organization's business on their own laptops and smartphones, under a Bring-Your-Own-Device ("BYOD") program to increase convenience and efficiency, but without sufficient BYOD policies, controls, or planning for naturally attendant consequences. This results in data security exposures, and difficulties in applying records retention policies and in preserving and collecting data for litigation.
- Privacy and information security controls are applied to an organization's service providers but are not used to ensure that service providers also meet the organization's records retention requirements. This results in inconsistent application of such requirements to records.
- Records managers initiate a robust data and email retention program without regard to potential technological limitations or the burden

> associated with retaining, searching, and reviewing the resulting data for eDiscovery purposes.

In the post-Sarbanes-Oxley world, many companies have adopted codes of conduct in which they broadly proclaim that the organization and its employees comply with all applicable laws (including privacy and data security requirements), protect confidential information, use electronic communications wisely, and follow procedures for retaining records. The siloed approach to addressing information issues, however, inevitably spawns a multitude of information-related policies adopted though various projects and initiatives. Thus, rather than a clear, uniform set of information policy guidance, employees face a cacophony of conflicting policies and procedures, making compliance virtually impossible in the heat of a competitive business environment, which negatively impacts productivity.

The "elephant in the room" is the organization's need to harness and control its information, coupled with the inadequacy of a siloed approach for accomplishing this crucial goal. The solution to this quandary is for organizations to find a way to bridge across their silos, so that issues of information compliance, risk, and value can be identified, understood, and addressed for the benefit of the entire organization.

B. Information Governance

Organizations that adopt Information Governance programs are able to bridge across silos, thereby perceiving and understanding information-related issues from the perspective of the overall organization. Information Governance also helps ensure that decisions and solutions regarding information compliance, risk controls, and value optimization will serve the needs of the entire organization rather than the insular needs of individual silos.

To accomplish Information Governance, organizations should do the following:

- Establish a structure for Information Governance, which will vary in form depending on the organization's size, complexity, culture, industry, and regulatory environment.
- Determine the organization's strategic objectives for Information Governance, based upon a comprehensive assessment of information-related practices, requirements, risks, and opportunities.
- Identify major stakeholders and understand those stakeholders' goals, needs, and concerns.
- Reconcile the various goals, compliance requirements, and risks addressed by different information-focused disciplines, such as RIM, privacy, information security, and eDiscovery.
- Implement an Information Governance program with the structure, direction, resources, and accountability to provide reasonable assurance that the program's strategic objectives will be achieved.

C. The Benefits of Information Governance are Significant

The advantages of establishing an Information Governance program are many and varied, depending upon the information-related issues and risks an organization faces. Beyond addressing the risks above, an organization-wide Information Governance program will help organizations achieve the following advantages, all of which add to the bottom line:

- Improved efficient access and effective use of information across an organization while it is still useful/valuable

- Business performance improvements, as users gain confidence that they can locate valuable information efficiently and reliably and better understand how to address information-related risks
- Realization of "option value," as the organization leverages existing information and technologies across diverse business units, consolidates technologies and administrative staff, and reduces license fees
- More reliable and efficient processes and procedures for eDiscovery and responses to audits and investigations and other incidents (e.g., a data breach)
- A framework for defensible disposition
- Better preparedness for new laws and emerging technologies that may introduce other challenges
- More effective risk management
- Reduced storage costs and administrative burdens, as obsolete and worthless information is eliminated
- Reduced costs and liability and enhanced compliance with legal obligations for records retention, privacy, data security, and eDiscovery, as information policies and processes are rationalized, integrated, and aligned in accord with the organization's Information Governance strategy

D. Senior Leadership Support is Essential

The commitment of senior leadership is crucial for organizations to be successful in adopting Information Governance. Such ongoing commitment is particularly important given the

challenge of effectively bridging across existing organizational silos and competing priorities.

Thus, senior leadership should sponsor and firmly support the organization's Information Governance efforts through the following:

- Endorsing and communicating the importance of Information Governance to the entire organization
- Chartering a structure of responsibility and accountability for implementing an Information Governance program
- Adopting or approving the strategic objectives of the Information Governance program
- Providing appropriate resources to implement and sustain the Information Governance program
- Establishing a supportive "tone at the top" and an environment in which Information Governance remains an organizational priority
- Removing barriers and resolving issues that may interfere with the strategic objectives of the Information Governance program
- Ensuring that the Information Governance program is administered in a manner consistent with its objectives and is periodically reviewed and updated

There is often a balance of value against cost or risk that changes over time for a given information asset. Organizations may leverage information effectively over the short term, but once the data's short-term use is expended, the data is often stored away and rarely reassessed for any long-term strategic value. Left ungoverned, this potentially valuable asset is not only wasted but also may become a significant liability.

Through proper Information Governance, organizations can realize additional benefit from their information assets over time while reducing risk and costs.

E. The Business Case for Information Governance

Multiple business cases can be established for pursuing Information Governance. Successful adoption of the Information Governance approach requires both strategic commitment (adoption as an organizational priority) and tactical efforts (such as specific projects to establish and implement the program). A business case will be needed, both to support the strategic commitment and to justify the expenditures of time, effort, and funding required for specific implementation projects. Because the business case for Information Governance must be persuasive at both strategic and tactical levels, the business case should include both strategic (qualitative) and project-based (quantitative, return on investment (ROI)) elements.

1. The Strategic/Qualitative Business Case

Information Governance is an ongoing program that evolves over time through maturity levels. As such, it is unrealistic to attempt to comprehensively quantify all benefits. One might just as easily attempt to exhaustively measure all benefits of managing the organization's tangible or people assets. ROI analysis is best used for applications of Information Governance to specific issues or projects within the Information Governance initiative, as discussed in Appendix D.

At a strategic level, the business case should instead convey how Information Governance aligns with and amplifies the core values and fundamental, strategic objectives of the organization:

- Low-Cost Provider

Organizations singularly focused on operational efficiency and cost control, such as in low-margin, high-volume industries or market segments, may adopt Information Governance to streamline information workflows and reduce unnecessary information storage and retention, thereby reducing costs and increasing business efficiency.

- Innovative Excellence

Organizations driven by creative innovation and excellence in products and services may adopt Information Governance to maximize the value of their information assets, helping them capture valuable information for innovative repurpose while minimizing the distraction of unnecessary information.

- Trusted Provider/Advisor

Organizations with the core value and brand of being a trusted business provider or advisor may adopt Information Governance to strengthen their protection of information that customers or clients entrust to the organization and to enhance third-party perceptions of the organization as a trusted custodian for such information.

- Integrity/Ethics

Organizations, including publicly traded companies and those in highly regulated industries, may adopt Information Governance as a complement to their internal control systems, ethics, and integrity programs to ensure information-related legal compliance and risk management.

- Data Privacy and Information Security Benefits

Organizations need to be concerned about ensuring the security of its information and the privacy of employee and customer data. Information Governance will provide a framework

for organizations to ensure the necessary controls are in place to protect and secure its information and reduce the amount of unnecessary information by following consistent defensible disposition practices.

- Improved Records Management

Information Governance improves an organization's records management in accordance with Generally Accepted Recordkeeping Practices and facilitates the management of information throughout its lifecycle with an emphasis on use, accessibility, and disposition.

In each of the above examples, Information Governance provides specific, tangible benefits that often can be quantified on an ROI basis as discussed below. Yet, in each example, Information Governance also amplifies the organization's core value of choice, by ensuring that information is handled in alignment with the strategic value or brand. This alignment allows Information Governance to reinforce the organization's fundamental values because information is managed in a way that fits an organization's culture.

Conversely, Information Governance also helps organizations avoid cultural dissonance for their core values, such as the "low-cost provider" that squanders money on information inefficiency and unnecessary retention; the "innovative excellence" organization that fails to optimize the value of its information; the "trusted partner/provider" that is careless with the information entrusted to it; or the organization espousing "integrity and ethics" that fails to adopt measures that treat its information as a valuable asset and that detect and prevent compliance lapses. Thus, adoption of Information Governance can have profound, strategic significance beyond the quantitative ROI measures mentioned below and considered in more detail in Appendix D.

2. The Quantitative/ROI Business Case

A typical ROI analysis weighs the benefits of a project against its cost and calculates the length of time it will take to recoup such cost. The quantitative aspects of the business case are best determined by focusing on specific applications of Information Governance to identified problems or opportunities or to distinct projects for implementation of the Information Governance program.[11]

The quantifiable benefits from pursuing Information Governance generally fall into four main categories: optimizing organization value, risk reduction, hard-cost avoidance, and soft-cost avoidance. See Appendix D for factors to consider when building a quantitative business case with these ROI categories.

11. *See generally* SUNIL SOARES, SELLING INFORMATION GOVERNANCE TO THE BUSINESS: BEST PRACTICES BY INDUSTRY AND JOB FUNCTION (MC Press 2011) (providing insight into the best ways to encourage businesses to implement an Information Governance program).

III. THE SEDONA CONFERENCE PRINCIPLES OF INFORMATION GOVERNANCE AND ASSOCIATED COMMENTARIES

Principle 1: Organizations should consider implementing an Information Governance program to make coordinated, proactive decisions about information for the benefit of the overall organization that address information-related requirements and manage risks while optimizing value.

Organizations benefit in several ways from managing information as a valuable asset. To realize these benefits, it is important that an effective Information Governance program be established in a manner consistent with the organization's industry, compliance, and risk environments.

Any Information Governance program should incorporate the following principles: transparency, efficiency, integrity, compliance, and accountability. To be successful, the Information Governance program must be sponsored and firmly supported by the organization's senior leadership. Clear and open communication among stakeholders with divergent interests is necessary, as is their willingness to put the good of the organization before the needs of their individual business group.

A core component of any Information Governance program should include a comprehensive data classification capability, combined with the effective and timely deletion of appropriate information. By taking a comprehensive approach to identifying and addressing information-related requirements, organizations can ensure compliance needs are met and conflicting issues are considered. It is also helpful to identify and assess information risks, such as user access control (information security) and system failure (business continuity and disaster recovery), and to ensure that such risks are understood so that

effective information controls are put in place. This approach also aids in understanding information-related strategic and operational objectives to help ensure that information value can be optimized without compliance lapses or uncontrolled risk.

To enable an organization to make decisions about information for the benefit of the organization, the primary responsibility of an Information Governance program should be to create and maintain processes and procedures necessary for a coordinated, overall approach. If agreement cannot be reached among stakeholders, the Information Governance program should provide a method for decisions to be made (subject to a challenge process) to enable the organization to move forward.

Responsible decision-makers should use the Information Governance program any time they make decisions about information. Care should be taken to design the Information Governance program so that it can be used regarding existing information and information that will be created. At the time decisions regarding information are being made, existing governance mechanisms (such as budgetary governance or systems approval) may not be designed for the current need of its users. However, these can be leveraged or modified, or new ones may be created, depending on an organization's circumstances.

Principle 2: An Information Governance program should maintain sufficient independence from any particular department or division to ensure that decisions are made for the benefit of the overall organization.

The Information Governance function must focus on the best interests of the organization. To fairly and effectively balance needs, however, the Information Governance program should have meaningful and balanced input from such departments as IT, Legal, Compliance, RIM, and the business units. One approach to accomplish this is to designate an executive, such as a

Chief Information Governance Officer, who has sufficient independence to balance the competing needs of stakeholders rather than the interests of a single department. Ideally, the executive in charge of the Information Governance program reports at the same level as a General Counsel (GC), Chief Compliance Officer (CCO), Chief Financial Officer (CFO), or Chief Information Officer (CIO). Another way to make decisions for the benefit of the overall organization is through a committee that has representation from impacted stakeholders, coupled with a process for elevating disagreements to a chief executive. Such a structure should be the ultimate goal for organizations with mature Information Governance programs. However, many organizations do not currently have in place any overarching Information Governance structure, and their initial steps may include assigning Information Governance responsibilities to designated individuals within departments or lines of business. As this is not the optimal governance structure to reap the benefits of a coordinated approach to Information Governance, organizations should strive for a structure that results in meaningful and balanced input from all impacted departments or divisions as their Information Governance programs mature.[12]

Many organizations have various departments (e.g., business units, IT, Legal, etc.) that take direction from a Chief Executive Officer (CEO) or Chief Operating Officer (COO). Because goals differ across departments or functions, conflicts of interest may arise if the executive responsible for the Information Governance program reports to an individual stakeholder department.

An Information Governance program should ensure that decisions about information are made in the organization's best

12. *See* Appendix B, *infra,* for a discussion of the Information Governance maturity continuum.

interests. This involves balancing the sometimes-competing interests of many stakeholders. This balancing creates the potential that a given decision may not align with the objectives of a given department, particularly when the decision involves a balancing of cost and risk. For example, the IT Department may believe a cloud-hosted service will reduce the cost of storing information, but the Legal Department may perceive an increased risk associated with the data being hosted in the cloud. In many cases, stakeholders can arrive at a mutually agreeable position that maximizes the benefit to the overall organization, such as by implementing mitigation steps that decrease the risk to one department without substantially increasing the cost to other departments.

Though it is appropriate for departments to operate autonomously in carrying out their primary function, decisions about Information Governance should be coordinated across all departments and stakeholders, as they impact the organization as a whole. Because such decisions require an overall balancing between the needs and interests of different stakeholders, it is important for the Information Governance function to be independent within the organization.[13]

Principle 3: All stakeholders' views/needs should be represented in an organization's Information Governance program.

Information Governance programs should seek to be inclusive and to consider the requirements of all parts of an organization (business units, departments, etc.) that have an interest in the storage, retention, and management of an organization's information.[14] This may require involvement from all the

13. For further explanation, *see* Appendix B, *infra*.

14. *Cf.* The Sedona Conference, *Commentary on Finding the Hidden ROI in Information Assets*, 13 SEDONA CONF. J. 267 (2012).

organization's departments or business units, requiring different levels of participation from stakeholders.

An inclusive process will ensure that decisions about the management of information represent all viewpoints by identifying and resolving potential conflicts early and prior to any action being taken that could have an adverse impact to the organization. For example, a litigation hold formulated by outside counsel might be revealed as overly broad or costly when presented by the GC in an Information Governance discussion that includes line-of-business stakeholders, the CIO, and other key Information Governance participants.

However, all stakeholders' participation does not require a "seat at the table" for every person, or even every department, with an interest in the organization's information. In larger organizations, active participation from every group could create an unwieldy team unable to reach decisions. A more effective approach would be to design an appropriate structure or methodology to ensure that all stakeholder interests are represented. An organization could create a process to identify groups with common interests, appoint certain committee members as proxies for other groups, request requirements documentation from every stakeholder, or design surveys or feedback sessions to ensure that all interests are adequately identified and represented.

In most organizations, stakeholders from the core disciplines of RIM, data privacy, information security, data governance, and eDiscovery should be represented in the Information Governance program. These disciplines will involve IT, Legal, Compliance, Risk, Audit, and RIM functions. Representatives of lines of business and core operational functions should also be consulted to ensure that the practical needs of the organization are properly considered. It is important to include active participation from core operational functions that have unique Information Governance issues. For example, HR, highly regulated

departments, and environmental functions typically have legally mandated retention for some of their information.

Principle 4: The strategic objectives of an organization's Information Governance program should be based upon a comprehensive assessment of information-related practices, requirements, risks, and opportunities.

An effective Information Governance program should be designed, implemented, and monitored based upon organization-wide objectives established from a comprehensive assessment of the interests and concerns of key stakeholders within the organization, such as IT, Legal, Compliance, RIM, and various business units. The program objectives should address and coordinate the stakeholders' existing practices and approaches to issues such as RIM, privacy, data security, and preservation; and must reconcile these practices and approaches with applicable legal requirements and business needs. The key responsibility of a cross-organizational Information Governance forum is to provide the mechanisms that allow decisions about information to include the viewpoints of all stakeholders, in order to recognize conflicts of any significant decision involving the organization's information assets. Another major responsibility of the Information Governance program is understanding stakeholder requirements and priorities. Although the Information Governance program is not ultimately responsible for execution of requirements, it owns responsibility for gathering stakeholder needs and priorities, tracking and identifying issues or conflicts resulting from decisions (including escalation, if required), and considering them to establish requirements that serve the good of the organization overall.

To determine its information-related practices, requirements, risks, and opportunities, an organization should first identify the various types of information in its possession,

custody, or control; assess whether it owns the information or possesses it on behalf of third parties; and determine whether the information is held by the organization, third parties on behalf of the organization, or both. The organization should next identify its current information lifecycle practices, including practices pertaining to the following:

- Creation and/or receipt of information
- Determination of the location and media for storing information, including in both active and inactive environments
- Disaster recovery and business continuity
- Security for private, protected, or confidential information, such as electronic protected health information ("ePHI"), protected health information ("PHI"), personally identifiable information ("PII"), payment card industry information ("PCI"), social security numbers, and sensitive identifiable human-subject research and export-controlled research
- Retention of information in both active and inactive environments
- Disposal/destruction of information, as well as exceptions from the normal data lifecycle (e.g., implementation, maintenance, and release of legal holds due to litigation or government proceedings)

A review of existing written policies, procedures, retention schedules, data maps, and contractual arrangements is helpful in identifying and understanding these information-related practices. However, input from the organization's stakeholders, including IT, Legal, Compliance, RIM, and business units, among others, is also essential to gaining an accurate and complete understanding of both the strengths of current

Information Governance practices and areas where improvement may be necessary.

Organizations can then assess their identified information types and related practices in light of information opportunities, risks, and compliance requirements, including the following:

1. Opportunities
    - Reducing costs and risks of complying with eDiscovery obligations by decreasing the volume of unnecessary information, understanding where information is stored, and considering eDiscovery costs and risks when approving locations or formats for creating or storing information
    - Monetizing the value of an organization's data
    - Reducing the risk of data breach or leakage by adopting sound, effective information security and storage measures
    - Using information to support evidence-based decision-making
    - Optimizing storage and accessibility of information to enhance productivity and efficiency
    - Realizing cost savings by decreasing the volume of unnecessary information, and rationalizing storage options to better meet demands while reducing cost
    - Enabling access to information for new and valuable combinations and uses
    - Enhancing the organization's reputation as a trusted custodian of PHI, PII, and other classes of protected information
    - Achieving cost savings and reducing risk through early stakeholder involvement and

proactive decision-making regarding storage, retention, and organization of business data

2. Risks

- Loss of records or other valuable information
- Loss of integrity, authenticity, and reliability of records or other valuable information
- Unavailability of information vital to the organization's continued operation
- Accumulation of information (both by the organization and third parties) not (i.e., never or no longer) required for legal compliance or business needs
- Creation or storage of information in locations or formats that increase the legal risk or business cost, without a corresponding business benefit to outweigh the increased risk and cost
- Creation of internal RIM requirements that are not followed
- Breach of ePHI, PHI, PII, PCI, social security numbers, sensitive identifiable human-subject research and export-controlled research, or other classes of protected information
- Harm to information from malicious access or attack
- Inability or failure to detect and respond effectively to data breaches
- Loss of intellectual property protection
- Loss of privilege or confidentiality of information
- Loss of information resulting from organization mergers and acquisitions (when companies are combined, it is common for the staff with the most knowledge of one organization's

data to leave, essentially leaving the combined organization with no way to know what the universe of data is, and where it is stored)
- Failure to preserve information subject to regulatory requirements or relevant to litigation, government proceedings, or internal investigations
- Over-preservation of information subject to regulatory requirements or relevant to litigation, government proceedings, or internal investigations
- Failure to release information back into its normal lifecycle once circumstances requiring an exception (e.g., legal hold) have expired

3. Compliance Requirements

    - Legal and contractual requirements may exist for the following:
        - Records creation, retention, management, and disposition
        - Privacy and security for ePHI, PHI, PII, and other classes of protected, private, and confidential information
        - Protection of intellectual property and confidential information
        - Preserving information relevant to litigation, government proceedings, and regulatory requirements

These considerations will differ among jurisdictions, industry sectors, and organizations, and there will be a range of risk tolerances and cultures regarding these matters. Industry

standards, maturity models, and benchmarking data for comparable organizations are useful considerations for this assessment.[15]

An organization should use the results of the above assessment to determine its objectives for Information Governance. Well-framed strategic objectives can guide the design and implementation of the organization's Information Governance program, helping to clarify what elements of structure, direction, resources, and accountability will be pursued, as discussed under Principle 5. Establishing strategic objectives in this

15. Useful standards and models include the following:

- International Organization for Standardization (ISO), Information and Documentation—Management Systems for Records—Fundamentals and Vocabulary (ISO 30300:2011).
- ISO, Information and Documentation—Records Management—Parts 1 and 2 (ISO 15489-1:2016; ISO 15489-2:2001).
- ISO, Information Technology—Security Techniques (ISO/IEC 27000:2018; ISO/IEC 27010:2015; ISO/IEC TR 27019:2017).
- ARMA Int'l, *Generally Accepted Recordkeeping Principles®*, https://cdn.ymaws.com/www.arma.org/resource/resmgr/files/Learn/2017_Generally_Accepted_Reco.pdf (updated 2017).
- ISACA, *A Business Framework for the Governance and Management of Enterprise IT*, http://www.isaca.org/COBIT/Pages/COBIT-5.aspx (last visited Feb. 4, 2019).
- *The Sedona Principles, Third Edition*, supra note 6.
- ARMA Int'l., *Information Governance Maturity Model*, https://www.arma.org/page/IGMaturityModel (last visited Feb. 4, 2019).

manner should clarify decision-making on priorities and funding of the effort. Strategic objectives should be measurable to better ensure that progress toward them can be observed and reported. Such measures may be quantitative (e.g., data volumes or run rates) or qualitative (e.g., assessment or audit against program standards or upon completion of transactions or litigation matters). Measurability of objectives is essential for accountability, as discussed under Principle 5. Perhaps the most important feature of this exercise is that it compels organizations to look beyond the confines of traditional silos within organizations.[16]

---

16. For example, in its Information Governance assessment, a financial services organization confirms that it has customer information subject to privacy and data security requirements, which it regularly transfers to the custody of various service providers in the ordinary operation of its business. From the siloed perspective of privacy and data security compliance, the organization satisfies the applicable requirements of the Federal Trade Commission's Safeguards Rule (Standards for Safeguarding Customer Information, 16 C.F.R. § 314 (2002)) by, among other things, establishing internal controls for selecting and retaining service providers and contractually requiring them to establish safeguards to ensure security for protected customer information. The organization also periodically audits its service providers to assess the effectiveness of their information security safeguards.

However, through its Information Governance assessment, the organization determines that its internal requirements for records retention periods are not followed by its service providers, such that some providers retain customer information for a shorter or longer period of time than the organization's records retention schedule requires. The organization also determines that its legal hold process may not include certain customer information relevant to litigation that is in the custody of various service providers, yet arguably within the "control" of the organization for discovery purposes.

As a result of the assessment, the organization decides that one of its strategic objectives will be to apply Information Governance controls to customer information possessed by its service providers. This will allow the organization to ensure that service providers implement appropriate

Principle 5: An Information Governance program should be established with the structure, direction, resources, and accountability to provide reasonable assurance that the program's objectives will be achieved.

Structure, direction, resources, and accountability are critical components in ensuring an Information Governance program meets an organization's strategic objectives. Depending on the size of the organization, other tactics may also be important, such as a change management and communication to raise awareness of the Information Governance function, user training, creating the Information Governance matrix, and gathering metrics required for management control and monitoring.

1. Structure

One means of ensuring that an organization's various information needs are comprehensively addressed is to establish a unified framework in which the organization's various information types can be categorized according to business needs, information-related compliance requirements, and risk controls. Such a framework should categorize information types by content and context.[17] This will normally require input from a wide

safeguards to protect customer information, comply with the organization's records retention schedule, and be responsive to legal holds that may be imposed upon customer information in their possession.

17. Information context is significant, because different copies or instances of the same information content may be used for different purposes, thereby triggering different compliance requirements and risks. For example, a single contract may simultaneously exist in multiple instances for different purposes, including the original executed hard-copy version; the scanned, digitized version that the organization declares as the official record of the contract; disaster recovery backup copies of the digitized contract; reference copies of the contract used for business convenience in various departments; and a preserved version of the contract under legal hold due to pending

range of subject matter experts, including, for example, Business Operations, HR, Accounting, Compliance, and Environmental.

Attached to this framework of information types are the applicable rules the organization applies to the respective information. These rules reflect legal and regulatory requirements for records retention, information management, and information security and protection. The rules reflect the organization's operational needs for how information will be retained, managed, and protected, and the organization's risk controls. The unified framework allows the organization to identify, understand, and follow the appropriate rules for its information types.

In place of functionally segmented (or "siloed") structures governing data security, retention, and preservation, an organization could establish an Information Governance matrix. This matrix is a classification structure for the organization's information types similar to a traditional records retention schedule or data security grid but that integrates all established rules governing the organization's information types. It is thus a repository of integrated rules for information from the organization's perspective as a whole, rather than merely one or more of its siloed functions. The matrix should be designed to meet the needs of various audiences and multiple uses within the organization. It is essential, for all of the organization's business information, that the organization establish and clearly communicate specific roles and responsibilities for complying with the integrated rules included in this governance matrix. Otherwise, "orphan data" can greatly increase the cost and risk of eDiscovery.

---

litigation. In each of these contexts, different compliance requirements and risks apply to the same information.

An organization should establish or adopt a common vocabulary for its various information types.[18] A common vocabulary helps ensure information is properly classified, so that the applicable rules for such information types can be identified and followed.

2. Direction

An organization should communicate to all information users (internal as well as external custodians, such as suppliers and contractors) their requirements for Information Governance. Vehicles commonly used by organizations to provide such direction include policies, contracts, retention schedules, Information Governance matrices, procedures and protocols, and guidance and training (including certification and testing for comprehension).

---

18. Whether an organization relies upon traditional structures, such as records retention schedules and data security grids, or integrates them into an Information Governance matrix, such structures are commonly organized as taxonomies. A taxonomy is a defined classification scheme or in many cases a hierarchy with classes and sub-classes forming "trees" of classification. In a taxonomy, it is only possible to move downward into sub-classes or upward into super classes that subsume all of the classes below. Taxonomies are flat and linear and therefore limiting. In contrast, ontologies link classes in a non-hierarchical way, forming associations that are non-linear. Ontologies are a representation of relationships between concepts. Thus, the widget purchase order may be associated hierarchically with accounting recordkeeping, but at the same time, it may also be associated with documentation of contract rights and duties and other business functions. Instances of the widget purchase order information may also, simultaneously, be associated with disaster recovery restoration, information protection issues (due to where versions of the purchase order are located physically or virtually), and applicable legal holds. The complexity of the digital environment, in which the same information content simultaneously exists in different locations and contexts and triggers different Information Governance rules, makes ontology a promising perspective for applying Information Governance to an organization's information.

The current state of Information Governance in many organizations involves an array of policies that directly or indirectly address Information Governance topics. Examples include a RIM policy, a communications policy, a computer use policy, an Internet and social media policy, a BYOD policy, an information security policy, and a legal hold policy. In many organizations, such information-related policies accumulate over time, each designed to meet the needs of distinct stakeholders and silos of the organization. They commonly address only a subset of Information Governance requirements and may be in conflict with each other. Organizations should identify all such existing policies, review them for inconsistencies and gaps in coverage, and reconcile them or integrate the majority of these policies into a cohesive, actionable Information Governance policy. Similar to the Information Governance matrix, an Information Governance policy expresses in one place all of the organization's policy-level expectations for governance of information across the entire spectrum of possession, custody, and control, regardless of location, custodial, or organization boundaries. Then, specific sub-level policies can be established under the unified approval identified by the policy.

Further to this point, contracts with third parties are an important aspect of defining responsibility for Information Governance. Organizations commonly allow information to be transferred to or held by third parties, such as service providers for business operations; management, legal, accounting, and technology consultants; data hosting providers; and hard-copy records storage providers. The organization's expectations for Information Governance, and its standards of accountability for managing information resources, should be incorporated into such third-party contracts.[19] For example, engagement letters

19. In some regulated sectors, contractual control of information protection by such service providers is an explicit legal requirement. For example,

and billing guidelines with law firms should confirm the firm's obligations to protect and preserve information, confirm the organization's rights to conduct periodic compliance audits and review, and require the firm's destruction or return of information after the matter or engagement is concluded.

Organizations should also have specific procedures and protocols that provide explicit direction on information creation, receipt, use, dissemination (including redundancy), protection, retention, preservation, and ultimate disposition. Organizations should also establish effective guidance and training regarding Information Governance, delivered in a way that confirms both awareness and understanding of policy rules, thereby empowering individuals to make timely, compliant decisions regarding information.[20] Accordingly, training and guidance resources should be tailored to meet the specific needs of recipients and should provide the concrete direction the recipients need in order to make information-related decisions consistent with the organization's Information Governance expectations.

3. Resources

Organizations should provide the people, technology, and implementation resources needed to support their Information Governance program and accomplish the organization's strategic objectives.

People resources include staffing of the management and administrative roles supporting the Information Governance program itself, as discussed above under Principle 3. Staffing

---

HIPAA-covered entities must contractually require their business associates to provide compliant security for ePHI created, received, maintained, or transmitted on behalf of the covered entity. 45 C.F.R. § 164.314(a) (2013).

20. Day v. LSI Corp., No. CIV 11–186–TUC–CKJ, 2012 WL 6674434 (D. Ariz. Dec. 20, 2012) (awarding sanctions against defendant for, among other things, defendant's failure to follow its own document retention policy).

should be commensurate with the program's scope and objectives, and roles and responsibilities should be defined. Key points of contact should be identified within the organization, and those in such roles should be accessible and responsive. People resources reflect the focus and engagement of stakeholder representatives, such as those from Legal, IT, Compliance, RIM, other administrative functions, and lines of business. People resources must recognize that Information Governance is part of everyone's job responsibilities within the organization.

Technology resources include systems and applications used for creating, using, and storing information, and into which should be placed methods and controls necessary for prudent Information Governance. Technology resources also include systems and applications for managing, tracking, and reporting regarding the Information Governance program itself. Both kinds of technology should be designed and implemented to address the program's scope and objectives. Information Governance technology resources should be procured only after requirements for such tools have been defined in a manner consistent with the organization's strategic objectives. Organizations should carefully match the capabilities of the contemplated technology against the program's desired objectives and should document decisions regarding any gaps.

Although the full scope of technology implementation risks and requirements is beyond the focus of this commentary, organizations must recognize that implementation resources are also needed. These include project management tools and processes to be used as elements of the organization's Information Governance program.

4. Accountability

The effectiveness of an Information Governance program will turn upon whether the organization establishes

accountability for meeting program expectations and achieving the organization's strategic objectives. In internal control systems, this atmosphere of accountability is the "control environment."[21] The organization's senior leadership establishes the tone at the top regarding strategic objectives, the importance of reaching these objectives, expected standards of conduct, and accountability. In all forms of direction, the visible commitment and support of the organization's senior leadership is crucial.[22]

Management reinforces these expectations, and the related roles, responsibilities, and accountability, across the organization. The Information Governance program should clarify roles and responsibilities for information users, their management, and those managing the Information Governance program.

Information Governance program objectives should be linked to observable and measurable outcomes. Compliance audits or comparable assessments of the program should be

21. The internal control concept of a control environment is a model that organizations may consider in pursuing Information Governance, particularly for establishing accountability and managing risks around specific objectives. *See* Committee of Sponsoring Organizations of the Treadway Commission (COSO), *Internal Control—Integrated Framework Executive Summary*, 3 (May 2013), https://na.theiia.org/standards-guidance/topics/Documents/Executive_Summary.pdf ("Internal control is a process effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.").

22. In some aspects of Information Governance, senior leadership involvement is legally required. For example, entities subject to the Federal Trade Commission's (FTC) Red Flags Rule must obtain board-level approval of the initial Identity Theft Program and must involve the board or senior management in the oversight, development, implementation, and administration of the Program. 16 C.F.R. § 681.1(e)(1) & (2). ISO 30300 provides that "[t]op management is responsible for setting an organization's direction and communicating priorities to employees and stakeholders." ISO 30300:2011, *supra* note 15.

conducted on both a random and periodic basis, followed by appropriate corrective actions as needed. The program's measured outcomes should be periodically compared to target objectives, and such outcomes should be tracked by those responsible for the Information Governance program.

The results of such outcome measures and program assessments should be reported periodically to the organization's senior leadership and stakeholders to provide reasonable assurance that the program's objectives are being or will be satisfied.

Principle 6: The effective, timely, and consistent disposal of physical and electronic information that no longer needs to be retained should be a core component of any Information Governance program.

It is a sound strategic objective of an organization to dispose[23] of information that no longer provides value to the organization, if that information is not required for statutory or regulatory compliance or legal hold purposes.[24] Despite this advice, many organizations struggle with making and executing

23. In this commentary, the "disposal of information" concept will be used narrowly to refer to the final destruction or deletion of information that no longer has any regulatory, statutory, compliance, legal, or operational value and is not subject to any retention or preservation requirement. The effective disposal of data should purge all copies of that information from relevant systems so that they are no longer retrievable.

24. Managed Care Solutions, Inc. v. Essent Healthcare, Inc., 736 F. Supp. 2d 1317, 1326 (S.D. Fla. Aug. 23, 2010) (rejecting the argument "that there is no reasonable business routine demanding that data be destroyed after [13 months], especially in light of developments in the technology field (including the ability to inexpensively maintain documents at an off-site server); and industry standards stating the exact contrary" (citing Matya v. Dexter Corp., No. 97-cv-763C, 2006 WL 931870, at *11 (W.D.N.Y. Apr. 11, 2006) and Floeter v. City of Orlando, No. 6:05-CV-400-Orl-22KRS, 2007 WL 486633, at * 7 (M.D. Fla. Feb. 9, 2007)).

effective disposition decisions. That struggle is caused by many factors, which include the following: (i) the incorrect belief that organizations will be forced to defend their disposition actions if they later become involved in litigation; (ii) the difficulty in appreciating how such disposition reduces costs and risks; (iii) the difficulty in determining how to design and implement effective disposition as part of their overall Information Governance program; (iv) the technical challenges in applying active management to environments not originally designed for them; and (v) the difficulty in segregating/parsing records from non-records. The Sedona Conference recognized the need for more scholarship on this topic and released a publication in August 2018, *Principles and Commentary on Defensible Disposition*, to provide guidance to organizations, and the professionals who counsel those organizations, on developing and implementing an effective information disposition program.[25]

If there is no statutory, regulatory, or preservation obligation, information should be disposed of as soon as the likely business value of retaining the information is outweighed by the cost and risk of retaining the information. This may require a culture shift in some organizations that have developed a "keep it just in case" mentality. Typically, the business value decreases, and the cost and risk increase as information ages. Timely disposal of information in a consistent and effective manner provides many benefits, including reduced storage and labor costs,[26] reduced costs and risks of complying with

25. *See* The Sedona Conference, *Principles and Commentary on Defensible Disposition*, THE SEDONA CONFERENCE (Aug. 2018 Public Comment Version), https://thesedonaconference.org/publication/Commentary_on_Defensible_Disposition.

26. Though some may view data storage as a low-cost concern, the maintenance, retention, and discovery-based review of unnecessary information is far from cheap. In the aggregate, storage is quite expensive. *See, e.g.*, Jake

discovery obligations, and an increased ability to retrieve important organizational information. Organizations should therefore consider procedures to achieve the regular destruction of unnecessary information.[27]

Organizations should also consider whether information considered private or confidential to third parties should be disposed of within a reasonable amount of time after it ceases to be useful to the organization to minimize the risk of disclosure. Separately, organizations that operate in jurisdictions where individuals' privacy rights are protected by law may need to develop robust "mandatory destruction" capabilities. For example, the European Union's General Data Privacy Directive requires that the information relating to a person who seeks to be "forgotten" by a holder of his/her personal information must be demonstrably and promptly removed, on demand.[28]

While most organizations are familiar with managing paper records (and most retention schedules were drafted with paper in mind), it is important that the organization's retention schedules account for both hard-copy and electronic records. For example, record owners may find it difficult to apply the concepts of original documents versus copies of documents to digital information.

The term "hold" is used broadly in this commentary to cover preservation obligations that are independent from routine recordkeeping requirements, such as reasonably anticipated or

---

Frazier & Anthony Diana, *'Hoarders': The Corporate Data Edition*, LEGALTECH NEWS (Dec. 19, 2012, 12:02 a.m.), https://www.law.com/legaltechnews/almID/1202581938140.

27. ARMA Int'l, *Generally Accepted Recordkeeping Principles®*, Principle of Disposition, *supra* note 15 ("An organization shall provide secure and appropriate disposition for information assets no longer required to be maintained, in compliance with applicable laws and the organization's policies.").

28. GDPR, *supra* note 2.

active litigation, governmental inquiries, outside audits, or contractual requirements. A hold may take various forms:

- A legal or litigation hold, i.e., the preservation of data for purposes of reasonably anticipated or active litigation, regulatory inquiries, or investigations
- A tax hold, i.e., the preservation of information in ongoing audit or review of records related to tax obligations, such as financial and accounting records
- A contractual hold, which is an agreed-upon obligation that an organization has with its customers, vendors, divested entities, or other third parties that requires the preservation or disposition of information and exists separately from the organization's standard retention schedule[29]

1. Records Retention

To create a proper data disposal process, an organization should consider all applicable legal, regulatory, and contractual requirements in conjunction with the business value of the organization's information. The organization might begin this process by evaluating its legal/regulatory requirements at all levels and across all jurisdictions relevant to its business (state, federal, and/or international) and clustering those records into

29. An organization should be wary of this type of obligation, as it could create onerous obligations to dispose of copies of electronic data that may not be within the control of the organization, as well as inconsistent obligations where different contracts prescribe different retention periods.

categories.[30] This exercise will enable the organization to more easily identify the appropriate retention period applicable to each category of records while also facilitating the analysis of certain key factors relevant to the retention determination, including the cost vs. risk associated with a category of records.[31]

Legal, regulatory, and compliance objectives are of paramount concern. It is equally important, however, that operational value (e.g., maintenance of historical records, research and development processes, and other business-driven objectives) be considered as the organization formulates its retention protocols and schedule. Otherwise, the organization may squander valuable opportunities to reduce cost while minimizing risk. For example, organizations should strive to avoid retaining information simply because it may be useful at some point in the future and instead undertake a cost-benefit and a risk-benefit analysis with respect to each category of data it maintains, thereby ensuring that the advantages of retaining a given set of information outweigh the potential costs and risks associated with disposing of that information.

2. Hold/Preservation Analysis

Before an organization disposes of any information, it should determine whether there are any legal, regulatory, or other obligations in place that require the organization to retain the information, regardless of its business value. To effectively identify its preservation obligations, it is advisable for the organization to develop and consistently implement protocols

30. For some organizations, local, municipal, and/or regional recordkeeping regulations may apply and, if so, should also be considered when developing an appropriate records retention schedule.

31. For more information, *see* ARMA Int'l, *Standards and Best Practices*, https://www.arma.org/page/Standards; and ARMA Int'l, *Generally Accepted Recordkeeping Principles*®, Principle of Disposition, *supra* note 15.

designed to track legal holds and map them to the relevant sources of information or take other steps to label, segregate, and preserve the information. A key aspect of this exercise is to communicate those protocols to the relevant individuals within the organization and provide a point of contact (typically, a member of the Legal or Compliance Department) who will address any questions regarding hold procedures and best practices.[32] This exercise should be repeated whenever the organization decides to create, store, and use information from any new source, such as websites, social media, and portable devices.

It is important for the relevant constituencies within the organization—not just the Legal or Compliance Department—to understand that a legal hold supersedes all other RIM policies and retention schedules, and that a hold requires the immediate suspension of the disposal process for all affected information during the time mandated by the hold. Thus, it is critical for the organization to incorporate a "hold and release" capability into its records disposition process, so that once the hold is released, the affected information can be placed back into the appropriate retention schedule.

3. Disposition

Once an organization verifies that no legal, regulatory, or operational requirements apply to the information, disposition decisions can be made. In some circumstances, an organization may be able to determine from readily available information whether a record retention or legal preservation requirement applies. In other circumstances, a more detailed investigation and analysis may be required. The analytical approach to such

32. For further information on legal holds, *see* The Sedona Conference, *Commentary on Legal Holds, Second Edition: The Trigger & The Process*, 20 SEDONA CONF. J. 341 (2019), *available at* https://thesedonaconference.org/publication/Commentary_on_Legal_Holds.

situations is beyond the scope of this commentary and is discussed more fully in The Sedona Conference *Principles and Commentary on Defensible Disposition*.[33] In addition, organizations considering disposition of inactive information sources should consult The Sedona Conference *Commentary on Inactive Information Sources*.[34]

Principle 7: When Information Governance decisions require an organization to reconcile conflicting laws or obligations, the organization should act in good faith and give due respect to considerations such as data privacy, data protection, data security, records and information management (RIM), risk management, and sound business practices.

Organizations often confront conflicting laws or obligations that apply to the same information, particularly when the organization conducts business across numerous jurisdictions.[35] A

---

33. *See* The Sedona Conference, *Principles and Commentary on Defensible Disposition*, 20 SEDONA CONF. J. 179 (2019).

34. *See* The Sedona Conference, *Commentary on Inactive Information Sources*, THE SEDONA CONFERENCE (July 2009 Public Comment Version), https://thesedonaconference.org/publication/Commentary_on_Inactive_Information_Sources.

35. Devon Robotics v. DeViedma, Civil Action No. 09-cv-3552, 2010 WL 3985877 (E.D. Pa. Oct. 8, 2010). The plaintiff in a breach of fiduciary duty and tortious interference case requested all ESI relating to the former employee defendant, his Italian employer (a rival), and the alleged breach of contract between the plaintiff and the defendant's new employer. The defendant moved for a protective order regarding the production of "documents owned by his employer," arguing that the disclosure was prohibited by the Italian Personal Data Protection Code. The court found that the defendant did not show good cause for a protective order and denied the motion, writing that the defendant made nothing but "a blanket assertion that any

common example involves the tension between data protection laws in the European Union that prohibit transferring "personal information" and U.S. federal court jurisprudence that mandates the production of such information during the discovery process.[36] In other circumstances, one jurisdiction may require an organization to preserve certain information for a specified period of time, while another jurisdiction may require such information be destroyed upon the owner's request.

When faced with Information Governance decisions triggered by such conflicts, the organization's key objective should be good-faith compliance with all laws and obligations. Due deference should be afforded to conflicting laws or obligations, particularly when the conflict arises out of interests that span different jurisdictions.[37] Further, the most significant legal/regulatory and business considerations should be prioritized. Not all conflicts are capable of complete resolution, and the organization will ultimately need to balance the competing needs, demands, and viewpoints of the stakeholders involved. To the extent compliance with all laws and obligations is not possible or practical, the organization should thoroughly document its

---

disclosure could violate Italian law." The court also stressed the importance of the requested ESI to the plaintiff's claims and that the comity factors outlined in *Société Nationale Industrielle Aérospatiale v. U.S. Dist. Ct. for S. Dist. of Iowa*, 482 U.S. 522 (1987), weighed in favor of disclosure.

36. *See, e.g.*, Heraeus Kulzer, GmbH v. Biomet, Inc., 633 F.3d 591 (7th Cir. 2011).

37. For example, with respect to the transfer of information from France to the United States for use in legal proceedings, which allegedly would have violated a French blocking statute, the U.S. Supreme Court held that U.S. courts should "take care to demonstrate due respect for any special problem confronted by the foreign litigant on account of its nationality or the location of its operations, and for any sovereign interest expressed by a foreign state." *Société Nationale*, 482 U.S. at 546. In so doing, "the concept of international comity requires in this context a . . . particularized analysis of the respective interests of the foreign nation and the requesting nation." *Id*. at 543–44.

efforts to reconcile the conflict and its resulting decision-making process.

Principle 8: If an organization has acted in good faith in its attempt to reconcile conflicting laws and obligations, a court or other authority reviewing the organization's actions should do so under a standard of reasonableness according to the circumstances at the time such actions were taken.

An organization's actions may be subject to review by a court or other governing authority regarding its attempt at resolving conflicting laws and obligations. That review should consider the specific circumstances when the Information Governance decision was made. Any judgment of the correctness of past actions to resolve conflicts should be based solely upon what was known at the time the decisions were made. Where a party has acted in good faith, it would be patently unfair to consider what they might have known had they possessed superior prescience.[38]

---

38. *See* The Sedona Conference, *The Sedona Conference International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition)*, Principle 2 (Jan. 2017), https://thesedonaconference.org/publication/International_Litigation_Principles ("Where full compliance with both Data Protection Laws and preservation, disclosure, and discovery obligations presents a conflict, a party's conduct should be judged by a court or data protection authority under a standard of good faith and reasonableness."). *See also* ABA Resolution 103 (2012) (adopted), *available at* https://www.americanbar.org/content/dam/aba/administrative/crsj/committee/feb-2012-dataprotection.authcheckdam.pdf ("[T]he American Bar Association urges that, where possible in the context of the proceedings before them, U.S. federal, state, territorial, tribal and local courts consider and respect, as appropriate, the data protection and privacy laws of any applicable foreign sovereign, and the interests of any person who is subject to or benefits from such laws, with regard to data sought in discovery in civil litigation.").

Application of the reasonableness standards requires that a court or other authority objectively assess the organization's actions or decisions in comparison to the actions or decisions made by a hypothetical, similarly situated organization acting reasonably under the same circumstances. In *Lewy v. Remington Arms Co.*,[39] the court outlined factors to be considered in assessing the reasonableness of a record retention policy for a spoliation instruction, including the following: (i) whether the policy was reasonable considering the facts and circumstances surrounding the relevant documents (i.e., whether a three-year retention policy is reasonable for a class of materials, such as email); (ii) whether any lawsuits relating to the documents had been filed, or may have been expected; and (iii) whether the document retention policy was instituted in bad faith.[40]

In determining good faith, courts or other authorities should give due deference to decisions by corporate officers or directors by applying the "business judgment rule," which is a presumption that a business decision was made "on an informed basis, in good faith and in the honest belief that the action taken was in the best interests of the company."[41]

Principle 9: An organization should consider reasonable measures to maintain the integrity and availability of long-term information assets throughout their intended useful life.

If the intended useful life of an information asset is long enough that risks or concerns may arise regarding the ongoing integrity and availability of the information, then organizations should consider appropriate measures designed to protect those

39. 836 F.2d 1104 (8th Cir. 1988).

40. *Id.* at 1112.

41. Aronson v. Lewis, 473 A.2d 805, 812 (Del. 1984) (citations omitted).

information assets. Therefore, long-term planning for availability and integrity depends on the circumstances involved, including the asset's purpose and storage media options.

For example, if an organization's intended retention period is 25 years and the media format it will be using has an expected life of 12 years, then specific planning will be required to ensure the ongoing integrity and availability of that information. Failing to ensure the integrity and availability of information assets may bring the risk of sanctions if an organization is unable to fulfill eDiscovery obligations.[42]

This principle is limited to "systems of record," meaning that copies (such as convenience copies) are outside its scope. Backup and recovery, disaster recovery, and redundant storage paradigms, such as Redundant Array of Independent Disks ("RAID"), are well-understood disciplines dictated by operational business continuity requirements and are therefore not covered by this commentary. Logical defects prior to "long-term" storage also are not covered by this principle or commentary.

1. Long-Term Digital Assets

The phrase "long-term" is used to mean a timeframe sufficiently long to involve planning for concerns such as the physical degradation of the storage medium or the impact of changing technologies.

Planning for the ongoing integrity and availability of long-term information assets is important for both physical and digital information, but it is especially important for digital assets that may have a long lifecycle or retention period. The risks and

42. United States v. Universal Health Servs., Inc., No. 1:07cv000054, 2011 WL 3426046 (W.D. Va. Aug. 5, 2011).

considerations should be evaluated as part of the long-term retention strategy.

To maximize the probability of ensuring the ongoing integrity and availability of digital assets throughout their intended useful life, organizations should make a good-faith attempt to balance risk and cost. Creating a long-term retention strategy appropriate to the value and type of the information involves considering a broad range of factors pertaining to the digital assets and the circumstances of the organization itself. These factors should include business value, regulatory importance, intended retention schedule, legal hold status, file format, continued availability of the technologies required to access and read, the likely failure rate of the storage medium as it is configured, the available budget and resources of the organization, and/or (for third-party services such as cloud storage, software as a service (SaaS), etc.), the contractual agreements between the customer and provider.[43]

Principle 10: An organization should consider leveraging the power of new technologies in its Information Governance program.

For many organizations, reliance on end-users to effectively manage information continues to work well. These organizations should consider how technology can help individuals to better oversee the information they are responsible for and to monitor management of the information. Examples of the former include limitations on the size of email accounts, or systems that automatically delete emails unless they are moved from the inbox or sent box. Appropriate use of this technology can significantly decrease the cost and risk of eDiscovery because emails frequently make up a significant percentage of information that

43. For a more detailed explanation of the specific areas of risk for digital assets, *see* Appendix C, *infra*.

is collected for litigation or government investigations. Similarly, organizations should consider using technology that automatically deletes voicemails after a fixed number of days. Companies can also monitor for over-retention by providing management with lists of the largest email accounts or reports on data that have not been accessed recently.

In addition to reliance on end-users, organizations should consider using advanced tools and technologies to perform various types of categorization and classification activities. While the rapid advances in technology threaten to render obsolete the technology described in this commentary, an organization should consider using technologies such as machine learning, auto-categorization, and predictive analytics to perform multiple purposes, including the following: (i) optimizing the governance of information for traditional RIM; (ii) providing more efficient and more efficacious means of accessing information for eDiscovery, compliance, and open records laws; and (iii) advancing sophisticated business intelligence across the organization.

1. Machine Learning, Auto-Categorization, and Predictive Analytics Defined

Machine learning is the "[f]ield of study that gives computers the ability to learn without being explicitly programmed."[44] Training filters to recognize spam email is one common example of machine learning. In theory, just about any classification problem arising in Information Governance can benefit from being modeled by machine-learning techniques. Some of these techniques do not rely on human intervention. For example, clustering or auto-categorizing data into data types or

44. Arthur L. Samuel, *Some Studies in Machine Learning Using the Game of Checkers*, 3(3) IBM J. OF RES. & DEV. 211–29 (1959).

classifications can be accomplished through software alone analyzing the properties of a data set.

One machine-learning technique of particular utility involves active learning by software through human interaction on the front end, where humans train the systems to learn through examples. "Predictive coding," "computer-assisted review," and "technology-assisted review" are terms used in the eDiscovery arena to describe the process whereby humans code sets of data into responsive and nonresponsive categories until the software can reliably analyze the remaining huge repositories of data.[45] As used here, "predictive analytics" means any machine-learning technique that combines human intervention on the front end with the power of machine learning to optimize the classification of information through automated rules.

2. New Technologies Meet Traditional RIM

If the structure, volume, or velocity of information flowing through networks does not allow or impedes the continued reliance on "end-users" to categorize content, organizations should consider taking steps that shift the burden of traditional RIM from individuals to technology through auto-categorization of content. For example, organizations may use existing software to analyze and categorize the contents of email for purposes of defensible deletion of transitory, non-substantive, or non-record content.[46] Organizations increasingly utilize

45. *See generally* Maura Grossman & Gordon Cormack, *The Grossman-Cormack Glossary of Technology-Assisted Review*, 7 FED. CTS. L. REV. 1 (2013).

46. The National Archives and Records Administration (NARA) has endorsed the use of email archiving and capture technologies using smart filters to sort content through role-based and rule-based architectures. *See* NARA Bulletin 2013-02, *Guidance on a New Approach to Managing Email Records* (Aug. 29, 2013), *available at* http://www.archives.gov/records-mgmt/bulletins/2013/2013-02.html.

predictive analytics to assist in categorization functions, where individuals train software to differentiate between types of records.

The first judicial opinions approving the use of predictive coding and technology-assisted review techniques for document review in eDiscovery were published in 2012.[47] In one case, the court stated that "the Bar should take away from this Opinion . . . that computer-assisted review is an available tool and should be seriously considered for use in large-data-volume cases where it may save the producing party (or both parties) significant amounts of legal fees in document review."[48] An important study by the Rand Corporation, anticipating this new direction in the law, concluded that predictive coding may significantly reduce eDiscovery costs by reducing the number of documents requiring eyes-on review.[49] The use of technology-assisted review for the exploration and classification of large document collections in civil litigation has evolved from a theoretical possibility to a valuable tool in the litigator's toolbox.[50]

---

47. *See, e.g.*, Da Silva Moore v. Publicis Groupe, 287 F.R.D. 182 (S.D.N.Y. 2012), *approved and adopted*, No. 11 Civ. 1279(ALC)(AJP), 2012 WL 1446534 (S.D.N.Y. Apr. 26, 2012); Global Aerospace Inc., et al. v. Landow Aviation, L.P., No. CL 61040, 2012 WL 1431215 (Va. Cir. Apr. 23, 2012); *In re* Actos (Pioglitazone) Products Liability Litig., No. 6-11-md-2299, 2012 WL 3899669 (W.D. La. July 30, 2012).

48. *Da Silva Moore*, 287 F.R.D. at 193.

49. Nicholas M. Pace & Laura Zakaras, *Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery*, RAND CORPORATION (2012), *available at* http://www.rand.org/pubs/monographs/MG1208.html.

50. *See* The Sedona Conference, *TAR Case Law Primer*, 18 SEDONA CONF. J. 1, 3 (2017).

3. Predictive Analytics and Compliance

Predictive analytics is also increasingly being utilized by organizations outside of the eDiscovery context, including in investigations and as an element of compliance programs. Predictive analytics is being used as an early warning system in compliance programs to predict and prevent wrongful or negligent conduct that might result in data breach or loss. To this end, companies use exemplar documents, sometimes in conjunction with search terms, to periodically search a target corpus of documents (usually email) to detect improper conduct.

4. Predictive Analytics and Business Intelligence

At its most fundamental level, predictive analytics assists in identifying information that may help to answer a question. There is no limit to the questions predictive analytics can help answer. Organizations are beginning to use predictive analytics to develop business intelligence about the organization itself, its information assets, and the market in which it operates.

Principle 11: An organization should periodically review and update its Information Governance program to ensure that it continues to meet the organization's needs as they evolve.

Organizations and their environments change. The footprint and nature of the organization's operations may expand, contract, or transform, and its technology capabilities and uses will evolve. The organization's environment will also change, including legal requirements for the retention, protection, preservation, and disposal of information. New information-related risks will also arise as time passes. Review of at least some aspects of many organizations' Information Governance

programs is legally required[51] and, regardless, is prudent given the inevitability of organizational and environmental change. Organizations, therefore, should periodically review and update their Information Governance program.

Program review differs from the monitoring activities that should be embedded in the organization's Information Governance program. Such monitoring activities observe whether information-related practices comply with the program's rules and risk controls. See Principle 5, Accountability. The program review should seek to determine whether the program itself, and its rules and risk controls, remain appropriate for governing the organization's information in light of organizational and environmental changes. A flawlessly executed Information Governance program will still result in compliance and risk exposures if elements of the program have become obsolete due to changed circumstances.

The review of the Information Governance program is akin to the assessment described under Principle 4. The organization should do the following:

---

51. For example, HIPAA policies and procedures must be reviewed periodically and updated as needed in response to environmental or operational changes affecting the security of ePHI. 45 C.F.R. § 164.316(b)(2)(iii). HIPAA security measures must also be reviewed and modified as needed to continue providing reasonable and appropriate protection for ePHI. 45 C.F.R. § 164.306(e). Comprehensive information security programs for customer information under the GLBA must be evaluated and adjusted in light of any material changes in operations or business arrangements. 16 C.F.R. § 314.4(e). Entities subject to the FTC's Red Flags Rule must ensure that their mandated Identity Theft Program is updated periodically to reflect changes in risks to customers or to their safety and soundness regarding identity theft. 16 C.F.R. § 681.1(d)(2)(iv). And entities that own or license personal information about Massachusetts residents must review their information security measures at least annually or whenever a material change in business practices reasonably implicates the security or integrity of records containing such personal information. 201 CMR. 17.03(2)(i).

- Identify any significant changes in its lifecycle practices for information
- Identify significant changes in applicable compliance requirements and risks regarding its information
- Review the organization's strategic objectives for Information Governance considering internal or external changes
- Review the results from monitoring and measuring performance of the organization's Information Governance program as an indicator of whether the program's rules and risk controls are adequate or should be refined

Those responsible for administering the organization's Information Governance program should be involved in the program review. The need for objectivity in conducting such a review may make it valuable to have an independent review of the program. And ultimately, because senior leadership is responsible for the results of Information Governance at the organization, such senior leadership should participate appropriately in the review process, receive the results of the review, and then provide direction, support, and resources for needed changes in the program.

No bright-line rule governs how frequently an Information Governance program should be reviewed. As with other business-driven initiatives, the frequency of review will most likely depend on many factors relating to the organization.[52] If an

52. Determining the appropriate frequency of review is a matter of business judgment. Courts generally defer to decisions by corporate officers and directors pursuant to the "business judgment rule," which is built upon the presumption that business decisions are made "on an informed basis, in good faith and in the honest belief that the action taken was in the best

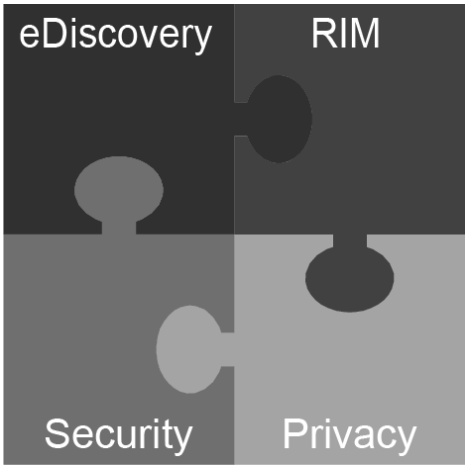
organization is rapidly changing through frequent acquisitions and divestitures, or periodically undergoes major updates to its technology systems, then its information environment is likely to be ever-changing to adapt to its new structure or systems. Alternatively, if an organization is relatively mature, has a stable operations model, or is not governed by frequently changing governmental regulations, it may be reasonable for it to conduct its reviews less frequently (e.g., biannually) to reassess and identify potential modifications to its recordkeeping, data security, and operational requirements. Further, an organization may be impacted by external pressures, such as regulations subject to frequent modification or regular compliance audits that require systemic changes. In such cases, the organization should be prepared to review and revise its Information Governance policies on an ongoing basis to meet the challenges posed by such changes. An organization should track pending legislation and regulations relevant to its industry to facilitate continued compliance with the regulations that affect its operations. It would be prudent to include a review of its Information Governance policies and procedures as part of its response to such developments.

As a result of the ongoing program review, update, and execution, an organization will have reasonable assurance its Information Governance program continues to meet both legal requirements and the organization's strategic objectives for information.

---

interests of the company." Aronson v. Lewis, 473 A.2d 805, 812 (Del. 1984), *overruled on other grounds*, Brehm v. Eisner, 746 A.2d 244 (Del. 2000).

APPENDIX A: INTERSECTIONS



Intersections Create Opportunities and Challenges

Although the functional areas of Records and Information Management (RIM), eDiscovery, Privacy, and Security are frequently separate, a successful Information Governance program requires them to work together. As there is some natural overlap among the four groups, this provides opportunities to combine resources and budgets. Conversely, the goals of the intersecting groups may clash and require resolution before an initiative can move forward. Identifying and leveraging these areas early in a program is an important task. The tables below define many of the synergies and conflicts in the intersections of these groups.

<table>
<tr><th colspan="3">RIM</th></tr>
<tr><td colspan="3">Primary Focus: Ensuring that records and information are properly maintained, accessed, and ultimately disposed of in accordance with statutory and regulatory requirements and with consumer expectations</td></tr>
<tr><th>eDiscovery
Intersection with Functional Area</th><th>Privacy
Intersection with Functional Area</th><th>Security
Intersection with Functional Area</th></tr>
<tr>
<td>Potential Synergy:
● Share similar metadata concerns
● Work together to respond to document requests by locating and preserving relevant information
● Support consistent defensible disposition of information in accordance with an organization's legal, regulatory, and operational requirements
● Enable an organization to know what it has and identify, preserve, retrieve, search, produce, and appropriately destroy data in normal course of business
● Protect against loss of content that could lead to sanctions, financial loss, and brand risk during eDiscovery
● Serve as evidence of official policy and help ensure that evidence can be authenticated
Potential Friction:
● RIM could retain drafts or outdated content due to relevancy
● RIM focus could be more narrowly targeted to "records," while eDiscovery focus is ESI</td>
<td>Potential Synergy:
● Define requirements for identification and classification of sensitive information
Potential Friction:
● RIM may need wide access and distribution, while Privacy seeks limits</td>
<td>Potential Synergy:
● Ensure that sensitive information is properly identified, maintained, accessed, and disposed of according to legal and regulatory requirements
Potential Friction:
● RIM may need wide access and distribution, while Security seeks limits
● Encryption may be required in Security but could frustrate accessibility by RIM</td>
</tr>
</table>

eDiscovery		
Primary Focus: Preserving and processing electronically stored information that is potentially relevant to impending or ongoing litigation in a timely, auditable, and efficient manner		
RIM **Intersection with Functional Area**	**Privacy** **Intersection with Functional Area**	**Security** **Intersection with Functional Area**
See RIM/eDiscovery intersection above	**Potential Synergy:** • Identify at point of creation information subject to privacy regulations to reduce risk that private information will be produced **Potential Friction:** • Producing private information protected by another country's laws can result in civil or criminal sanctions • Refusing to produce private information may result in civil or criminal penalties under U.S. laws	**Potential Synergy:** • Ensure that sensitive data and information are available, if relevant, and that out-of-date information is disposed of according to legal and regulatory requirements • Satisfy an organization's "duty to preserve" for forensic collections **Potential Friction:** • Security encryption requirements can hamper eDiscovery efforts accessibility by RIM

Security		
Primary Focus: Ensuring the confidentiality, integrity, and availability of information and assets		
RIM **Intersection with Functional Area**	**eDiscovery** **Intersection with Functional Area**	**Privacy** **Intersection with Functional Area**
See RIM/Security intersection above	See eDiscovery/Security intersection above	**Potential Synergy:** • Enforce the access rights defined by Privacy **Potential Friction:** • Privacy requirements may hamper security investigations

Privacy		
Primary Focus: Ensuring private information is secured, protected, and managed in accordance with statutory, regulatory, privacy, and operational requirements		
RIM **Intersection with Functional Area**	**eDiscovery** **Intersection with Functional Area**	**Security** **Intersection with Functional Area**
See RIM/Privacy intersection above	See eDiscovery/Privacy intersection above	See Security/Privacy intersection above

APPENDIX B: MATURITY CONTINUUM AS IT RELATES TO INDEPENDENCE

It is important to consider the independence of the Information Governance function of an organization when making determinations such as assessing the current maturity or planning how to increase the future maturity of an Information Governance program.

While not all organizations have a sufficiently mature Information Governance program to warrant the appointment of a C-level executive in this role, we believe that organizations must ultimately view Information Governance as requiring an executive leader who is accountable to the CEO or COO to ensure that decisions are made in the best interests of the overall organization, rather than for the good of distinct departments.

A common difficulty when balancing costs and risks occurs when the choices have dissimilar characteristics that make comparison difficult. For example, a clearly defined cost saving may need to be weighed against a high-impact, low-probability event, such as statutory fines in the event of leakage of protected data, where it is difficult to quantify the probability of the event occurring or the costs. Whatever risk management methodology is used to balance cost and risk, it will be more accurate to make the determination by looking at the problem from the perspective of the overall organizational impact.

However, if the executive in charge of Information Governance reports to an individual department, there is the potential for the interests of that department to be given greater weight than the overall interests of the organization. The simple fact that the department to which the executive reports funds their work and rates their job performance may result in such a bias.

Therefore, the level of independence of the Information Governance function of an organization is an important component of the Information Governance maturity continuum.

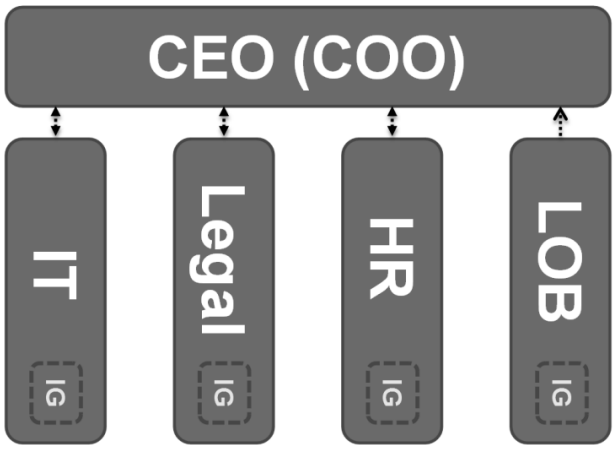
Maturity and Independence

The following discussion is intended as a reference to aid in assessing the current level of maturity of an information function, planning how to move an organization further along the Information Governance maturity continuum, or deciding what is sufficient independence for a given organization. The concepts described below can be adapted for the specific circumstances of an organization.

Note: The following graphics are highly simplified, generic representations of potential organizational structures at varying points along the maturity continuum. The graphics depict the coordination and accountability at a departmental level (IT, Legal, HR, and Line of Business (LOB)). Specific functions, such as RIM, Privacy, Security, eDiscovery, etc., are intentionally not shown because they generally reside within a stakeholder department.

Immature

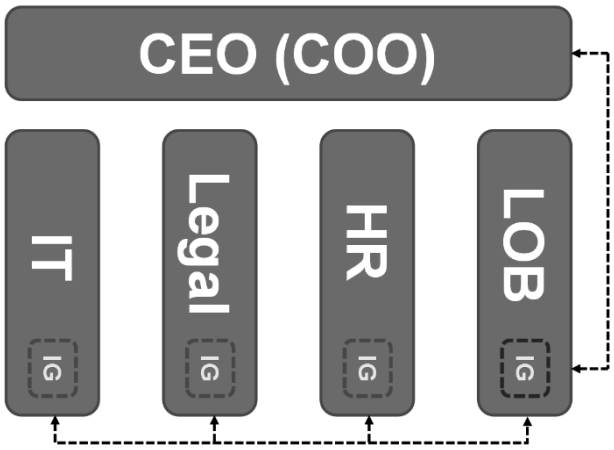
Immaturity is characterized by a lack of overarching coordination of Information Governance stakeholders and no single point of accountability to the CEO or COO for overall governance of information.



At the immature end of the maturity continuum, lack of coordination creates a potential for missing important requirements. Decisions and requirements reside in silos, and cross-functional coordination is ad hoc. There is potential for departmental decisions that conflict with other stakeholder requirements and that are not in the interests of the organization overall. There is also potential for inconsistent treatment of different items in the same category in the same circumstances.

Less Mature

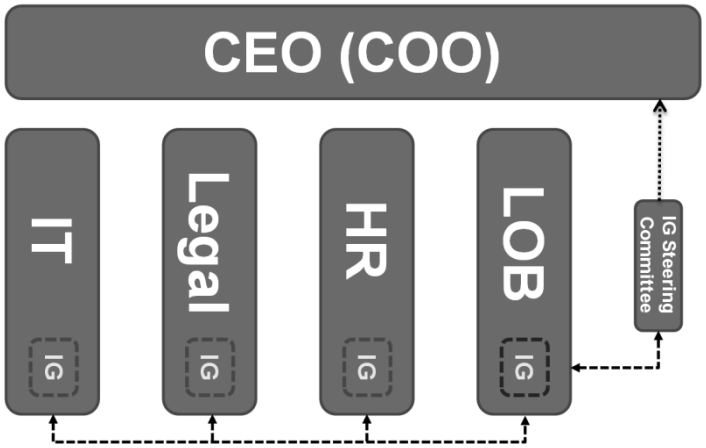
At this area of the maturity continuum, ownership of Information Governance process resides within a stakeholder department.



This creates a potential conflict of interest, due to misaligned incentives.

More Mature

At this area of the maturity continuum, ownership of Information Governance process resides in a stakeholder department but is accountable to a steering committee of C-level executives from the stakeholder departments who are accountable to the CEO or COO.

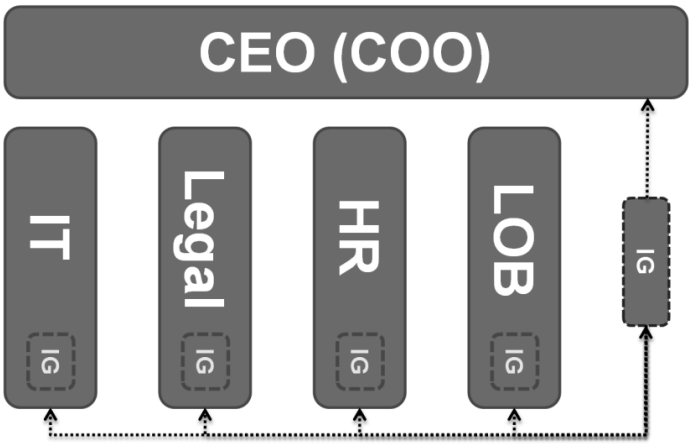


There is still potential for conflict of interest for the executive in charge of Information Governance (who resides in a stakeholder department) and for the C-level executives on the

Information Governance steering committee because the goals of the individual departments may conflict with the goals of the overall Information Governance program.

Mature

A mature Information Governance function is characterized by an executive who resides in a separate Information Governance department and is accountable to the CEO or COO for coordinating stakeholders across all departments and functions and balancing decisions for the benefit of the organization overall.



APPENDIX C:
RISKS ASSOCIATED WITH DIGITAL ASSETS

Risks

There are specific areas of risk for digital assets that organizations should consider, including the following:

Integrity

The term "integrity" is used to mean the authenticity and reliability of the information. In some situations, this may simply mean the logical content of the information has not been altered. In other situations, it may mean a guarantee that the file has not changed.

The integrity of the information, or of information required to access the information (such as an index or necessary metadata), may be compromised by factors such as unauthorized alteration or degradation of the storage medium. These risks can become particularly acute during platform migration.

Consideration should be given to (i) the level of integrity required both for the digital asset in question and the technologies required to read and access the data, and (ii) the level of difficulty involved in repairing or recovering damaged digital information.

Careful consideration should also be given to the file format, storage medium (including the configuration of that storage medium), and the circumstances of operation and storage to ascertain the likelihood of data loss.

Digital storage media without moving parts (such as flash drives, solid state drives, and tape) or with rarely moving parts (such as storage devices intended for infrequent use that power off when not in use) still fail. Unused storage media on a shelf (for example, forensic collections on individual storage media in an evidence lab) will eventually become unusable. Given the relatively short lifespan (say, three to five years) of some items of

storage media, a legal hold or retention requirement that may exceed the reasonably expected lifespan could necessitate specific long-term planning due to the failure rate of the technology involved.

Availability

The term "availability" is used to mean "able to be used when needed," which includes the following:

- being able to access information in a timely manner (for example, within applicable service-level agreements, contractual requirements, or timeframes indicated by legal requirements); and
- being available within an agreed-upon lead time (depending on business need).

Note that availability can apply to any element (such as security mechanisms to protect the data, access rights required to access the data, or applications required to interpret or read the data) and does not necessarily mean continuous availability.

The availability of information, or information required to access the information (such as an index or necessary metadata), may be compromised by obsolescence or unavailability of technology required for accessing the information (or index, or necessary metadata) in a timely manner.

Considerations

When planning for ongoing integrity and availability of digital assets throughout their intended useful life, important considerations include the following.

Technology Refresh Period

The phrase "technology refresh period" is used to refer to the timeframe in which technology components are expected to

fail and within which planning needs to occur for replacing those components.

Organizations should exercise prudence when considering the technology refresh period for long-term digital assets. For example, if the expected lifespan of the storage medium is seven years, then the technology refresh period should be less than seven years. The timing of the technology refresh period compared to the technology's expected lifespan is a matter of risk calibration and business judgment.

Planned Migrations

Obsolescence of technology is a major consideration in long-term storage of digital assets and requires careful planning. Migrations (moving to a new platform for the archive as a whole or for a component of the archive) are a consequence of obsolescence that must be planned. All elements of the archiving system, including search-and-retrieval capability as well as storage medium, should be considered in terms of obsolescence. Organizations should consider creating an obsolescence review period as part of their long-term archival planning, because unlike a technology refresh period (which can be ascertained in advance for each technology refresh cycle by reference to the expected life of the technology components), the probable time of obsolescence may not be knowable in advance.

Migrations may also require format conversions, and integrity-checking technologies (see below) are particularly critical to ensure the data is not inadvertently changed during a migration.

Matching Storage Medium to the Type of Electronic Information

It is important to match the characteristics of the storage medium to the requirements of the information being stored. For example, micrographics work particularly well for text documents—especially those held for reference purposes—but not

for binary files, such as audio files or Computer Aided Design (CAD) files. Micrographics also may not work well for files that need to be in digital format, because a scanning or conversion process will be required before the file can be used.

The expected failure rate of the storage medium should be considered in terms of the expected retention period. For example, regulated utilities or pipelines often involve document retention periods of decades, which can be longer than the life of the plant.

Integrity-Checking Technologies

Passive integrity-checking technologies can be used to assess if a file has changed. These technologies include such mechanisms as hash values created by hash algorithms computed when a file is retrieved and if the file has changed. Unfortunately, passive integrity-checking technologies have no inherent mechanism to repair files and restore them to their original form—they can only alert you when a problem has occurred.

Active integrity-checking technologies can be used not only to assess if a file has changed but also (if appropriately configured) to restore a file to its originally form. There are many proprietary examples of integrity-checking archive technologies. Because these technologies are generally well-understood and well-documented, they are not discussed further here.

Long-Term Physical Information Assets

When considering storage using physical media, such as paper, it is important to ensure that the expected life of the storage medium exceeds the retention requirements. In the case of printed paper, the expected life of different types of paper, as well as different types of ink, can vary a great deal. It is also important to consider the storage conditions (such as humidity and temperature) required to ensure the ongoing integrity of the

physical assets, because this can affect the expected life of the physical storage medium.

APPENDIX D:
THE QUANTITATIVE/ROI BUSINESS CASE

As discussed in the commentary, a successful Information Governance approach requires both strategic commitment (adoption as an organizational priority) and tactical efforts. This Appendix discusses approaches to establishing an acceptable return on investment (ROI) for particular projects.

A typical ROI analysis weighs the benefits of a project against its cost and calculates the length of time it will take to recoup the cost. The quantitative aspects of the business case are best determined by focusing on specific applications of Information Governance to identified problems or opportunities or to distinct projects for implementation of the Information Governance program.[53]

The quantifiable benefits from pursuing Information Governance generally fall into four main categories: optimizing organization value, risk reduction, hard-cost avoidance, and soft-cost avoidance.

Optimizing Organization Value

Information Governance can help make information assets available for new, valuable uses. It can also allow organizations to derive value from engaging in what might otherwise be cost-prohibitive endeavors, due to efficiencies and cost savings realized through Information Governance practices. In general, Gartner has identified the following benefits of an Information Governance program, which add to organization value, and we provide some examples:

- **Effectiveness** (e.g., document-centric collaboration tools)

53. *See generally* SOARES, *supra* note 11 (providing insight into the best ways to encourage businesses to implement an Information Governance program).

- **Cost/efficiency** (e.g., imaging/workflow solutions replace traditional paper-oriented processes)
- **Customer service** (e.g., customer-relationship solutions that lead to better market penetration and customer satisfaction)
- **Competitive advantage** (e.g., more modern tools and reliable information allow speedier delivery of goods or services to customers)
- **Revenue** (e.g., as a result of enhanced social media and web presences and solutions)[54]

A core benefit of an Information Governance program is to ensure that information used for different purposes across the organization—e.g., for sales and marketing, but also for planning, billing, fulfillment, financial, customer feedback, and other downstream purposes—is reliable or trustworthy, accurate, and in formats usable across platforms or applications. Achieving these objectives requires that the IT department understands not only the business purposes and objectives but also whether data elements require special protections or treatments (e.g., for legal, RIM, privacy, or security reasons).[55] Yet, oftentimes, when a large organization initiates such a program, it finds that different business units or functions use different terminology for the same content concept. For example, an organization may refer to outside business partners as vendors, suppliers, associates, or providers, and may collect various information about such entities in systems that support particular functions within the organization. But if the terminology—or application—differs between and among business units,

54. *See* Karen M. Shegda & Kenneth Chin, *First 100 Days: Enterprise Content Management Initiatives*, GARTNER (July 7, 2011), *available at* http://www.gartner.com/id=1739415.

55. *See, e.g.*, SOARES, *supra* note 11, at 149.

opportunities to cross-sell or otherwise leverage the information about the business partners may be missed.[56] Thus, an early goal for an Information Governance program may be to develop a common vocabulary and understanding of what information-related assets exist. Once that is done, the organization may realize that business advantages may be achieved—at virtually no cost—by cross-utilizing existing information or systems.[57]

Mergers and acquisitions, or technology upgrades, also present opportunities (and challenges) for improving data quality and organization revenues by, for example, merging (and purging) customer lists to identify strong customers across multiple business lines.[58]

Risk Reduction

Risk reduction is also a significant benefit of Information Governance. Business value may not be realized if an unanticipated risk creates an unexpected cost. For example, organizations may leverage information over the short-term (e.g., email for current communications), but once the information is no longer useful, the electronically stored information (ESI) is often stored away, rarely accessed, and often never reassessed to determine whether the benefits of continued retention outweigh

56. As another example, it has been reported that one manufacturing company discovered and eliminated 37 unique definitions of "customer" across its enterprise and agreed on a single, standard definition. Robert Routzahn, *Business and IT Collaboration: Essential for Big Data Information Governance*, IBM BIG DATA & ANALYTICS HUB (July 5, 2013), *available at* http://www.ibmbigdatahub.com/blog/business-and-it-collaboration-essential-big-data-information-governance.

57. *See, e.g.*, The Sedona Conference, *Commentary on Finding the Hidden ROI in Information Assets*, *supra* note 14.

58. A medical-device manufacturer estimated that improving ship-to addresses in a 100,000-item database could increase aftermarket sales by $1 million. SOARES, *supra* note 11, at 69.

the risks. Thus, what was once a business asset may become a source of risk for certain organizational areas, such as compliance or eDiscovery, while providing little or no benefit for other organizational areas, such as business units. Through proper Information Governance, organizations can recognize these perils and elect to remediate their un- or under-utilized information assets and optimize the business value of information while managing the associated risks.

Many types of adverse events can be avoided through effective Information Governance. The value of risk reduction can be estimated by quantifying the potential losses that would result if an adverse event occurred and determining the reduced likelihood of such an occurrence due to effective Information Governance. Some examples of risks posed by information assets follow:

- **Data Leakage:** Many companies have valuable intellectual property that is more likely to be lost or leaked to the public and/or competitors if not properly managed through policies and procedures that emanate from a mature Information Governance program.
- **Privacy Breaches:** A myriad of regulations applicable to particular sectors in the United States (e.g., HIPAA to health information, GLBA to financial institutions, Family Educational Rights and Privacy Act (FERPA) to federally funded educational institutions) require certain data to be protected and impose fines and other sanctions when the data is not properly protected or is improperly disclosed.
- **Security Lapses:** Regulations, such as the self-regulatory Payment Card Industry Data Security Standards, require companies to protect

credit card and other payment information or face fines.

- **Brand Impact:** A breach of private customer information, such as contact information or social security numbers, can adversely impact an organization's brand and result in lost sales and/or consumer goodwill.
- **Litigation/Regulatory Risk:** Access to the most relevant information at the inception of litigation or a regulatory inquiry may allow for an earlier and more accurate assessment of litigation risk and, thus, permit such events to be more effectively and economically managed.

Hard-Cost Avoidance

Many benefits flowing from an Information Governance program are based on the premise that certain future costs can be delayed, reduced, or avoided entirely because lesser volumes of data will be kept in a more efficient manner. These benefits can be quantified, and in an Information Governance program, often arise from the following areas:

- **Storage:** Storage and maintenance costs can be radically reduced by rationalizing data storage options, eliminating outdated information assets that no longer serve a legitimate business, legal, or regulatory purpose, moving valuable information that is occasionally and non-critically accessed to cheaper storage, and minimizing the need for additional storage. A systematic approach to Information Governance may allow an organization to archive its less-active and less-critical data on less-expensive tiers of storage, which in turn can eliminate unnecessary duplication of documents and

associated backup overhead and better enable data disposition in line with organizational policy.

- **Outdated Backup Media:** Eliminating the retention of large (and outdated) quantities of backup media, such as magnetic tapes, reduces the costs of backup media and related storage, labor, and transfer expenses.
- **Personnel Costs:** A successful Information Governance program will reduce the volume of ESI and make it easier to manage and to find information. Accordingly, fewer personnel would be required to manage the reduced volume, allowing the organization to realign resources appropriately.
- **eDiscovery Costs:** A reduced volume of electronic information can, in the event of litigation, reduce litigation costs significantly, because there will be less information to process and review.[59]

Soft-Cost Avoidance

Improved Information Governance also saves time and effort that can be deployed for other activities. For example, having a more efficient method for storing and accessing email messages might save 30 minutes per day for each employee, netting a direct financial savings to the organization or allowing employees to focus on more useful activities. Soft costs are often difficult to quantify, but the following are useful considerations:

---

59. A widely cited 2012 Rand survey states that the review process alone averages $18,000 a gigabyte, meaning that with collection, preservation, hosting, etc., eDiscovery costs can easily exceed $20,000 a gigabyte. Pace & Zakaras, *supra* note 49.

- **Economies of Scale:** Managing information on an ad hoc basis can result in overlooked requirements and risks, unrealized benefits, and tremendous amounts of inefficiency due to the redundancy of effort this entails. Economies of scale can be realized by having an overarching Information Governance program at an organizational level, which generates processes and procedures to govern how information assets are handled.
- **Organizational Inefficiencies:** Organizations with excessive amounts of uncategorized information assets are often unable to locate needed information in a timely and efficient manner. An Information Governance program that creates an infrastructure for information assets promotes shorter client response times, allows the repurposing of institutional knowledge, and enhances continuous improvement efforts.

THE SEDONA CONFERENCE COMMENTARY ON DEFENSIBLE DISPOSITION

A Project of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1)

Author:

The Sedona Conference

Drafting Team:

Lauren A. Allen
Ross Gotler
Logan J. Herlinger
Mark Kindy
Jesse Murray
Ken Prine
David C. Shonka

Drafting Team Leaders:

Tara Emory
Becca Rausch

Editors-in-Chief and WG1 Steering Committee Liaisons:

Kevin F. Brady
Dean Kuckelman

Staff Editors:

David Lumia
Susan McClain

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 1. 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 Defensible Disposition,* 20 SEDONA CONF. J. 179 (2019).

PREFACE

Welcome to the final, April 2019, version of The Sedona Conference *Commentary on Defensible Disposition*, a project of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). 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, and intellectual property rights. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The idea for this *Commentary* arose from discussion in 2016 among the Steering Committee liaisons and team leaders in charge of updating the 2014 *Commentary on Information Governance,* which was a topic for discussion at the Sedona Conference WG1 2016 Midyear Meeting. The leadership recognized that with the staggering amount of data that is produced daily, there was a need for guidance for organizations and counsel on the adequate and proper disposition of information that is no longer subject to a legal hold and has exceeded the applicable legal, regulatory, and business retention requirements. The subject of defensible disposition as a separate topic was first discussed at the 2016 Annual Meeting, where it received a very favorable reception. Then at the 2017 Midyear Meeting, a session was dedicated exclusively to "Defensible Disposition of Information." As a result of that panel discussion and the dedicated work of the drafting team, a preliminary draft of this *Commentary* was presented for member comment at the 2018 Midyear Meeting. The drafting team acted on the various recommendations the membership provided, which resulted in the public comment version of this *Commentary* in August 2018. Where appropriate, the comments received during the public comment

period have now been incorporated into this final version of the *Commentary*.

The Sedona Conference acknowledges the efforts of Drafting Team Leaders Tara Emory and Becca Rausch, who were invaluable to driving this project forward. We also thank drafting team members Lauren A. Allen, Ross Gotler, Logan J. Herlinger, Mark Kindy, Jesse Murray, Ken Prine, and David C. Shonka for their efforts and commitments in time and attention to this project. Finally, we thank Kevin Brady and Dean Kuckelman who served as both the Editors-in-Chief and WG1 Steering Committee Liaisons to the drafting team.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG1 and several other Working Groups in the areas of international electronic information management, discovery, and disclosure; patent damages and patent litigation best practices; data security and privacy liability; trade secrets; and other "tipping point" issues in the law. 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
April 2019

TABLE OF CONTENTS

I. INTRODUCTION

Principle 6 of The Sedona Conference *Commentary on Information Governance* provides the following guidance to organizations:

> The effective, timely, and consistent disposal of physical and electronic information that no longer needs to be retained should be a core component of any Information Governance program.[1]

The Comment to Principle 6 explains:

> It is a sound strategic objective of an organization to dispose of information that no longer provides value to the organization, if that information is not required for statutory or regulatory compliance or legal hold purposes. . . . If there is no statutory, regulatory, or preservation obligation, information should be disposed of as soon as the likely business value of retaining the information is outweighed by the cost and risk of retaining the information. . . . Typically, the business value decreases and the cost and risk increase as information ages.[2]

Despite this advice, and similar advice from other sources, many organizations continue to struggle with making and executing effective disposition decisions. That struggle is often caused by many factors, including the incorrect belief that

---

1. The Sedona Conference, *Commentary on Information Governance, Second Edition*, 20 SEDONA CONF. J. 95, 139 (2019), *available at* https://thesedonaconference.org/publication/Commentary_on_Information_Governance. "Information Governance" is "an organization's coordinated, interdisciplinary approach to satisfying information compliance requirements and managing information risks while optimizing information value." *Id.* at 104.

2. *Id.* at 139–40.

organizations will be forced to "defend" their disposition actions if they later become involved in litigation. Indeed, the phrase "defensible disposition" suggests that organizations have a duty to defend their information disposition actions. While it is true that organizations must make "reasonable and good faith efforts to retain information that is . . . relevant to claims or defenses," that duty to preserve information is not triggered until there is a "reasonably anticipated or pending litigation"[3] or other legal demands for records. Another factor in the struggle toward effective disposition of information is the difficulty in appreciating how such disposition reduces costs and risks. Lastly, many organizations struggle with *how* to design and implement effective disposition as part of their overall Information Governance program.

These Principles and Commentary regarding disposition of information ("Commentary") attempt to address these three factors and provide guidance to organizations, and the professionals who counsel them, on developing and implementing an effective disposition program. This Commentary uses "information" to refer to both physical and electronic information.

3. The Sedona Conference, *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1, Principle 5 at 93 (2018) [hereinafter *The Sedona Principles, Third Edition*].

II. PRINCIPLES

Principle 1. Absent a legal retention or preservation obligation, organizations may dispose of their information.

Comment 1.a. Organizations should, in the ordinary course of business, properly dispose of information that they do not need.

Organizations may avoid retaining information that is not subject to retention or preservation obligations.[4] Regular disposition of obsolete information is simply an information management best practice, related to good housekeeping and Information Governance, which was acknowledged by the U.S. Supreme Court in *Arthur Andersen LLP v. United States*:

> '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. It is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under ordinary circumstances.[5]

In *Andersen,* the Court reversed and remanded a criminal conviction under a federal obstruction statute, noting that "[a] 'knowingly corrupt persuader' cannot be someone who persuades others to shred documents under a document retention policy when he does not have in contemplation any particular

4. *See* The Sedona Conference, *Commentary on Inactive Information Sources*, Principle 2, THE SEDONA CONFERENCE (July 2009 Public Comment Version), https://thesedonaconference.org/publication/Commentary_on_Inactive_Information_Sources.

5. 544 U.S. 696, 704 (2005) (internal citation omitted).

official proceeding in which those documents might be material."[6]

Similarly, the advisory committee notes to Federal Rule of Civil Procedure 37(e)[7] make clear that the duty to preserve electronically stored information (ESI) is triggered when litigation is filed, or reasonably anticipated:

> The new rule applies only if the lost information should have been preserved in the anticipation or conduct of litigation and the party failed to take reasonable steps to preserve it. . . . The rule does not apply when information is lost before a duty to preserve arises.[8]

Thus, organizations should not be required to "defend" their disposition of any information that takes place before that duty arises. Indeed, information about the organization's Information Governance program and the organization's disposition practices *before* the duty to preserve arises are typically not discoverable.[9]

---

6. *Id.* at 708. The Court did not decide whether the Andersen employees did "have in contemplation any particular official proceeding"; instead, the Court reversed and remanded because "the jury instructions [at the trial court] were flawed in important respects."

7. Rule 37(e), which focuses exclusively on ESI, may provide serious consequences for organizations that "fail[ed] to take reasonable steps to preserve" information "that should have been preserved." FED. R. CIV. P. 37(e).

8. FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment.

9. *See The Sedona Principles, Third Edition*, *supra* note 3, at 127, Comment 6.c. ("[P]arties should not be required to produce documentation of their discovery processes unless there has been a showing of a specific deficiency in their discovery processes.").

Illustration: In a products liability suit, the plaintiff requests discovery regarding the product manufacturer's written Information Governance program, its retention schedule, and a list of relevant information that no longer exists; when that ESI was destroyed; and why that information was destroyed. In responding to the manufacturer's relevance and proportionality objections, the plaintiff makes no showing that the manufacturer violated its duty to preserve ESI after the lawsuit was pending or reasonably anticipated. The manufacturer is entitled to stand on its objections.

Of course, once the duty to preserve has been triggered, organizations must take reasonable steps to preserve relevant ESI, regardless of whether their Information Governance program would otherwise allow or require its disposition. These preservation obligations are discussed in *Comment 1.b.*

Similarly, there may be an obligation to preserve information for government investigations, as discussed in *Comment 1.c.*, and there may be a statutory or regulatory obligation to retain certain information, as discussed in *Comment 1.d.* Lastly, the disposition program should avoid disposing of information that continues to provide operational or other business value to the organization, as discussed in *Comment 2.a.*

Comment 1.b. When designing and implementing an information disposition program, organizations should consider the obligation to preserve information that is relevant to the claims and defenses and proportional to the needs of any pending or reasonably anticipated litigation.

A detailed discussion of when the duty to preserve is triggered, and what is required to meet that duty, is beyond the scope of this Commentary. A general description of those

preservation duties is included in *The Sedona Principles*,[10] and a more specific discussion is in The Sedona Conference *Commentary on Legal Holds*.[11]

Information Governance programs must provide for meeting those duties even where the program would otherwise call for disposition of the ESI, such as when the information has met its retention period and no longer provides any business value. Although Information Governance programs do not create a preservation duty where it does not already exist, they may come under judicial scrutiny if an organization fails to meet its obligations to preserve ESI for pending or anticipated litigation. As explained by the advisory committee notes to Rule 37(e):

> [C]ourts may sometimes consider whether there was an independent requirement that the lost information be preserved. Such requirements arise from many sources—statutes, administrative regulations, an order in another case, or a party's own information-retention protocols. The court should be sensitive, however, to the fact that such independent preservation requirements may be addressed to a wide variety of concerns unrelated to the current litigation. The fact that a party had an independent obligation to preserve information does not necessarily mean that it had such a duty with respect to the litigation, and the fact that the party failed to observe some other preservation obligations does not itself prove that its efforts to

10. *Id.* at 51–53, Principles 5 and 14.

11. *See generally* The Sedona Conference, *Commentary on Legal Holds, Second Edition: The Trigger & The Process*, 20 SEDONA CONF. J. 341 (2019).

> preserve were not reasonable with respect to a particular case.[12]

Thus, even before a duty to preserve arises, selective disposal may still carry risks.[13] For example, if an organization's Information Governance program provides for "selective disposition" of information that would be hurtful if litigation later arises, while allowing for the retention of information that provides little value other than it might help the organization, some courts may consider such an approach as evidence that the organization anticipated litigation when it designed its Information Governance program.

> *Illustration:* Pursuant to its retention schedule, a product manufacturer routinely disposes of product testing results that show the product is unsafe but retains testing results that show the product is safe. The manufacturer later argues that it did not anticipate litigation until it was sued, years after the unhelpful testing results were destroyed. In determining when litigation was anticipated, or reasonably should have been anticipated, the court may consider, among other factors, the "selective disposition" by the organization. In addition, if the

---

12. FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment ("The rule does not apply when information is lost before a duty to preserve arises.").

13. *See* Micron Technology, Inc. v. Rambus Inc., 645 F.3d 1311, 1317–29 (Fed. Cir. 2011) (affirming sanctions for spoliation of evidence plaintiff destroyed in an effort to become "battle-ready" for litigation); *see also* United States *ex rel.* Carter v. Bridgepoint Education, Inc., 305 F.R.D. 225, 243 (S.D. Cal. 2015) ("[A] defendant remains free to operate their business in its ordinary course in the absence of the reasonable probability of a certain lawsuit and so long as it does not render data inaccessible purely with the intent of stymying such legal action."); *cf.* FED. R. CIV. P. 37(e) (authorizing the imposition of spoliation sanctions where there is an "intent to deprive").

> court determines that the organization violated a duty to preserve, the court may consider the organization's "selective disposition" in determining whether the organization acted with an "intent to deprive" under Rule 37(e)(2).[14]

Information Governance programs should also include a provision to return to "normal" retention/disposition procedures after a duty to preserve ceases. Events during the life of a matter may warrant adjusting the scope of what is preserved. The *Commentary on Legal Holds*[15] observes that it is reasonable for parties to review and revise a legal hold notice when they receive new information that could affect the scope of a legal hold. *The Sedona Principles, Third Edition*, similarly observes that

> [p]reservation obligations may expand, or contract, as the contours of claims and defenses are clarified during the pendency of a matter. If the scope of the claims or defenses expands, parties may need to increase their preservation efforts, which may require them to amend their preservation notices. Conversely, when the scope of claims or defenses contracts, the party preserving the information will have an interest in modifying its

14. *See* Barnett v. Deere & Co., No. 2:15-CV-2-KS-MTP, 2016 WL 4544052 (S.D. Miss. Aug. 31, 2016) (declining to find sufficient evidence of bad faith and denying sanctions where lawnmower manufacturer's destruction of safety information occurred pursuant to its records policy and before plaintiff's injury, even though defendant had a "'long history of litigating rollover claims'"); *cf.* Phillip M. Adams & Assocs., LLC v. Dell, Inc., 621 F. Supp. 2d 1173, 1191 (D. Utah 2009) (duty to preserve arose when manufacturer was "sensitized" to product issue and should have had a reasonable expectation of litigation when similar class action claims arose against other manufacturers years earlier).

15. The Sedona Conference, *Commentary on Legal Holds*, *supra* note 11, at 373, 399–403.

> preservation efforts and notices so that it may resume normal information management procedures for information that is no longer relevant to the claims or defenses.[16]

Prior to the close of discovery, any number of events may provide information that expands or contracts the scope of preservation. These events include reviewing and responding to discovery, interacting with opposing counsel about discovery, and incorporating substantive developments such as amendment, dismissal, or summary judgment. Information gained at such points often clarifies relevant issues, which may warrant adjusting the related legal hold to account for additional or removed issues, claims, defenses, or data sources.

Similar analysis might take place after the close of discovery in light of events such as trial, appeal (provided that the appeal, even if successful, would not increase the scope of discovery), or any other significant but not entirely final resolution. Organizations may also consider disposing of ESI that it collected during the litigation but determined not to be relevant. For example, this can include ESI that was culled based on search criteria that have not been challenged or have been agreed to by opposing counsel, and no future challenge is anticipated.

Comment 1.c. ***When designing and implementing an information disposition program, organizations should consider the obligation to preserve information that is relevant to the subject matter of government inquiries or investigations that are pending or threatened against the organization.***

---

16. *Supra* note 3, at 96.

Treatises often combine discussions regarding preservation obligations in civil litigation and investigations because the general tenets are similar.[17] But preservation obligations can differ, because they are often governed by different statutes, court procedural rules, and case law. For many investigations, organizations that receive subpoenas should engage the investigating authority to determine its preservation obligations; however, the agency's own rules, or lack of clear rules, may place parties in a disadvantaged position.

Further, the stakes for failing to preserve information may be different for government investigations. For example, parties under a federal investigation may be subject to potential penalties for the obstruction of justice,[18] as opposed to the Rule 37(e) "provisions for sanctioning a party who fails to preserve ESI."[19]

The point at which an organization no longer has a preservation obligation related to an investigation also differs from litigation. The duty to preserve normally ends when the investigation is closed and no further action, including subsequent litigation, is reasonably anticipated. In certain instances, it may be difficult to determine whether an investigation has been completed, leading to the potentially difficult decision of whether to contact the government to discuss the status of the inquiry. Such a discussion could lead to confirmation that a preservation obligation no longer exists, but it might also lead to renewed focus on a dormant matter. While it may be difficult

17. *See* David C. Shonka, *Responding to the Government's Civil Investigations*, 15 SEDONA CONF. J. 1, 8 (2014) ("The principles that govern retention in investigations are the same principles that govern retention in civil litigation: parties are to take prompt and reasonable, not herculean, steps to preserve and stop the routine destruction and disposition of relevant materials.").

18. *See* 18 U.S.C. § 1505 (providing for up to five years in prison for obstruction of investigatory proceedings).

19. FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment.

for an organization to determine when an investigation has been completed, some federal agencies allow, through regulation, for the disposition of information relevant to an investigation if the investigation has been dormant for some specified length of time.[20]

Comment 1.d. When designing and implementing an information disposition program, organizations should consider applicable statutory and regulatory obligations to retain information.

Information retention laws and regulations should be a cornerstone of Information Governance policies. Some of these retention requirements apply to specific information, while others require organizations to retain information sufficient to show compliance with some substantive obligation; for example, information sufficient to substantiate expenses that the organization deducts on its tax returns. Both of these broad categories of retention requirements are found in U.S. federal and state statutes, regulations, sub-regulatory authority, foreign laws[21] and regulations, as well as regulations promulgated by nongovernmental regulatory bodies, e.g., the Financial Industry Regulatory Authority (FINRA) in the financial sector. These laws are often enforceable by civil and sometimes criminal penalties.[22]

---

20. *See, e.g.*, 16 C.F.R. § 2.14(c) (Preservation obligations for Federal Trade Commission investigations end upon notice of closing of the investigation or "after a period of twelve months following the last written communication from the Commission staff to the recipient or the recipient's counsel.").

21. While this section focuses on U.S. retention requirements, organizations need to consider retention requirements in all jurisdictions in which they have employees and do business.

22. For example, 29 U.S.C.S. § 216 provides for monetary fees up to $10,000 and potential imprisonment for those who violate Labor Department record keeping requirements. 29 U.S.C.S. § 216(a) (2008).

Some retention requirements apply generally, regardless of the business sector that the organization operates in. For example, many kinds of information about employees are regulated and subject to explicit minimum retention periods or requirements that information be kept available for audit purposes.[23] Other requirements may or may not apply to a specific organization, depending on a number of factors, including: the organization's structure and industry, the nature of the information created by the organization, and the jurisdiction(s) to which the organization is subject. An organization must ensure its compliance with applicable laws by identifying and complying with requirements that may apply to its information.

While the number of legal retention requirements applicable to an organization may differ greatly based on the factors listed above, some common retention requirements apply to most organizations. For example, even small organizations in unregulated industries must comply with federal and state rules related to tax regulations.[24]

Some highly regulated business sectors within the United States must comply with additional retention requirements that are set forth in federal or state statutes, regulations, or sub-

23. For example, job applications, job postings, personnel records, payroll records, reasonable accommodation requests, and immigration records are subject to records requirements under the Americans with Disabilities Act (ADA) of 1990, the Age Discrimination in Employment Act (ADEA) of 1967, Title VII of the Civil Rights Act of 1964, the Fair Labor Standards Act (FLSA) of 1938, and the Immigration Reform and Control Act (IRCA) of 1986. Other employee records may be subject to the Fair Credit Reporting Act (FCRA) of 1969, 15 U.S.C. § 1681 (seven-year reporting period); the Lilly Ledbetter Fair Pay Act of 2009; Employee Retirement Income Security Act (ERISA) of 1974; and Occupational Safety and Health Act (OSHA) of 1970.

24. *See* 26 U.S.C. § 6001; 26 C.F.R. § 1.6001-1.

regulatory guidance. These sectors include financial,[25] energy,[26] and healthcare.[27] For example, healthcare providers are subject to requirements that vary by state, type of provider, age of the patient, and the patient's condition.[28] In addition to those state requirements, the Health Insurance Portability and Accountability Act (HIPAA) imposes a six-year retention period.[29] Like healthcare providers, banks and financial organizations are also subject to broad retention requirements under a number of

25. *See generally* Truth in Savings Act (TISA), 12 U.S.C. ch. 44 (1991); Equal Credit Opportunity Act (ECOA), 15 U.S.C. § 1691 *et seq*. (1974); Electronic Funds Transfer Act, 15 U.S.C. § 1693 *et seq*. (1978); Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act of 1970 (Bank Secrecy Act), 31 U.S.C. § 5311 *et seq*.; Truth in Lending Act (TILA) of 1968 (Regulation Z), 12 C.F.R. § 226; and 2014 Financial Industry Regulatory Authority (FINRA).

26. *See generally* Energy Policy Act of 2005, Pub. L. No. 109-58, 119 Stat. 594; 18 C.F.R. § 35; 18 C.F.R. § 284; 18 C.F.R. §§ 366–369; 18 C.F.R. § 368.3; 18 C.F.R. § 375; 36 C.F.R. § 1236; *General Records Schedules Transmittal 23*, U.S. NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (Sept. 2014), https://www.archives.gov/files/records-mgmt/grs/grs-trs23.pdf; *General Records Schedules Transmittal 24*, U.S. NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (Aug. 2015), https://www.archives.gov/files/records-mgmt/grs/grs-trs24.pdf.

27. 42 C.F.R. § 422.504(d)(2)(iii); 42 C.F.R. § 482.24(b)(1); 45 C.F.R. § 164.316(b)(2); 45 C.F.R. § 164.530. *See generally* 21 C.F.R.; ALA. ADMIN. CODE r. 420-5-7-.13; 10 N.Y.C.R.R. § 405.10; REV. CODE WASH. (ARCW) § 70.41.190.

28. *See, e.g.*, *Individual Access to Medical Records: 50 State Comparison*, HEALTH INFORMATION & THE LAW, http://www.healthinfolaw.org/comparative-analysis/individual-access-medical-records-50-state-comparison (last updated Sept. 24, 2013).

29. Health Insurance Portability and Accountability Act of 1996, 45 C.F.R. § 164.316(b)(2).

regulatory schemes, including the Gramm-Leach-Bliley Act (GLBA) and state statutes.[30]

The Sarbanes-Oxley Act (SOX) imposes different record retention requirements on publicly traded companies as opposed to privately held companies.[31] Its requirements relate to work documents underlying any audit or review, insider dealings, and documents related to government inquiries.[32]

30. *See, e.g.*, Gramm-Leach-Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338 (1999); N.Y. BANKING LAW § 128 (McKinney 2011); ADVISX RISK MANAGEMENT, RECORD RETENTION SCHEDULE FOR BANKS (2018).

31. Sarbanes-Oxley Act of 2002, Pub. L. 107–204 § 802, 116 Stat. 745.

32. *Id*.

Principle 2. When designing and implementing an information disposition program, organizations should identify and manage the risks of over-retention.

Comment 2.a. Information has a lifecycle, including a time when disposal is beneficial.

Like everything else, information has a lifecycle that begins with its creation or receipt and ultimately ends with its disposal. The length of that lifecycle and the course it takes depend on each recipient's use for the information. Thus, the creation of information marks the beginning of its lifecycle for the author, while the receipt of the information marks the beginning for each recipient. The end of the lifecycle depends on the use for the information. And, of course, these uses vary greatly among recipients and among types or categories of information. For example, the useful lifecycle for some types or categories of information varies (e.g., employee contact information is principally useful to most users only for as long as that employee remains with the organization—whether two weeks or 40 years); the utility of other information is transient (e.g., the usefulness of the content of an email may end when it is read or assimilated into larger work); still other information may have a defined life (e.g., information subject to a regulatory disposition requirement); and some information may have permanent value (e.g., information of historical significance).

The lifecycle of information thus depends on the context in which it is created and used. Effective (and defensible) Information Governance programs require organizations to figure out the useful life of all types of information and then set meaningful retention periods for each type. Such decisions should be based on informed business judgments and may include factors other than the immediate "business need" for the information. For example, some information may not be actively used by the

organization for ongoing business operations but may have long-term business benefits (e.g., to safeguard the design plans for certain products or to ensure an orderly transfer of knowledge to successor employees or successor owners of the business).

Information not subject to legal or regulatory obligations should be retained only as long as justified by its operational value to the organization. Determining the operational value of information involves a cost/benefit analysis. The costs at issue are not simply the storage costs to maintain the information but also the risks inherent in retaining the information longer than necessary. This analysis can represent a significant cultural shift in how the organization previously looked at the retention of information. As organizations grapple with the necessary cultural shift toward disposition of stale information, there can be a tendency to overstate the business value of retention, without full consideration of the increased costs and risks associated with retained information. Operational value of information can be evaluated based on its value to: (i) business function and corporate governance; (ii) internal audit and compliance; (iii) potential (but not yet "reasonably anticipated") litigation; and (iv) contract requirements.

1. Business Function and Corporate Governance

Much information has operational value for a relatively brief time; some of it is stale immediately after it is created. Day-to-day business communications and operational documents may only be required for that day. Other documents may be required for years, such as specifications for a long-term project, or active contracts with multi-year terms. Corporate governance documents generally provide permanent value to an organization, as they are foundational. The operational value of information can be ascertained by working with business departments and

custodians who create and use the information and assessing how often various types of information tend to be accessed after they are created.

2. Internal Audit and Compliance

Similar to legal requirements, organizations may create internal compliance programs as part of a corporate governance program. Such policies may require retention of information that exceeds legal requirements, and audits of compliance may require availability of additional supporting documents and information. Such categories of information need to be retained for as long as they are required by the compliance program.

3. Potential (but not yet "reasonably anticipated") Litigation

Beyond preservation requirements for existing or anticipated litigation, some organizations may elect to retain information that is not subject to a preservation requirement but could be valuable in future litigation that is not yet "reasonably anticipated." For example, manufacturers may opt to retain records documenting safety testing of their products, either because experience dictates or industry practices show that in the event they face a lawsuit for an injury, this information could be of value if litigation ensues. Organizations often retain documents related to research and development in case they need to defend a challenge to a patent. Retention based on business needs regarding potential litigation should be tailored to the organization's litigation risk profile and should be carefully balanced against the risks and costs of retaining the information beyond its business function. In general, such information should be retained only for as long as potential litigation is a risk.

4. Contract Requirements

Many organizations are parties to contracts that require retention of information for a specified period and then require disposition. Such arrangements may appear in retainer agreements between parties who exchange proprietary information about their organizations or sensitive private information about their employees and customers.[33]

Comment 2.b. To determine the "right" time for disposal, risks and costs of retention and disposal should be evaluated.

Information that is not subject to a legal, regulatory, or business retention obligation should be disposed of as soon as the cost and risk of retaining the information outweighs the value of retaining the information. Accurately determining information lifecycles and implementing an orderly disposition process are complex undertakings. An organization should know its information, its information systems, and its comfort with various levels of risk. A variety of teams within an organization[34] must collaborate in order to achieve successful

33. Such provisions may also appear in case management orders and protective orders.

34. For example, the Information Technology (IT) team usually focuses on information storage and potentially retrieving inadvertently deleted information. The Information Governance team focuses on enhanced and appropriate information accessibility, information lifecycles, and appropriate disposal at the predetermined end of those lifecycles. The security team is primarily concerned with restricting access to data to only appropriate personnel and preventing breaches. Somewhere in the mix are the lawyers, who may be primarily concerned with the legal compliance of the policies the organization adopts; the stakeholders, who primarily want quick access to the information they need and may not particularly care about where that information ends up; and the directors and managers, who must balance the benefits and risks of whatever course the organization should take. All these

Information Governance design and implementation. Organizations benefit from appropriately disposing of information when it reaches the end of its legally required or functionally useful life. Some of those benefits include: (i) increased productivity and efficiency; (ii) reduced storage costs; (iii) improved legal compliance; (iv) reduced discovery costs and risks; and (v) enhanced data privacy and security benefits.

1. Increased Productivity and Efficiency

To show the waste of resources and lost productivity that results from keeping information beyond its required retention, an organization need only consider the time that individual employees waste in searching their own files for information they have previously prepared or read and stored. Almost anyone who uses a computer regularly can relate to such situations. If these individual experiences are multiplied by the number of employees in an organization who use computers, it is possible to grasp the likely scope of the problem. This waste is an economic loss that has two aspects: first, that which results from the inability to promptly find information when it is needed; and second, that which results from trying to isolate the correct information from the mass of information in the system. The first of these relates to information organization and management; the second relates to records disposition and a failure to dispose of unneeded information.

In addition to the issues presented by individual employees and their own filing and retention habits or processes, similar issues are raised by corporate- or division-level systems that collect and retain information. If allowed to accumulate, the volume of this information can quickly aggregate into petabytes or more. Even for modern computing systems, it takes much more

---

groups need to collaborate when adopting and implementing any Information Governance program and information disposition program.

time to process data when it contains large volumes of unneeded information.[35] Simply, being able to find the right information quickly results in greater efficiency and higher productivity.

2. Reduced Storage Costs

Although storage costs are relatively inexpensive and have for a long time been declining, information is accumulating rapidly, and in some cases exponentially. Moreover, storage costs accrue for the duration of the information storage, whether one year, two years, or indefinitely. To the extent the Information Governance process properly categorizes information, it can be managed efficiently from the beginning to the end of its lifecycle. These efforts reduce ever-increasing and unnecessary storage costs by limiting data growth of systems in use, as well as reducing the burdens of retired legacy systems, from which data retrieval can be expensive.

3. Improved Legal Compliance

In weighing the benefits of an information disposition program, organizations should consider their legal obligations to dispose of information. There are several situations in which an organization may be obligated to dispose of information, such as where the information is subject to (a) statutory or regulatory mandates (e.g., the Federal Trade Commission (FTC) Disposal Rule, the HIPAA Privacy Rule, and the Children's Online Privacy Protection Act (COPPA)[36]); (b) court orders that compel the

35. Large data volumes can greatly impact the performance and user experience with systems—even crippling the system in some circumstances.

36. *See* Children's Online Privacy Protection Act, 16 C.F.R. § 312.10 (1998) (A company is allowed to retain children's personal information "for only as long as is reasonably necessary to fulfill the purpose for which the information was collected." After that, the company must delete it using "reasonable measures to protect against unauthorized access to, or use of, the

destruction of information (e.g., certain protective orders governing discovery information following litigation); and (c) contractual agreements that require the parties to dispose of information at a specified time. Depending on the circumstances, any failure to dispose of information subject to a disposition requirement may result in fines, civil penalties, litigation sanctions, contempt citations, or even damages claims, as well as attendant litigation expenses. These punitive results can be severe.[37]

Organizations should also pay attention to information disposition requirements imposed by foreign law. Although a discussion of global privacy laws and policies is beyond the scope of this Commentary, it is worth noting that some nations take a far more restrictive view about the use of personal information than the United States. For example, privacy has been treated by the European Union (EU) as a fundamental human right for many years. Laws restrict the use of personal information and generally require disposition after its intended use, as exemplified by the General Data Protection Regulation (GDPR), effective in EU countries as of May 2018.[38] Among other things, the

---

information."). On May 31, 2018, the FTC clarified (i) when children's personal information must be deleted, and (ii) how the requirement applies; as well as recommended that covered companies review their information retention policies to ensure they are in compliance. *See* Jared Ho, *Under COPPA, data deletion isn't just a good idea. It's the law.*, FEDERAL TRADE COMMISSION (May 31, 2018), https://www.ftc.gov/news-events/blogs/business-blog/2018/05/under-coppa-data-deletion-isnt-just-good-idea-its-law?utm_source=govdelivery.

37. For example, HIPAA Privacy and Security Rule violations carry maximum civil penalties of $50,000 per violation, with an annual maximum of $1.5 million, and potential criminal penalties including imprisonment. *See* 45 C.F.R. 160.404.

38. *See* 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.

GDPR restricts the use of personal information, heavily regulates its "onward transfer," establishes disposition and breach notification requirements, requires erasure of or the "right to be forgotten" for personal information, and imposes substantial penalties (up to 4% of a firm's global turnover) for violations of the law. Notably, EU regulators assert that the law has extraterritorial effect, which could mean an organization that properly collects information in the EU and transfers it to the United States may be liable in the EU for losses occurring in the United States, even if the losses are caused by a later recipient of the information. While the scope and reach of the GDPR (and other nations' similar privacy laws) are at this time not firmly settled, organizations may wish to consider the possibilities when crafting information disposition programs.

4. Reduced Discovery Costs and Risks

While a major goal of the 2015 amendments to the Federal Rules of Civil Procedure was to address serious problems associated with the impact of the expanding volume of electronically stored information in civil discovery,[39] over-retention and improper or ineffective disposition efforts still pose a significant risk and drive up discovery costs. The more information an organization maintains and the longer it is retained, the more it will cost to identify, preserve, search, and produce that information in the event of litigation, investigation, or any other

(L 119/1), *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN [hereinafter GDPR]. *See also* Article 29 of Directive 95/46/EC Data Protection Working Party, *available at* https://iapp.org/resources/article/all-of-the-article-29-working-party-guidelines-opinions-and-documents/.

39. *See* JOHN G. ROBERTS, JR., 2015 YEAR-END REPORT ON THE FEDERAL JUDICIARY 5 (Dec. 31, 2015), https://www.supremecourt.gov/publicinfo/year-end/2015year-endreport.pdf.

instance of compulsory process.[40] Also, if an organization does not properly account for preservation requirements in its disposition processes for systems subject to automatic deletion, the organization may be exposed to litigation sanctions or other penalties.

a. Likelihood and Size of Potential Discovery

When conducting a discovery[41] response risk analysis in the context of information disposition, an organization should start by reviewing its overarching risk portfolio. It should assess the nature of its business, the types of information maintained, and its litigation/investigation/audit history to predict the likelihood of various types and costs of future discovery responses, and the types of information affected by those instances. This analysis should help the organization identify information types most likely to be subject to discovery and structure disposition practices accordingly.

For example, consider a small online cloud-based service provider. The organization does not have a physical product, and its product liability exposure is low. It has a small workforce, so there is a risk of employment litigation, but no risk of large class action employment lawsuits. Based upon industry experience for similarly sized organizations, the main litigation risk is likely to be in contract or intellectual property disputes. Therefore, when determining how litigation risk impacts its disposition practices, the first priority could be information

40. *E.g.*, third-party subpoena, civil investigative demand, regulator request, or audit.

41. The discovery process can involve litigation as well as other compulsory processes, such as a subpoena from a government agency or from a litigating party.

relevant to breach of contract and intellectual property litigation, including but not limited to trade secret claims.

Consider also a small technology company in the business of creating mobile healthcare apps with a dual purpose: (i) serving the individual users by providing general information and allowing them to track their personal health trends through individual data input; and (ii) using that input to generate big data in order to identify statistically significant trends, in turn serving the individual users as well as the various healthcare providers invested in the company. This company has the same considerations as the cloud-based service provider referenced above, but also has a variety of additional data privacy and security concerns because the end users enter personal information into the mobile apps. Other concerns might include investigations by state and federal agencies in the healthcare, digital privacy, and security realms. These additional concerns should be considered when structuring a comprehensive information disposition policy and the procedures for implementing the policy, including cessation of routine disposition when litigation, investigation, audit, or other compulsory process instances arise.

b. Potential Costs of Discovery, Given Data Volumes and Types

While the nature and scope of information that must be preserved when discovery instances arise is case-specific, making it impossible to calculate the exact costs related to any such circumstance, studies have analyzed typical discovery costs from preservation through document production.[42] These studies

42. *See, e.g.*, William H.J. Hubbard, *Preservation Costs Survey Final Report*, ELECTRONIC DISCOVERY LAW (Feb. 18, 2014), https://www.ediscoverylaw.com/files/2014/02/Hubbard-Preservation_Costs_Survey_Final_Report.pdf; Nicholas M. Pace & Laura Zakaras, *Where the Money Goes:*

may help organizations conduct informed risk assessments as discussed above, as they indicate that preservation and production costs (internal and actual out-of-pocket) may be managed by better disposition practices. Such cost reductions may include:

(1) less cost to track down information sources that may contain relevant information;

(2) less cost searching for and analyzing old and inactive legacy information sources to determine whether they contain relevant information;

(3) less cost implementing and monitoring preservation obligations;

(4) a smaller volume of information to collect and process into review-ready format;

(5) less time and effort spent reviewing documents; and

(6) fewer documents to produce.

Ever-developing eDiscovery technology, such as Technology Assisted Review (TAR), may help to defray costs, but that does not serve as a substitute for a comprehensive information disposition policy. First, reduction elements 1–4 above are not affected by use of this type of technology. Second, many cases and investigations are not suitable for use of advanced technologies because the matter is simply too small to justify the cost but may nonetheless consume significant discovery resources. Third, machine identification of relevant documents generally

---

Understanding Litigant Expenditures for Producing Electronic Discovery, RAND INSTITUTE FOR CIVIL JUSTICE (2012), https://www.rand.org/pubs/monographs/MG1208.readonline.html.

becomes more effective and efficient as the percentage of responsive documents increases. Finally, even when TAR is used, other review costs, such as review for privilege and other sensitive information, can still be expensive.

c. Risks Associated with Discovery and Improper Disposal

Organizations should not be sanctioned in litigation for failing to produce information that was properly disposed of before litigation was reasonably anticipated, and an organization should not be found to have obstructed justice for failing to produce information properly disposed of before an investigation commenced. In *Solo v. United Parcel Service Co.*, the producing party had already disposed of information sought in discovery by deleting it from its active information location. While the information could have been produced from backup tapes, the court found that a "valid business reason" existed for the deletion and did not require "extraordinarily burdensome" production of the information.[43]

Counsel should actively engage their client in a discussion about the creation and implementation of an Information Governance program and, in particular, information disposition activities, because those may affect how the organization complies with its discovery obligations. For example, pursuant to Rule 26(g)(1) of the Federal Rules of Civil Procedure, an attorney who signs a discovery response certifies that she has made a reasonable effort to assure that the client has provided all available

43. 2017 WL 85832 (E.D. Mich. Jan. 17, 2017); *cf.* United States *ex rel.* Guardiola v. Renown Health, No. 3:12–cv–00295–LRH–VPC, 2015 WL 5056726 (D. Nev. Aug. 25, 2015) (finding a party's deliberate reliance on disaster recovery tapes for preservation reflected failure to adopt "a sensible email retention policy," so the organization could not be excused from its large burden of compliance).

documents that are responsive to the discovery demand.[44] If the certification violates the rule "without substantial justification," under Rule 26(g)(3) the court "must impose an appropriate sanction on the signer, the party on whose behalf the signer was acting, or both." Therefore, the risk of sanctions for improper response to a request for production extends to counsel who make such representations, their clients, or both.

5. Enhanced Data Privacy and Security Benefits

An organization must be concerned about the security of its information, and particularly its commercial, financial, employee, and proprietary information, no matter its age or format. Proper, timely, and routine disposition yields less information. It is cheaper and easier to protect less information than more. In the event of a loss or breach, the cost of information recovery and the burden of notifying interested parties decrease when the volume of information lost is smaller and the sensitivity of compromised data is known.

Indeed, a security breach[45] can cause substantial harm for any organization. According to a 2018 study sponsored by Raytheon and conducted by the Ponemon Institute, the average cost

---

44. FED. R. CIV. P. 26(g) advisory committee's note to 1983 amendment.

45. While this section focuses on information breach, organizations face non-breach security risks as well. Most state information breach statutes cover the unauthorized access or acquisition of personal information ("PI"). *See, e.g.*, CAL. CIV. CODE 1798.82; MASS. GEN. LAWS ch. 93H; TENN. CODE ANN. § 47-18-2107. If information is compromised, but no PI is acquired by an unauthorized person, there might not be a "breach," but the security has still been affected. For example, if an organization's information is attacked in a denial-of-service attack, the information may not have been "breached" under most statutory definitions, but the organization's information security has been compromised nonetheless, potentially yielding a variety of business risks and costs.

of a single information breach was roughly $4 million.[46] The average cost paid for each lost or stolen record containing sensitive or confidential information was $148 per record.[47] Cost components include: (i) detection and escalation;[48] (ii) notification;[49] (iii) post data breach response;[50] and (iv) lost business.[51] These costs correlate to the volume of information breached—the more information lost, the greater the attendant costs.[52] The costs and risks of a breach vary by industry.[53] Because of additional privacy and security requirements, heavily regulated industries such as healthcare and finance[54] have information-breach costs well above the $148-per-record average.[55] In addition, a mega breach or a breach of more than 1 million

46. PONEMON INST. LLC, 2018 COST OF DATA BREACH STUDY: GLOBAL OVERVIEW 1 (July 2018), https://www.ibm.com/security/data-breach [hereinafter PONEMON STUDY].

47. *Id*.

48. *Id.* at 16.

49. *Id*.

50. *Id.*

51. *Id*.

52. *Id.* at 17.

53. *Id.* at 2. *See also* VERIZON, 2016 DATA BREACH INVESTIGATIONS REPORT 3–4 (2016), http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf.

54. For example, recall the breaches at Target and BJ's Wholesale. *See, e.g.*, Peter Cooney & Supriya Kurane, *Target agrees to pay $10 million to settle lawsuit from information breach*, REUTERS (Mar. 18, 2015), https://www.reuters.com/article/us-target-settlement/target-agrees-to-pay-10-million-to-settle-lawsuit-from-data-breach-idUSKBN0MF04K20150319; *In re* BJ's Wholesale Club, FEDERAL TRADE COMMISSION (Sept. 23, 2005), https://www.ftc.gov/enforcement/cases-proceedings/042-3160/bjs-wholesale-club-inc-matter.

55. PONEMON STUDY, *supra* note 46 at 18.

comprised records may well exceed the $148-per-record average.[56] Organizations operating in the European Union may face similarly heightened information privacy laws, as well as the related heightened risks and costs.[57]

For these reasons, organizations have a strong incentive to limit information-breach exposure by reducing the amount of information retained and employing secure and defensible disposition practices. Organizations with less data can more easily protect their data at less cost. Regulatory agencies are now recommending that organizations, as part of their cybersecurity program, have policies for the secure disposal of information that is not required to be retained by law or regulation.[58] The FTC also recommends that organizations consider data minimization (i.e., limiting the collection of consumer data, and retaining that information only for a set period of time, and not indefinitely) to reduce the attractiveness of those repositories to data thieves, the harm done to consumers when breach occurs, and the risk of use of the data in ways not consistent with its intended use.[59]

Disposition practices should protect against a variety of potential security breach incidents, including, but not limited to, malicious and targeted external cyberattacks, phishing attacks,

---

56. *Id*. at 40.

57. *GDPR Key Changes*, EU GENERAL DATA PROTECTION REGULATION, https://www.eugdpr.org/key-changes.html (last visited Dec. 27, 2018).

58. *See* NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES, 23 N.Y.C.R.R. § 500 (2017), Section 500.06 Audit Trail and Section 500.13 Limitations on Data Retention (requirements for audit trails and annual compliance reports by Chief Information Security Officer).

59. *See* FTC STAFF REPORT, INTERNET OF THINGS, at iv (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

malware, social engineering, employee error, unique vulnerabilities of legacy storage systems that are not updated with security patches, and malicious actions by insiders.[60] Therefore, when developing a secure information disposition plan, organizations should not only focus on the physical destruction of hard-copy records and computer hardware, but also pay particular attention to how information is stored, transferred, and ultimately destroyed. This includes in-house systems as well as storage and other services provided by third parties and cloud service providers. As more organizations move all or part of their information infrastructure offsite or into the cloud, the number of possible information breach points increase. When instituting an information disposition plan, an organization should make sure third parties, including cloud service providers, who store or have access to the organization's information also comply with its disposition plan. This involves negotiating for appropriate disposition and security language in contracts and auditing/confirming that if the organization disposes of information based on its Information Governance policy, a third party will not be holding onto a copy of that information, unbeknownst to the organization.

60. *See* VERIZON, *supra* note 53, at 7–8, 17.

Principle 3. Disposition should be based on Information Governance policies that reflect and harmonize with an organization's information, technological capabilities, and objectives.

Comment 3.a. To create effective information disposition policies, organizations should establish core components of an Information Governance program, which should reflect what information it has, when it can be disposed of, how it is stored, and who owns it.

First, the organization should establish at least the following Information Governance components, which reflect what information it has and how processes apply to that information:

1. Classification

The "what" of the process: An organization should know what types of information are stored before determining appropriate retention periods and procedures. Defining information categories into a taxonomy is a prerequisite to organizing information according to the information that they contain. Category definitions need to balance the ease of use of broadly defined records categories against different needs that could be addressed through narrowly defined records. Categories can be defined based on criteria such as the content of the documents, the business group or employee that created them, where the records are stored, and the type of files.

2. Retention Periods

The "when" of the process: Retention periods should define how long each classification of records should be retained and when it should be eligible for disposition. Historically, many

organizations created only minimum periods for records retention, yet did not specify whether information should be disposed of after the retention period. Retention periods can be based on criteria such as date created, last date accessed, and a set passage of time after an event (e.g., a product release, a contract expiration, or departure of an employee).

Without retention schedules for different categories of data, organizations often can only dispose of information that is older than a single maximum retention period that is long enough that it can be applied to all information. While better than nothing, this likely results in massive over-retention and failure to realize many benefits of an effective information disposition policy.

3. Knowledge of IT Infrastructure

The "how" of the process: An organization's Information Technology (IT) infrastructure dictates what mechanisms are available to delete information. Disposition processes depend on where information and copies of information reside, what options exist to preserve and delete it, and whether deletion can or should be automated. If the Information Governance team determines that existing IT infrastructure does not support desired processes, the organization will need to consider updating its available technology.

4. Ownership

The "who" of the process: As described below, every organization needs personnel for documentation, oversight, and maintenance of information disposition as part of the Information Governance program. Designated personnel can provide oversight, help identify potential risks, provide flexibility should objectives change, and may provide valuable metrics regarding performance and efficiency.

Comment 3.b. Organizations should understand their technological capabilities and define their information objectives in the context of those capabilities.

To create a successful disposition policy, organizations should define their information objectives. In addition, they should assess their technological capabilities, so they can make decisions about their policies that reflect those circumstances.

Where the available technology limits the achievability of information objectives, the organization should decide whether to revise the objectives, update the technology, or both. Technological capabilities affect key decisions when designing a disposition program, such as the possibility of automated records management, how broadly to define records categories, and how policies will be applied to records.

1. Automated Records Management

Automation of ongoing retention and disposition policies may create a more reliable and consistent process than reliance on employees' manual efforts. Therefore, organizations may evaluate their existing information management technologies and consider new technologies to automatically retain, delete, preserve, and archive information, and to facilitate searching.[61]

Selection of records management tools should reflect business needs, litigation portfolio, information volume, and IT infrastructure. An organization should maintain documentation of how each information management tool is used to comply with its information processes.

61. Organizations that automatically delete or alter records may need to suspend those processes if the information becomes subject to a legal hold.

2. Records Categories

There are many factors to consider in organizing records. In deciding which type of classification system to use, the organization should assess relative risks and benefits. Granular classification systems enable precise document control, make retrieval of needed information easier, and minimize the risk that the organization will accumulate records that raise liability concerns. Conversely, big-bucket classification systems will be easier to understand (increasing the likelihood of compliance) and administer, but increase the risk associated with the accumulation of unwanted and useless records.

3. Policies for Different Groups

Information disposition policies can be implemented uniformly across an entire organization, or they can be applied differently to different groups, such as offices, departments, or job functions. When making these decisions, the organization should consider what information is stored by each of these groups and how that information tends to flow within the organization.

4. Location of Records

In some cases, organizations may use location to guide disposition decisions, either because a data source is configured to store a certain type of information (e.g., email servers or voicemail), or because employees have been directed to store a certain category of information in a specific location (e.g., all marketing records are stored in a specific shared network folder).

For example, an organization may decide to automatically delete all email on its email server that is over 60 days old, as long as it implements a process to move or copy to other locations emails or attachments with content requiring retention or preservation beyond 60 days. In this example, because there is

a process in place to move records for longer-term storage, the organization can use the email server location to guide disposition on the remainder of the email. In other cases, location should not be used to guide disposition.

5. Legal Hold

An organization must determine whether and how it will continue with its information disposition policies when implementing a legal hold and how it will return to its disposition procedures when the hold is lifted. When implementing a legal hold, an organization's options could include: (i) suspend deletion for the entire organization, or part of the organization; (ii) suspend deletion for information from specific employees; or (iii) continue all deletion but find an alternative way to effectively segregate and preserve relevant information. The cost of this decision may have a wide-ranging effect on the organization.[62] At one end, the cost of suspending all disposition may be minimal; but the cost resulting from excessive accumulation of unnecessary information may be substantial. At the other end, the need to carefully tailor preservation efforts and take extra steps to save only the most relevant information will likely make the cost of complying with the legal hold more expensive; but the overall information disposition program will continue unhindered.

The approach selected will also affect how the organization will return to its disposition program when a legal hold is lifted. The approach will want to ensure that preserved information that is now eligible for disposition will be deleted; while information still within its retention period (or on another legal hold) can be retained for the duration of that period, and then deleted. The organization will benefit if its disposition program includes

62. For example, the organization might move relevant emails into an archive folder before an auto-delete function disposes of them.

a process for dealing systematically with information no longer subject to legal holds.

As a practical matter, organizations should incorporate legal hold assessment into their disposition policies. Assessment actions could include: (i) instituting a procedure that notifies IT and suspends automatic deletion on relevant custodian and production systems as soon as the organization is aware of the preservation obligation; or (ii) incorporating preservation checks into the disposition process, giving users the ability to confirm that information is not subject to a preservation obligation before it is destroyed.

6. Disposition by Business Partners, Contractors, Vendors, and Cloud Services

Information disposition polices could be viewed as ineffective if a third party continues to hold copies of an organization's information past its established retention period. Whenever organizations plan to exchange information with outside providers or partners, they should predetermine the degree of control they maintain over their own information after these exchanges. To the extent possible, they should ensure continued control to implement retention and deletion policies. Third parties should be vetted to determine whether they can comply with the organization's requirements for preserving and disposing of its information. The organization should ensure it maintains the control it needs through its third-party contracts. When terms of service govern the relationship, such as with a cloud information service, those terms should be monitored for periodic changes.

Many cloud service providers are in business to provide convenient storage for their customers and have no particular understanding of an organization's records management practices

and retention or disposition practices.[63] Organizations should carefully review cloud service contracts before entering into them. Whenever possible, they should choose providers who will support the organization's Information Governance policies.[64]

7. Backups and Disaster Recovery Systems

Business continuity and disaster-recovery systems, including backup tapes,[65] pose the potential for significant burden and delay in discovery. While case law and The Sedona Conference support the concept that backup tape rotation cycles do not have to be suspended in anticipation of the typical litigation,[66] they may be subject to preservation and become a source for production if they contain relevant information that is not

63. *See* ARMA INTERNATIONAL, GUIDELINE FOR OUTSOURCING RECORDS STORAGE TO THE CLOUD (2010).

64. If that is not possible, an organization may consider the feasibility of encrypting information before it is stored in the cloud, and then disposing of the decryption keys at appropriate times, thus achieving "virtual" if not actual disposition. This alternative is not an ideal solution, however. For a further discussion of encryption, *see* The Sedona Conference, *Commentary on Privacy and Information Security: Principles and Guidelines for Lawyers, Law Firms, and Other Legal Service Providers*, 17 SEDONA CONF. J. 1, 28–33 (2016) [hereinafter *Commentary on Privacy and Information Security*].

65. While more and more companies are moving from tape to disk or cloud-based solutions, the discovery issues that tapes raise can hold true for other types of recovery systems, regardless of medium.

66. *See* Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 218 (S.D.N.Y. 2003) ("*Zubulake IV*") (As a general rule, a "litigation hold does not apply to inaccessible backup tapes" which "may continue to be recycled."). *See also The Sedona Principles, Third Edition, supra* note 3, at 113, Principle 5, Cmt. 5.h. ("Absent good cause, preservation obligations should not extend to disaster recovery backup tapes created in the ordinary course of business.").

otherwise available, are reasonably accessible, and are proportional to the needs of the case.[67]

As with other forms of information storage, the longer an organization maintains secondary copies of information as part of its backup or disaster-recovery process, the greater the risk that the information will need to be preserved, searched in future litigation, or subject to a security breach. Searching for information takes time and resources, and searching for information in a difficult-to-access system such as backup tapes compounds that burden. An effective way to lower the risk of unique information residing on backups is to use short rotation cycles for backups. Backup rotation cycles (both tape and virtual backups) should be no longer than is necessary to ensure business continuity. Moreover, information storage policies, procedures, and systems should be designed such that business-continuity and disaster-recovery systems can be used only in the event of a system failure to ensure the availability of business-critical information, and not to recover information accidentally deleted in the ordinary course of business.

8. Enforcement

Monitoring compliance is key to the success of an Information Governance program. An audit process is

---

67. *See, e.g.*, Pension Comm. of the Univ. of Montreal Pension Plan. v. Banc of Am. Sec., LLC, 685 F. Supp. 2d 456, 479 n.99 (S.D.N.Y. 2010) (abrogated on other grounds):

> A cautionary note with respect to backup tapes is warranted. I am not requiring that *all* backup tapes must be preserved. Rather, if such tapes are the *sole* source of relevant information (*e.g.*, the active files of key players are no longer available), then such backup tapes should be segregated and preserved. When accessible information satisfies the requirement to search for and produce relevant information, there is no need to save or search backup tapes.

recommended to assess whether records are being managed as anticipated and employees are following policies. For example, an organization may periodically report on information volume metrics, sample certain information sources, and interview business operations employees regarding document management practices. When noncompliance or weaknesses in established policies are discovered, such issues should be appropriately addressed. The policy should state what methods will be used for auditing, who has enforcement authority, and what steps (including penalties) the organization should take to address noncompliance.

While an organization is not legally required to document its information disposition processes and events, documentation can support enforcement and facilitate auditing of whether information has been deleted.[68] For example, policies can describe how legal holds are implemented, including use of any legal hold software. Any significant ad hoc deletion events, such as a "cleanup" event or information destruction by a third party, may be recorded in a disposition log. Documentation of audit procedures, and results of audits, may strengthen the credibility of an organization's claims that it follows its written policies. Similarly, employee training in compliance with Information Governance policies may provide key evidence supporting the

68. For example, if relevant information is no longer available when litigation arises, documentation of information disposition policies and practices could be used to demonstrate that the information was properly deleted, as well as the timing of the deletion. In the event of alleged spoliation, courts may look to policies and procedures for retention and preservation to determine the culpability of a party. *See* Barnett v. Deere & Co., No. 2:15-CV-2-KS-MTP, 2016 WL 4544052 (S.D. Miss. Aug. 31, 2016) (denying sanctions where lawnmower manufacturer's destruction of safety information occurred pursuant to its records policy and before plaintiff's injury, even though defendant had a "'long history of litigating rollover claims'").

defensibility of an organization's information disposition and preservation policies and procedures.

9. Maintenance

Organizations should periodically reassess their information, technology, and objectives, and update their Information Governance programs to address changing circumstances related to disposition. To stay current, organizations should conduct regular reviews of legal, operational, and technological developments that may concern their Information Governance program. Organizations may also uncover gaps in their intended procedures through the audit process. To keep up with evolving needs, organizations may need to update disposition policies, disposal procedures, or adopted technologies.[69]

In addition to regularly occurring reviews, organizations should identify events that may lead to ad hoc reviews designed to maintain or improve information disposition. For example, before new technologies are deployed, they should be subject to an onboarding process that determines whether they are compatible with the existing Information Governance program.[70]

69. Consider how email, instant messaging, and, most recently, team collaboration tools (e.g., Slack) brought with them unique Information Governance challenges.

70. Specifically, new applications can be evaluated to determine whether: (i) the new applications support automatic disposal; (ii) the disposed-of information could still be recovered; and (iii) there is a process for preserving information if subject to a legal hold. This assessment should occur whether deployed within the organization or hosted by a third party.

III. INFORMATION DISPOSITION CHALLENGES

While information disposition is important and increasingly necessary for organizations, its practice is not always straightforward. Information disposition can create challenges especially in the following areas.

A. Unstructured Information

Even for organizations that have implemented sound document retention and information disposition policies and procedures, unstructured information presents difficult challenges. Unstructured information often predates the implementation of current document management processes. While new information may be created and organized in a way that enables the organization to manage it through its lifecycle, unstructured information, by definition, lacks structure, so it is much more difficult to manage. Media and format obsolescence with legacy systems can create access problems, along with increased discovery costs due to missing hardware, lapsed software licenses, or software that does not work on current operating systems. An organization should conduct a due diligence review to identify all active and inactive legacy information sources, determine the information contained in them, and assess what information needs to be retained and what can be deleted.

Related data challenges may also include dealing with inactive information sources, as described in The Sedona Conference *Commentary on Inactive Information Sources*. Inactive data sources include: (i) data that is orphaned, for which no one in the organization is able to provide insight on its content or historical use; (ii) legacy data, which is no longer compatible with the organization's systems or programs; and (iii) dormant data, which is no longer used or accessed. As with all information,

inactive information should be disposed of when it no longer meets legal retention requirements or business needs.[71]

In some cases, organizations will not know whether a source of inactive information is subject to retention requirements. In such cases, the organization should consider the potential costs of identifying information subject to retention, the likelihood that the source contains such information subject to retention, and the potential importance of such information to the organization. This analysis may involve interviewing employees who may have knowledge of the information, reviewing documentation regarding the source, or performing statistical sampling.[72]

B. Mergers and Acquisitions

Mergers and acquisitions can result in the acquisition of another organization's data policies and practices, including record retention plans (or lack thereof). The impact on the original organization's record retention policies and procedures can be significant and complicated. Acquisition of an organization with poor or ineffective Information Governance policies can create significant risk until strong processes can be applied to the information. The acquiring entity should already have its own Information Governance processes in place, but it will need to assess whether those processes are a good fit for the information from the acquired entity. Organizational knowledge of that information may be lost if employees leave, creating

71. The Sedona Conference, *Commentary on Inactive Information Sources*, THE SEDONA CONFERENCE (July 2009 Public Comment Version), https://thesedonaconference.org/publication/Commentary_on_Inactive_Information_Sources.

72. *See, e.g.*, Solo v. United Parcel Service Co., No. 14-12719, 2017 WL 85832 (E.D. Mich. Jan. 10, 2017) (allowing possibility of sampling relevant data in context of a burdensome discovery request).

additional risk and making assessment of the information difficult.[73] Merging the two entities' document retention policies and practices should be done carefully and deliberately, and should ideally involve a collaborative approach, including personnel from both entities.

C. Departed, Separated, or Former Employees

A retention policy should outline steps for managing information of employees who leave the organization. Former employees' records should generally be retained in accordance with records retention policies but may need to be held longer, depending on the circumstances of the departure. For example, an organization may retain information from employees who present a higher risk of litigation, such as terminated employees, longer than other employees. Whenever possible, an employee's exit interview should include questions to ensure that the organization has made a good-faith effort to identify and access important operational and legal records, and that the employee will no longer have access to sensitive business information.

In the event of a legal hold, an organization may need to preserve all of a former employee custodian's information to comply with its preservation obligations, as the individual is not available to directly manage the information in compliance with the preservation notice. This can lead to significant over-

73. In *Phoenix Four, Inc. v. Strategic Res. Corp.*, the court, though declining to issue an adverse inference, determined that the elements of an adverse inference instruction were satisfied when unproduced information was found on the dissolved organization-defendant's server during a routine repair call. The court made this determination despite the defendant's explanation that the ignorance of the existence of the information was due in part to the post-dissolution departure of defendant's technical specialist. No. 05-4837, 2006 WL 1409413 (S.D.N.Y. May 23, 2006).

retention, especially in organizations with large litigation portfolios, where one legal hold can overlap with the next.

D. Shared File Sites

Shared file areas such as network departmental folders or SharePoint often become unwieldy when there is no software available or configured to connect information to retention schedule categories.

E. Personally Identifiable Information

Personally Identifiable Information ("PII") may have specific requirements based on privacy laws. Privacy laws may specify how long information must be retained, what and when information must be deleted, and compliant methods of deletion.

F. Law Firms, eDiscovery Vendors, and Adversaries

Outside counsel, legal service providers, and other parties to litigation may also possess copies of an organization's information produced during discovery in legal matters.[74] While counsel have an ethical duty to protect their client's confidences, eventual disposition of client information should be defined by agreement. Depending on the nature of the relationship and the matter, an organization may have different requirements for how long its information should be retained after a matter is closed. Organizations should notify outside counsel of those specific retention requirements and ensure that counsel are able to and do comply, at the appropriate time, with the requirement to dispose of such information. Work-product and attorney-client communications are distinct from preexisting organization

74. For an in-depth discussion of information security, privacy, and retention considerations for third-party legal service providers, *see Commentary on Privacy and Information Security*, *supra* note 64.

business information and may therefore have different retention requirements.

As part of litigation, an organization may also provide copies of its information to other legal service providers, such as eDiscovery and trial presentation providers, and to other parties in its matters. The organization and its attorneys should consider whether a stipulation, confidentiality agreement, or protective order can help protect the information from further disclosure and ensure its proper disposition at the end of the case. For example, the organization may want to limit access to its information to the adversary's outside counsel and their consultants and experts, but bar access by in-house counsel. Or, if in-house counsel does gain access to the documents, at least limit access to prevent other individuals in the organization who do not need access to this information from seeing it. Also, a protective order might reasonably require that all persons who get copies of the information, including counsel, experts, and anyone else, be required to certify at the end of the case that all copies of the information in question have been returned to the organization or destroyed. Still, other provisions may prohibit the use of the information in any other litigation, or its production to other parties in discovery—at least without notice to the producing party. Provisions such as these may be the organization's best chance to make sure its business information does not fall into the hands of competitors or other adversaries after litigation.

G. In-House Legal Departments

In-house legal departments may encounter similar problems as outside counsel, as described above, because they often receive copies of information from elsewhere in the organization. Robust tracking and classification systems are key to addressing this issue.

H. Hoarders

Audits should be conducted regularly to identify users who are in violation of the Information Governance program. This could include users who routinely back up email to their computer, use an external storage device (it is best to forbid this outside of special permission), or use shared network storage to save stale content. Ideally, an organization's information disposition system will identify content by date last modified, date last accessed, date created, and file type; each of these metadata fields may be used to monitor for potential violators of the Information Governance program.

I. Regulations

Organizations should make certain that their information management processes and Information Governance policies and procedures consider all applicable regulations, including "approved but not yet adopted" regulations (e.g., The GDPR, which was adopted in April 2016 but had a May 25, 2018, enforcement date), as appropriate.

J. Cultural Change and Training

An organization should clearly outline its expectations for compliance with each component of the information lifecycle, including disposition. Disposition of data in particular can be met with resistance by employees who fear they will lose valuable information. Successful program implementation depends on the organization's ability to change employees' existing behavior, which is best achieved when the organization communicates its new expectations to employees in an efficient manner and provides adequate education and training on new policies

and procedures.[75] A successful Information Governance program must have support from the organization's senior management with regard to funding and a commitment to cultural change.

75. For example, implementing an automated records management program should incorporate procedures whereby personnel can designate discrete data for preservation for legal or other organizationally defined reasons. Personnel should be aware of and trained on how to efficiently use these systems.

THE SEDONA CONFERENCE COMMENTARY ON DATA PRIVACY AND SECURITY ISSUES IN MERGERS & ACQUISITIONS PRACTICE

A Project of The Sedona Conference Working Group on Data Security and Privacy Liability (WG11)

Author:

The Sedona Conference

Drafting Team Leader:

Sara Romine

Drafting Team:

Jay Brudz
Craig Carpenter
Cordero Delgadillo
Charlyn Ho
Daniel Meyers
Dana Post
John J. Rosenthal
Jeffrey C. Sharer
James A. Sherer

Steering Committee Liaison:

David Moncure

Staff Editors:

David Lumia
Michael Pomarico

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference's Working Group 11. They do not necessarily represent the views of any of the individual participants or their

employers, clients, or any organizations to which they may 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 Data Privacy and Security Issues in Mergers & Acquisitions Practice,* 20 SEDONA CONF. J. 233 (2019).

PREFACE

Welcome to the final, May 2019 version of The Sedona Conference *Commentary on Data Privacy and Security Issues in Mergers & Acquisitions Practice*, a project of The Sedona Conference Working Group 11 on Data Security and Privacy Liability (WG11). This final version of the *Commentary* supersedes the public comment version published in May 2018. 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, and intellectual property rights. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

The Sedona Conference acknowledges Drafting Team Leader Sara Romine for her leadership and commitment to the project. We also thank drafting team members Jay Brudz, Craig Carpenter, Cordero Delgadillo, Charlyn Ho, Daniel Meyers, Dana Post, John Rosenthal, Jeff Sharer, and James Sherer for their efforts and commitments in time and attention to this project. We thank Anand Shah and Maria Garrett for their assistance. Finally, we thank David Moncure for his guidance and input as the WG11 Steering Committee Liaison to the drafting team.

In addition to the drafters, this nonpartisan, consensus-based publication represents the collective effort of other members of WG11 who reviewed, commented on, and proposed edits to early drafts that were circulated for feedback from the Working Group membership. Other members provided feedback at WG11 annual and midyear meetings where drafts of this *Commentary* were the subject of dialogue. The publication was also subject to a period of public comment. On behalf of The Sedona Conference, I thank all of them for their contributions.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG11 and several other Working Groups in the areas of electronic document management and discovery, cross-border discovery and data protection laws, 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
May 2019

FOREWORD

In the ordinary course of business, companies acquire, use, and disseminate vast amounts of data. This data can provide a company with a competitive advantage, be instrumental to a company's day-to-day operations, or serve no tangible purpose at all. For these reasons, the information possessed by a company can have a range of values but be accompanied by varying degrees of risk depending upon the security of the data and whether its use or dissemination triggers any privacy concerns. Consequently, data privacy and security issues must be considered in an acquisition, and can have a significant impact on the value and terms of the deal, including whether or not to acquire certain data as part of the transaction and how to value that data.

Perhaps the most prominent example of the impact that privacy and security issues can have on a deal is Verizon's contemplated acquisition of Yahoo. After Verizon and Yahoo reached an agreement by which Verizon would acquire Yahoo's core internet operations, it was revealed that Yahoo had suffered two large data breaches impacting more than one billion customers.[1] Verizon and Yahoo delayed the acquisition to assess the impact of the data breaches on the terms of the deal, including the purchase price.[2] Ultimately, in response to pressure from Verizon, Yahoo reportedly agreed to lower the purchase price by

1. Greg Roumeliotis & Jessica Toonkel, *Yahoo Under Scrutiny After Latest Hack, Verizon Seeks New Deal Terms*, REUTERS (Dec. 15, 2016, 9:38 A.M.), http://www.reuters.com/article/us-yahoo-cyber-idUSKBN14420S.

2. Thomas Gryta & Deepa Seetharaman, *Verizon Puts Yahoo on Notice After Data Breach*, WALL ST. J. (Oct. 13, 2016, 7:28 P.M.), https://www.wsj.com/articles/verizon-sees-yahoo-data-breach-as-material-to-takeover-1476386718.

approximately $350 million.[3] The Yahoo example demonstrates the significant impact that privacy and security issues can have on a deal. For this reason, the Yahoo deal is referenced at various points in this *Commentary* as an example. These issues, however, are not limited to high profile "mega deals." Privacy and security concerns exist in virtually every deal.

This *Commentary* is intended to provide practical guidance on data privacy and security issues that must be considered in a potential acquisition. In doing so, it approaches these issues from the perspective of the buyer. It is not intended to be exhaustive, but rather to provide a framework for addressing the privacy and security issues that likely will impact a transaction. Although the title of this *Commentary* refers to "Mergers & Acquisitions" (because such terms are almost always used in tandem to describe a particular area of law practice), the *Commentary* focuses exclusively on acquisitions because true corporate statutory mergers of unrelated entities are increasingly rare.

3. Brian Womack, *Verizon Suggested Price Cut of Up to $925 Million for Yahoo Deal*, BLOOMBERG (Mar. 13, 2017, 12:46 P.M.), https://www.bloomberg.com/news/articles/2017-03-13/verizon-suggested-price-cut-of-up-to-925-million-for-yahoo-deal.

TABLE OF CONTENTS

I. INTRODUCTION

"Information is crucial to modern businesses. Information can have great value, but also pose great risk, and its governance should not be an incidental consideration."[4] This is no less true in an acquisition, where the impact of information on the deal is multifaceted. First, the target company or asset has its own (often unique) data privacy and security issues that may affect the inherent value of the target. Second, the security of sensitive information shared during the due-diligence phase must be ensured because of the possibility of data breach. Third, post-deal integration activities—both strategic and logistical—may hinge on data privacy and security issues, forcing the buyer to change its business strategy or even its operations to accommodate unforeseen issues.

This *Commentary* approaches these issues through the lens of the typical "deal framework" and is thus divided into the three basic stages of a transaction: (i) determining the scope of the acquisition; (ii) conducting due diligence; and (iii) closing and post-closing considerations. At the end of each stage, there is a short summary containing the key "takeaway" points. In addition, the *Commentary* aims to give practical demonstrations of those processes, including sufficient background information to demonstrate how the *Commentary*'s proposed guidance will work in the real world. Given this approach, the *Commentary* is not intended to be exhaustive and certainly could not be—the scope of the issues that may arise will necessarily turn on the specifics of a given transaction and the terms negotiated by the buyer and the seller.

It is our hope that the *Commentary* will be of use not only to professionals working on an acquisition, but also to those

4. The Sedona Conference, *Commentary on Information Governance*, 15 SEDONA CONF. J. 125, 130 (2014).

individuals who will work on the post-deal integration of the acquired assets. In an effort to distill the scope of our analysis into a more practical form, we have also appended to this *Commentary* a summary of the categories and types of data implicated in the deal analysis (Appendix A); sample representations and warranties that address privacy and security concerns (Appendix B); and basic due-diligence requests (Appendix C). Of course, this work product is simply a starting point for analysis and will need to be tailored to each specific transaction.

II. STAGE ONE: DETERMINING WHAT THE BUYER WANTS TO ACQUIRE AND NEGOTIATING APPROPRIATE DEAL TERMS

A. Identifying and Assessing the Different Types of Data That Will Be Acquired

Advancements in computer processing have empowered companies to amass and control data at a faster pace, in larger quantities, and of a greater variety. This reality makes the valuation of risks and benefits associated with such data increasingly difficult. Consequently, the context of data (how and where it was created), the content of data (what information it contains), and the rules that may apply to such data (internal and external policies, court decisions, federal laws, state laws, and regulations) can seem overwhelming. Complicating matters, "new" types of data and novel uses of "old" data may lead to the enforcement or application of arcane and ill-suited rules. Likewise, the ability of the buyer to unlock the potential value of the target's data can be greatly impacted by the nature and type of data systems involved. Thus, in an analysis of an impending acquisition, classification of the target's data is vital to calculating its related value and risk.

Any analysis of an impending acquisition should include a data-classification framework to assist the buyer in determining whether to "take it" or "leave it" as it relates to particular types of data. Data governance models frequently use complex data-classification systems. These systems offer value by automating compliance requirements based on classification. Data classification for an acquisition analysis, however, should remain as simple as possible without impeding effectiveness.

At its most basic level, buyers use data classification to answer two threshold questions: (i) what exactly is the data; and (ii) what value, obligations, and risks accompany it? Data classification is not straightforward, and classes of data often

overlap. It is critical for buyers to think through data classification at the outset, determining how differences in types of data and the regulation of that type of data will account for differences in the classification system. Appendix A of this Commentary sets forth and describes the different categories of data that parties to an acquisition may wish to use as a classification starting point. In addition to these categories of data, Appendix A sets forth particular types of data that are subject to certain laws and regulations that require heightened privacy and security practices (and are subject to regulations or industry group best practices that can be binding on industry members or simply provide guidance). After the parties to the transaction categorize the data subject to the transaction, they should determine whether such data categories trigger special protections. Due to the constantly evolving global regulatory landscape governing data privacy and security, the buyer should consider Appendix A as just one resource to consult when assessing the protections and obligations applicable to the relevant data categories.[5]

Determining whether a company complies with its privacy policies is crucial. Costly enforcement actions can result from a company's failure to follow its consumer-facing privacy policies.[6] Parties to an acquisition must also consider the particular

5. Additional resources include The Sedona Conference, *Data Privacy Primer*, 19 SEDONA CONF. J. 273 (2018).

6. Parties should consider: (i) the type of data collected; (ii) how the data is used; (iii) the target company's policies and third-party agreements relating to such information; and (iv) whether the target company complies with its consumer-facing policies. *See, e.g.*, The Sedona Conference, *International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition)*, THE SEDONA CONFERENCE (Jan. 2017), https://thesedonaconference.org/publication/International_Litigation_Principles. In 2014, when Facebook acquired WhatsApp, the Federal Trade Commission and European data protection authorities warned the companies that the parties' failure to abide by WhatsApp's privacy notice would constitute a deceptive act under

treatment of data that enters and exits a country because of export controls[7] and cross-border data protection concerns. Because legal requirements vary at the international, federal, and state levels, analysis requires a data-, industry-, and jurisdiction-specific assessment.

The point of this analysis is to determine the values and risks associated with data that are a necessary part of the acquisition and, for other data, whether to acquire it or leave it behind.

B. The Scope, Ownership, and Transferability of the Data Being Acquired

Fundamentally, a party cannot sell more than it owns. For this reason, after identifying the data that is subject to the acquisition, the parties should specify the extent of the transferor's rights to the data. Ownership may be unclear. Cloud and software-as-a-service (SaaS) storage platforms, employee or customer information in the possession of corporations, and shared intellectual property often preclude up-front ownership analysis. Accordingly, contractual terms, privacy policies, and applicable regulatory regimes should be analyzed to accurately understand and document precisely what rights of ownership or access to relevant data the seller possesses.

Even though the seller has rights to obtain, possess, and use data, the seller may not be able to transfer all of those rights. Buyers must recognize constraints on data transferability, particularly when the deal is structured as an asset sale. Such constraints will often be in the form of pre-existing contractual restrictions found in the seller's existing privacy policies or

---

the Federal Trade Commission Act and European data protection and privacy laws. *See In re: WhatsApp*, ELECTRONIC PRIVACY INFORMATION CENTER, https://epic.org/privacy/internet/ftc/whatsapp/ (last visited May 9, 2019); Agency Information Collection Activities, 80 Fed. Reg. 2423 (Jan. 16, 2015).

7. *See, e.g.*, BIS Export Administration Regulations, 15 C.F.R. §§ 730–774.

contracts. Diligent buyers should extensively review any such policies to avoid any data transferability issues or limitations that may exist following the acquisition.

C. Subjects of Disclosure, Representation, or Warranty

After assessing and determining the data that will be acquired, the buyer should consider the representations and warranties from the seller that the buyer needs to ensure receipt of its anticipated acquisition and to allocate risk appropriately. Some sample representations and warranties are provided in Appendix B. The following are important matters on which the buyer will want to receive representations from the seller.

1. Compliance with Data Privacy Laws, Regulations, Industry Standards, and Privacy Policies

Privacy regimes are comprised of a complex web of intersecting laws, regulations, and industry standards.[8] Historically, buyers spent little time focusing on the seller's record and information management practices and privacy concerns related to the data being sold. Buyers would frequently obtain all of the seller's data "just in case." Notwithstanding the costs associated with storage and retrieval of this data, utilizing these historic practices subjected buyers to unnecessary legal, regulatory, and business risks.

8. For example, a Massachusetts healthcare company that accepts credit card payments may be required to comply with the privacy norms embodied in the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Massachusetts breach notification and information security laws, Payment Card Industry (PCI) standards, and the Federal Trade Commission Act's prohibition against fair or deceptive trade practices. Failure to comply with any of these requirements can result in heavy fines, decreased operational capabilities, and severe reputational and business issues.

While some companies operating within this complex framework have invested the time and resources required for compliance with each applicable norm, others have not. A third party looking to acquire a company—and, in particular, a company that operates in an unfamiliar industry or regulatory environment—faces an uphill battle to understand the applicable privacy regime, let alone measure the target company's compliance with it.

Accordingly, the deal documents should: (i) identify which legal and industry-based privacy norms apply to the target company's business; (ii) identify the contours of the target company's current and prior privacy statements and policies (including any policies that limit the target company's ability to transfer or sell personal information to third parties); and (iii) represent the extent to which the target company is currently in compliance with the two prior points. Additional consideration should also be given to the target company's historical compliance with industry-based privacy norms. Buyers will often require the target company to represent that its business has been in compliance with applicable privacy rules and regulations for a certain look-back period. The parties should also consider whether to include privacy-specific indemnification provisions in the documents to protect the buyer against any variances from the seller's representations. In sum, buyers today are encouraged to vet properly any compliance-related issues throughout the due-diligence process well before closing.

2. Disclosure of Known or Potential Data Compliance-Related Incidents

The representations in the acquisition documents should include disclosures of the target company's known or potential compliance-related incidents, including: (i) contractual violations relating to the use or storage of data; (ii) pending or current investigations relating to data privacy and information

security; and (iii) data-breach incidents or threats, including whether there were any private or regulatory actions taken in response to such incidents. These disclosures can include what actions were taken in response to data-breach incidents in order to comply with state and federal breach notification laws and any related privacy complaints, litigations, enforcement actions, consent decrees, or remediation activities. To the extent an issue is identified during the due-diligence period, the parties may wish to include special indemnities in the purchase agreement to address any associated risks. For additional discussion on indemnities, see Section IV(C).

3. Information Security Representations

Data privacy and information security are related but distinct fields. It is important to consider the inclusion of representations concerning the target company's information security programs and infrastructure. For companies with a robust written information security program, such representations can be accomplished by attaching a copy of the written policy to the acquisition documents and including a representation that the target company is in compliance with the requirements and provisions of that policy.

For companies that lack a pre-existing written information security program, additional due diligence may be required, or the seller may be required to provide a more detailed description of its security apparatus. This description should include the physical, administrative, and technical safeguards the target company has implemented to protect its data from unauthorized access. Those safeguards may include: (i) data access controls; (ii) use of encryption; (iii) Bring Your Own Device (BYOD) or Corporate-Owned Personally Enabled policies; (iv) disaster-recovery and data-backup procedures; (v) corporate training programs; and (vi) the existence of any incident response plans.

4. Cyber Insurance

The parties should also consider whether the target company has insurance policies that provide coverage for the buyer against data privacy or security incidents. This inquiry can be accomplished in the due-diligence process or through representations. If the latter process is chosen, the representation should include coverage limits (per incident and in aggregate) and what third-party services are covered.

5. Export Control

For companies that export goods or services across borders, the parties should consider whether to include: (i) a list of the countries to which the exports occur, and (ii) a representation and warranty that all applicable export licenses have been obtained for each applicable country. These concerns can also be addressed during due diligence as a supplement to or replacement of such representations.

D. Stage One Summary

During the initial stage of the acquisition, the buyer should:

- identify specific types of data to be acquired and assess the information governance requirements and the risks associated therewith;
- determine the scope, ownership, and transferability of the data being acquired, including any contractual or common-law restrictions on the sale or transfer of the data;
- assess the target company's current compliance with any applicable data privacy laws, regulations, industry standards, and the target company's own privacy policies;
- obtain disclosures of any known or potential data compliance-related incidents, including

any data-breach incidents and legal actions taken against the target company;

- procure representations and warranties concerning the target company's information security program and infrastructure, including by appending any applicable policies and obtaining representations that the target company is currently in compliance with all such policies;
- determine the existence of any cyber insurance policies; and
- obtain disclosure of any countries to which the target company provides goods and services, and obtain representations and warranties that all necessary export licenses have been acquired.

III. STAGE TWO: PERFORMING DUE DILIGENCE

A. Data Privacy and Security in Acquisition Due Diligence

A well-informed buyer is more likely to achieve its goals for an acquisition. Accordingly, pre-signing due diligence is an integral part of the deal-making process. The success of the transaction relies upon reducing the risks associated with both the transaction and the post-transaction going concern and justifying the costs paid and strategy envisioned in the transaction.[9]

Traditional due diligence is used to determine the liabilities, efficiencies, and price of a proposed transaction. Due diligence often provides insight into whether the buyer should proceed with a given deal and whether the deal value should be adjusted. A buyer uses the diligence process to determine whether there are any incompatibilities that could not be identified based on public information. Traditional mergers and acquisitions (M&A) diligence typically is useful in identifying "red flags" or unanticipated liabilities not covered by representations and warranties relating to:

- assets (tangible and intangible);
- organization;
- contracts;
- customers;
- employment information;
- environmental issues;
- finances;
- litigation profile;
- suppliers and distributors; and

9. James A. Sherer et al., *Merger and Acquisition Due Diligence: A Proposed Framework to Incorporate Data Privacy, Information Security, e-Discovery, and Information Governance into Due Diligence Practices*, 21 RICH. J.L. & TECH. 5 (2015).

- tax issues.

Recently, data privacy and security have become important subjects of diligence. This trend is driven in significant part by burgeoning legal implications. A changing regulatory landscape has increased the risk associated with unknown data privacy and security practices.[10] Responses to these regulations are complex as well, and many organizations are struggling to keep up. Under such circumstances, buyers may be better served assuming an environment of noncompliance for targets, and therefore working to determine an appropriate risk analysis for post-transaction activities.[11]

Proper data privacy and security diligence can aid in demonstrating the maturity level of the target with respect to: (i) data privacy and security issues; (ii) determining greater cost certainty for the transaction; (iii) identifying integration or migration issues early in the transaction; and (iv) decreasing the buyer's risk.[12]

As discussed in more detail below, data privacy and security diligence in an acquisition should, at a minimum, consider: (i) the type of sensitive information involved; (ii) the location of sensitive information; (iii) the target's current and historic data security and privacy practices; (iv) known vulnerabilities and breaches; and (v) the target's relationship with vendors. This information is imperative for the buyer to be able to understand and assess the risks of liability associated with the target company. This information must be requested and reviewed by someone who understands the business and legal implications stemming from the acquired information. Therefore, the parties should each establish a transaction "quarterback" to serve as the

10. *Id*.

11. *Id*.

12. *Id*.

point person and to coordinate the diligence process, and a diligence team with clear objectives and subject-matter expertise. The proper team is particularly important with respect to data privacy and security diligence, which may fall outside of the expertise of traditional M&A lawyers.

B. Considerations in Conducting Data Privacy and Security Due Diligence

1. Due Diligence on Data Privacy and Security Issues Should Not Run Afoul of Prohibitions on "Gun-Jumping"

Exchanging information prior to the consummation of a transaction is appropriate so the parties may properly structure the deal to ensure they are receiving the benefits of the bargain. Competition laws generally permit the disclosure or exchange of such information, including competitively sensitive information, as part of the due-diligence process. However, the disclosure or exchange of certain information—or using such information to integrate the acquisition prior to closing—can constitute "gun-jumping" in violation of civil or even criminal antitrust enforcement under, for example, Section 1 of the Sherman Act or Section 7A of the Clayton Act. In addition, the Antitrust Division of the Department of Justice has interpreted the Hart-Scot-Rodino (HSR) Act to prohibit an acquirer from exercising "substantial operational control" over an acquired company prior to the expiration of the HSR waiting period.[13] As a general matter, the disclosure or exchange of information relating to data security will generally be judged under the "rule of reason" as opposed to "per se" treatment under a naked

13. *See* Complaint for Equitable Relief and Civil Penalties at 15, United States v. Gemstar-TV Guide Int'l, Inc., No. 1:03 CV000198 (D.D.C. Feb. 6, 2003), ECF No. 1.

anticompetitive restraint.[14] Parties should, therefore, be cognizant that any exchange of information undertaken in conducting due diligence relating to data security issues is designed for that purpose and not unrelated purposes that might, for example, be used as evidence to support a claim of "gun-jumping."

2. Deal Considerations

While all acquisitions would benefit from some level of data privacy and security diligence, there is no one-size-fits-all approach, and the data privacy and security diligence will vary deal to deal. The focus, scope, and significance of the data privacy and security diligence review will depend on a number of factors, including:

- the transaction size and complexity;
- the transaction structure;
- the ongoing obligations of the parties;
- the type of location of any relevant sensitive information;
- cross-border considerations; and
- the industry.

These considerations will likely drive the scope of data privacy and security diligence and are initially analyzed by the buyer or party undertaking the analysis.

(a) Initial Steps

Data privacy and security should be considered in acquisitions for two primary reasons. First, as discussed in more detail in various other sections herein, the buyer should investigate the target's privacy and security practices to analyze the risk and adjust the deal value. Second, both parties have a duty to maintain confidentiality, privacy, and security during the

14. *See* United States v. U.S. Gypsum Co., 438 U.S. 422, 438 (1978).

transaction. This is especially critical during the diligence process, where sensitive information of both parties is accessed and shared.

In light of these privacy and security concerns, prior to starting the diligence process, the parties should execute a nondisclosure agreement (NDA) to establish the terms of data sharing and set forth the restrictions and protections for that information. The NDA should limit the scope of data access and use and describe any additional protections for particularly sensitive or regulated information, such as Personally Identifiable Information (PII), Protected Health Information (PHI), credit card information, or trade secrets.

Once an NDA is negotiated and executed, the buyer will have an opportunity to make specific requests regarding the information it would like to review during diligence. The seller will then attempt to complete the buyer's diligence checklist by providing relevant information and documents. Then, the target will attempt to fill out the checklist and provide the requested materials. Typically, this is done via a traditional or virtual data room (VDR), which can be created by one of the parties, an agent of one of the parties, or a third-party data-room provider. In setting up a VDR for a transaction, the transaction parties should consider the following:

- Who will be responsible for hosting the VDR?
- Who owns the data in the VDR?
- What security measures will apply to the VDR?
- Who is liable for a breach of the VDR?

VDRs can be hosted by the transaction parties (e.g., through a company-run Dropbox or File Transfer Protocol (FTP) site), an agent of one of the parties (e.g., an investment banker or broker), or a third-party VDR provider. If one of the parties is hosting the data room, the parties should make clear who owns the data

and the privacy and security protocols. Typically, each party will own the data it uploads, with access and use subject to the NDA. If a third party is hosting the data, the transaction parties should carefully review their engagement letter or service agreement with the third party and identify the allocation of risk and security protocols and compare these to the costs of the services.

(b) The Virtual Data Room

VDRs have emerged as a technology-based due-diligence tool used to facilitate access for purposes of disclosure and document sharing in M&A transactions. VDRs allow companies to maintain and share critical business information in an online environment, streamlining all stages of the document and communications process. In connection with such transactions, these internet-based document repositories capture, transmit, handle, and store confidential, proprietary, and sensitive information regarding their customers and clients of their customers.

Due to the increased reliance on VDR technology and the amount of sensitive data shared during typical M&A diligence, data security is a primary concern in preparing and using a VDR. Unauthorized access to a VDR could result in widespread, irreparable damage to any number of parties, as well as to the deal itself. Unauthorized access or disclosure of proprietary information caused by a compromised VDR can negatively impact the value of a business, its market share, investor return, and competitive advantage. This is especially true in the context of M&A diligence where data rooms often contain highly confidential information, such as pre-initial-public-offering due-diligence reviews, bankruptcies and restructurings, audits, proprietary intellectual property, employee or customer PII and PHI, and fundraising initiatives. The unauthorized access or disclosure of this type of information can have significant economic

consequences on all parties. Therefore, strong data protection and cyber security practices are essential.

In order to engage a VDR service provider and gain access to its platform, prospective customers enter into contractual arrangements. Companies and their advisors should thoroughly vet their VDR service providers to ensure the VDR is adequately protected throughout the diligence process. The amount of security required could vary depending on the deal considerations, but standard VDR security should address the following:

- strong username and password controls;
- industry-standard encryption options;
- deterrence features, such as watermarking;
- access control, such as view-only;
- lock-down procedures; and
- partitioning and the availability of additional security for highly sensitive information.

Many of these security functionalities within a VDR are referred to collectively as "Information Rights Management" (IRM) tools. Ensuring the VDR selected for a particular transaction has the necessary IRM capabilities should be a threshold inquiry.

Customers that enter into agreements with VDR service providers must be cognizant of the allocation of risk and damage limitations that apply to security-breach situations. VDR agreements often require the customer to bear sole responsibility for monitoring, preventing, and notifying the VDR service provider of unauthorized access.

(c) Beyond the Data Room

Although data privacy and security review is becoming more prevalent in M&A diligence, current diligence practices that attempt to incorporate data privacy and security issues are generally still subject to traditional diligence limitations,

including the lack of context regarding the data being shared in the VDR and often limited access to key personnel. This is further complicated by the significant inconsistencies in how companies deal with data privacy and security due to the lack of a "standard" in this space.

Because of this, and because of the importance of data privacy and security, buyers may request additional diligence beyond the data room. This is particularly prevalent in transactions with highly sensitive information or significant potential liabilities. In such transactions, the buyer may request that the target share the results of its most recent security audits, penetration tests, or other vulnerability assessments, or even undergo independent third-party assessments as part of the diligence process if such information is not available or up to date. The target's willingness to undergo additional assessments will likely depend on the cost of such assessments relative to the value of the transaction and the buyer's negotiating position. Where, for instance, a buyer is permitted to engage in an additional assessment, it must identify the right people within the target to query. Because critical people often leave before an acquisition or asset purchase is finalized, having direct access to these individuals before the transaction is beneficial, as this information will be much more difficult to obtain post-closing. Once the individuals are identified, each of the categories and types of data identified in Appendix A should be explored.

(d) Types of Data

In conducting due diligence, the buyer should obtain a thorough understanding of the types of data maintained by the target, and, in turn, which categories of data the parties intend

to include and exclude from the transaction.[15] This information will help potential buyers understand: (i) the laws applicable to the data; (ii) whether consent is needed to transfer the data (under data protection laws); (iii) the types of security required to protect the data; and (iv) how to integrate the target's digital assets into the buyer's final information technology (IT) infrastructure. The diligence will further allow the buyer to identify and evaluate data protection concerns (and documentation about the way in which they were dealt with) to determine how much of the existing infrastructure and practices can be drawn into the new organization. In addition, diligence on the data types may provide information on how the potential purchaser will be able to access data protected by passwords and data stores with limited access rights. These inquiries may incorporate questions regarding how any data migration will impact the business-continuity procedures of the buyer and may influence the ultimate deal.

(e) Where the Data Is Stored

The locations where the target keeps data, and why and how the data function is integrated within the target, may also influence the ultimate outcome and value of the deal. The potential buyer must be satisfied, for example, that the target has retained adequate records required by federal, state, and foreign law, as well as by the internal policies of the target. If data is located in countries with strict data protection laws, the target will have to consider the measures that must be taken to secure, process, and transfer that data in accordance with applicable laws. The

15. In conducting the above diligence, it is helpful to determine automatic-deletion periods, retention periods, and backup tape practices of the target. To the extent the target lacks an adequate retention policy, there may be excess data stored with the target that need not be transferred as part of the transaction to save costs of storage and future destruction of data.

location of data may also implicate employee monitoring of emails and other human resource (HR) functions, as well as customer consents.

Much of the knowledge regarding the location of the target's data likely resides in a corporate data map or with the target's corporate records manager. If there is no central policy or point of responsibility, another avenue of inquiry is into existing information governance projects.

The following information will help to identify the locations where the data is stored:

- A schedule of all in-house servers, Network Attached Storage document management systems, or data warehouses maintained by the target
- A schedule of all cloud computing services/collaboration services used by the target
- Whether each service is hosted internally or by a vendor other than the target
- A schedule listing all personal computers owned by the target. For portable computers, determine whether encryption is applied at the drive level.
- Whether the target provides or permits the use of portable hard drives (USB drives) for business purposes, and the controls applied for approved uses
- Whether information of the target resides only on target-owned devices, or may also reside on employee-owned devices (e.g., smartphones, tablets)
- Whether employee access to "self-help" cloud computing services (e.g., Gmail, Google Drive, Dropbox, Evernote) is allowed or prohibited

For data that is being hosted by outside vendors, the buyer should obtain copies of service agreements, including data security and privacy obligations of the vendor. The provisions in these agreements on which to focus include the following:

- *Security Provisions:* Assess whether the agreements contain adequate language on how a vendor is required to secure the data of the target.
- *Audit Rights:* Evaluate whether the target has the right to audit the vendor to ensure the security of the target's data.
- *Data-Breach Language:* Evaluate whether the agreements have language addressing:
    - the vendor's notification responsibilities in the event of a data breach;
    - whether the vendor is required to indemnify the target for a data breach;
    - whether the vendor is required to cooperate with the target in the event of a breach; and
    - damages-limitation clauses in the event of a data breach.
- *Data Protection Language:* To the extent a vendor is hosting data that is governed by foreign data protection laws, the agreements should contain detailed language regarding which laws apply and explain that the vendor is acting as a data processor.
- *Ownership and Access:* Confirm that the target has maintained ownership and access rights to the data stored on the outside vendor's hosted environment.

(f) Review of Privacy Policies and Related Compliance

The due diligence associated with the deal should incorporate a consideration of data privacy issues. For those deals involving multinational organizations (which might simply mean the collection of data from multiple countries), the issue of privacy rights violations is beginning to take on the same level of concern that traditional antitrust reviews have had.[16] This privacy policy review step should incorporate privacy policies provided to employees and other personnel. The review should consider the availability and composition of consent forms relating to collection, storage, and use of data, whether such forms are updated over time, and whether they are consistent with current use. The review should examine consumer-facing privacy policies, evaluate whether privacy policies comply with current Federal Trade Commission (FTC) expectations,[17] and determine whether privacy policies are followed internally at the target.

This review should also consider those privacy policies provided to the target's customers, its suppliers, and the general public—especially with language permitting acquisitions in mind, as the permissions incorporated into those policies may determine exactly how the buyer may use otherwise-private data post-deal.[18] These issues may be addressed by reviewing

16. Kakoli Bandyopadhyay et al., *A Framework for Integrated Risk Management in Information Technology*, 37 MGMT. DECISION 437 (1999).

17. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (Mar. 2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

18. *See* Letter from Fed. Trade Comm'n to Hon. Shelley C. Chapman regarding *ConnectEdu, Inc.*, No. 14-11238 (Bankr. S.D.N.Y.) (May 22, 2014), https://www.ftc.gov/system/files/documents/public_statements/311501/140523connecteducommltr.pdf.

both the existing data collected, and also by reviewing and cataloging changes in the target's privacy policies over time. Not all data will necessarily have the same permissions attached to it. This review should always incorporate compliance with state laws,[19] as well as international law when warranted.[20]

(g) Information Governance Policies and Record Retention Schedules

Despite the importance of information governance policies and record retention schedules, they are not often considered in the context of deal due diligence. This is not surprising. Even IT infrastructure and post-deal integration is sometimes an afterthought.[21] Still, given the rapid growth in data and its effect on deal considerations,[22] a request for and review of available data retention policies and record retention schedules should be at the forefront of the due-diligence process. The practitioner should confirm that existing policies address each of the data locations identified during the deal due-diligence process.

Next, the buyer should square the policy and schedule information with considerations regarding privacy policies and related data, confirming the policy identifies data types as well as levels of confidentiality (e.g., sensitive consumer PII, classified, confidential, and public). This confirmation process may also determine whether the policies and schedules are reasonable

---

19. The Sedona Conference, *Commentary on Privacy and Information Security: Principles and Guidelines for Lawyers, Law Firms, and Other Legal Service Providers*, 17 SEDONA CONF. J. 1 (2016).

20. Donald C. Dowling Jr., *How to Ensure Employment Problems Don't Torpedo Global Mergers and Acquisitions*, 13 DEPAUL BUS. L.J. 159 (2000).

21. Monideepa Tarafdar & Sufian Qrunfleh, *Examining Tactical Information Technology—Business Alignment*, 50 J. OF COMP. INFO. SYS. 107 (2010).

22. Paul P. Tallon, *Corporate Governance of Big Data: Perspectives on Value, Risk, and Cost*, 46 COMPUTER 32 (2013).

considering the level of confidentiality and business needs for access to the information.

Legal hold practice stands as the exception to the proverbial rule, where certain portions of the information governance policy and record retention schedule may need to be suspended based on retention periods and automatic data transfers or deletions. The buyer should determine whether appropriate safeguards are in place to suspend schedules during litigation holds. This may include practices specific to the deal itself, where information associated with the deal might relate to subsequent deal litigation.[23] A good start for this type of analysis may be a review of existing legal hold practices, policies, and other related information, which would then be read in conjunction with the policies and schedule.

(h) Determine Applicable Automatic-Deletion Periods

A number of organizations—as well as individuals acting on their own—have automatic-deletion policies. For example, it is not uncommon to have email management policies that delete email after certain periods of time, or when email is moved to other locations within (or outside) the email program. As noted in prior guidance, "an automatic deletion policy is coupled with options so that the user can move email of significance to an appropriate alternative storage location."[24] Advisors to the acquisition process, especially those involved in post-deal integration activities, should determine whether any of these rules-based systems would apply in the integrated environment and whether any legal holds apply that would require the

23. John C. Montana, *Retention of Merger and Acquisition Records and Information*, 34 INFO. MGMT. J. 54 (Apr. 2000).

24. The Sedona Conference, *Commentary on Email Management: Guidelines for the Selection of Retention Policy*, 8 SEDONA CONF. J. 239, 241 (2007).

suspension of any automatic-deletion practices.[25] This issue may also determine whether any of the automatically deleted data should be collected pre-integration while still available, perhaps in connection with a prior or prospective legal hold.

(i) Determine Backup Tape Practices

Backup tape practices in support of organizational information technology practices may be determined by reference to International Organization for Standardization (ISO) standards. In addition, certain compliance groups may retain backup tapes and related materials in accordance with regulatory standards—this type of transition (or lack thereof) has caused issues for merging organizations.[26] Finally, there may be exceptions to normal practices associated with backup tapes pursuant to existing legal holds,[27] where information technology professionals may or may not be aware of what the legal department has sequestered in accordance with those holds.[28]

(j) Review Warehousing (Including Third-Party) Practices

While warehousing issues are uncommon in current M&A due-diligence approaches,[29] they remain an important part of

25. EEOC v. JP Morgan Chase Bank, N.A., No. 2:09-cv-864, 295 F.R.D. 166 (S.D. Ohio 2013).

26. Sherer, *supra* note 9 (citing Order Instituting Administrative and Cease-and-Desist Proceedings at 2, UBS Sec. LLC, Exchange Act Release No. 52022 (July 13, 2005) (Admin. Proc. File No. 3-11980)).

27. The Sedona Conference, *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, 19 SEDONA CONF. J. 1 (2018).

28. *See* Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 218 (S.D.N.Y. 2003).

29. James A. Sherer et al., *Merger and Acquisition Due Diligence Part II—The Devil in the Details*, 22 RICH. J.L. & TECH. 4 (2016).

post-deal integration activities, especially where such activities may include "warehouses of poorly organized boxes" instead of clean, well-managed, and ordered records.[30] A review of such practices should incorporate both a policy review as well as an interview step with the target subject-matter expert knowledgeable about or responsible for such activity.

3. Existence of and Implementation of Data-Classification Policies and Related Security Measures

In addition to considering the location of information, the type of information (including whether it is comprised of or contains PII or PHI), and the manner in which the information is stored or deleted, the buyer should also consider a review of data-classification policies. This review would confirm that existing policies or schedules classify data according to its level of sensitivity. The buyer should also consider the impact to the target should that data be disclosed, altered, or destroyed without authorization according to the data's characterization (e.g., private, sensitive, internal, public). For government-contractor data or related reviews, this evaluation might also consider whether policies comply with FIPS PUB 199.[31] This evaluation would begin by obtaining and reviewing baseline security controls for each classification. The review would then confirm whether baseline security controls are appropriate for safeguarding that data.

Depending on how highly sensitive data is categorized and treated, there may be sensitive data-specific repositories within the target as well. Consideration of this point should

30. Montana, *supra* note 23.

31. U.S. DEP'T OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., COMPUT. SEC. DIV., FIPS PUB 199, STANDARDS FOR SECURITY CATEGORIZATION OF FEDERAL INFORMATION AND INFORMATION SYSTEMS (Feb. 2004), http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

incorporate further investigation of the policies detailing how data classified as highly sensitive is handled, as well as reviewing employee training materials that implement such policies.

For data classified as "sensitive," the buyer should determine whether the target has a policy to encrypt the data in transit and at rest. Finally, the buyer should consider whether the target has implemented technical controls to enforce that policy. This review will determine how the buyer may access data in company/security access controls post-deal, perhaps by determining the criteria used for granting access to each service or data repository (e.g., whether criteria permits access only to employees having a business need for that access).

In addition to determining what data should be classified as sensitive, the buyer should determine whether the information is being protected. This requires a review of affirmative security systems and requirements associated with the data, which begins with a determination of what systems are in place and how they are documented. IT and general security are often mature functions within most organizations, and there should be a number of straightforward policies available for due-diligence review, including wireless internet service providers. In addition to those policies and interviews with responsible parties, we suggest that the buyer make plans for affirmative post-deal physical-security activities, as these might slip through the cracks during integration. These physical security activities include: (i) engaging a third-party security consultant to audit for vulnerabilities; (ii) establishing a monitoring program; (iii) identifying physical security procedures for employee, contractor, and third-party workers; and (iv) evaluating third-party requirements for physical security.

4. Business Critical Functions

There is data that is classified, and data that is critical to the ongoing operations of the target organization. While the two are not mutually exclusive, organizations often build out a separate practice for bringing the organization back "online" given a disaster or other failure—in whole or in part—of the enterprise's operations.[32] The due diligence might begin with an evaluation of the target's disaster-recovery and business-continuity plans. But instead of stopping at the four corners of the plans, the buyer should also determine: (i) whether it will substitute its own policies or plan for assets pre- or post-integration; (ii) whether the plans are all-or-nothing propositions, such that the buyer might implement a disaster-recovery plan and identify basic provisions of that plan; (iii) how such implementation might work; and (iv) what, if any, are the third-party requirements associated with such disaster-recovery and business-continuity plans.

The buyer might also undertake a business impact analysis of business-critical systems (e.g., order entry, manufacturing, shipping, receiving), determining which processes, systems, and data are most critical to the continued business operations of the target. This should lead to the next steps: understanding what additional systems are dependent on business-critical systems, and assessing the consequences of losing such systems. The buyer should also obtain and evaluate backup and disaster-recovery plans for business-critical systems, perhaps in conjunction with an evaluation of the backup tape system. Finally, the buyer should evaluate whether resources and priorities allocated to the recovery of business systems are commensurate with the criticality of the systems.

32. Balachandra Reddy Kandukuri et al., *Cloud Security Issues*, 2009 IEEE INT'L CONFERENCE ON SERVS. COMPUTING.

5. Due Diligence Beyond the Data Room

In addition to the reviews of policies and technical specifications of the target's information systems and data flows, separate interviews with target employees regarding how data is really collected, stored, and used are likely to be helpful. Unfortunately, this information may walk out the proverbial door during the pendency of the deal or after its conclusion.[33] When available, these interviews should be carried out with representatives of the target's IT, HR, C-suite, and "other" functions. For IT, discussions should consider current employee access as well as third-party employee access, and how those might change during the process where the target's systems are integrated into the buyer's policy and IT environment. Likewise, HR representative interviews might further examine both the documented policies and procedures associated with information capture, storage, use, and disposal as well as the realistic practices within the organizations.

While the C-suite executives may not be well-positioned to talk about the use of information at every level of the organization, the information in their possession may be paramount for continuing operations post-integration. The buyer should focus on both the preservation of that information as well as any data generated in the meantime. Finally, depending on the operation of the target, the buyer should examine who else might be part of the target's information lifecycle. These participants may include: (i) providers of sourcing or supplier activities (and their agreed-upon compliance metrics); (ii) other third parties or cloud providers that host information; (iii) customer data and records of interactions (e.g., portals); and (iv) social media and related marketing, advertising, and sales platforms.

33. Sherer, *supra* note 9.

C. *Adapting the Due-Diligence Process to the Changing Terms of the Deal or Information Being Provided*

During the due-diligence phase, the parties may need to supplement or alter their due-diligence requests or the proposed representations and warranties that form the backbone of the transaction. Frequently, the transaction is on hold during the due-diligence process because the information disclosed through the due-diligence process could have significant impacts on the proposed transaction. By this point, a term sheet, letter of intent, or similar document may be in place (along with the NDA), and draft transaction documents may be circulated. But details are typically not finalized until after diligence takes place. During the due-diligence phase, one or both parties to the proposed transaction could obtain information that affects the negotiation, deal structure, and the draft documents, or that could potentially derail the deal. Early due-diligence responses could also lead to follow-up due-diligence requests as the parties try to refine their understanding of one another and the proposed transaction.

Follow-up due-diligence requests may seek additional information or additional support for prior responses. The data and documents shared during due diligence can identify undisclosed assets or liabilities, title issues, incompatibilities or inefficiencies, cultural or "fit" issues, tax considerations, additional costs, compliance issues, or other critical, nonpublic information. This new information could impact the value of the deal, the representations and warranties of each party, the asset-disclosure schedules, or post-closing integration and migration. Because of this, the diligence process often leads to new rounds of negotiation and revised transaction documents. For example, when Verizon learned that Yahoo, its acquisition target, had suffered two large-scale data breaches prior to the acquisition closing, Verizon immediately halted the closing and sought

additional information (in addition to a substantial reduction in the purchase price).

If the parties are unable to resolve issues identified in the due-diligence process, the transaction could be postponed or killed. These post-diligence considerations are particularly important in the privacy and security context where assets are sensitive, compliance can be complicated and burdensome, and latent incidents may go undiscovered for years in the normal course of business. In this context, the information and documents exchanged in the due-diligence process may require the parties to update schedules of included or excluded assets and liabilities (including data, data-streams, licenses and permissions, and hardware), revise or extend data privacy and security representations and warranties, or adjust plans for post-deal information technology and information security migration and integration.

D. Stage Two Summary

During the due-diligence phase of the deal, the parties should:

- identify a deal team "quarterback" with data privacy and security expertise;
- assess the type of sensitive information involved, the location of sensitive information, the target's current and historic data security and privacy practices, known vulnerabilities and breaches, and the target's relationship with vendors;
- execute the necessary NDAs to establish the terms of data sharing and set forth the restrictions and protections for that information;
- determine responsibility for creation and maintenance of a VDR to share information

requested in the due-diligence phase and determine responsibility for the privacy and security controls over the VDR itself;

- consider whether any due diligence needs to be conducted outside of the VDR and perform all necessary analyses;
- obtain a thorough understanding of the types of data utilized by the seller and the specific data that is being included or excluded from the transaction;
- interview any necessary personnel or third-party vendors regarding how the relevant data is collected, stored, or used by the seller;
- determine where the relevant data is stored by the seller;
- review the target company's privacy policies and notices, the target company's compliance with those policies and notices, and the target company's compliance with international, federal, state, and local laws and regulations;
- review available data retention policies, document retention schedules, automatic-deletion schedules, backup tape processes, and warehousing practices;
- review data-classification policies and related security measures;
- assess the target company's disaster-recovery and business-continuity plans and determine whether and to what extent the target company or the purchaser's plan will govern post-closing; and
- determine whether any existing due-diligence requests or representations and warranties need to be supplemented, modified, or

terminated based on the information acquired during the due-diligence phase.

IV. STAGE THREE: CLOSING AND POST-CLOSING CONSIDERATIONS

Post-deal integration of information technology and information security systems simultaneously presents great challenges and great opportunities. Historically, records and information management was an afterthought in an acquisition, where the speed to close the deal took priority over the practical considerations of running the acquired business. In most transactions, the buyer simply took possession *en masse* of the seller's electronic and hard-copy records and dealt with them. Sometimes the buyer would merge the seller's records with its own records, other times the buyer would maintain separate systems running in parallel, and still other times it would place the records in offsite storage or equivalent "just in case," perhaps discarding some categories of records that were deemed not to have ongoing value.

Today, the "take it all and sort it out later" approach often has significant downsides. In addition to the hard and soft costs associated with storing enterprise data (which some estimates have placed at $5,000 per terabyte or more), over-retention of data can needlessly create serious legal, regulatory, and business risks. Today buyers are finding that when it comes to data privacy, the old saying that "possession is nine-tenths of the law" could not be further from the truth, and that if care is not taken to ascertain what rights the buyer has to use and transfer personal information collected over time from customers, clients, and others, some or all of the buyer's plan to extract value from that information could be thwarted.[34] All modern companies possess large stores of electronic information. As a result,

34. Letter from Fed. Trade Comm'n, Bureau of Consumer Prot., to WhatsApp and Facebook (Apr. 10, 2014), https://www.ftc.gov/system/files/documents/public_statements/297701/140410facebookwhatappltr.pdf.

any transaction involves significant information assets. Those assets should be an integral part of the diligence process and receive prompt attention upon closing.

A. Mechanisms for Allocating Information-Related Risks

In many ways, the risks associated with data privacy and security are no different than the myriad other contingencies that are addressed by buyers and sellers during due diligence, negotiation, and post-closing dealings and, accordingly, often can be addressed using familiar tools. A full discussion of such tools, and when and how they can best be used to apportion information-related risks between buyers and sellers, is beyond the scope of this *Commentary*; however, two common examples warrant brief mention.

1. Purchase-Price Adjustments

Purchase-price adjustments are common in private-company acquisitions. Generally, for example, if an acquisition has a closing date separate from the date of the signing of the purchase agreement, a working-capital adjustment often is part of the transaction documents. This adjustment is in place to capture any change in the target's working capital between the date the purchase agreement is signed and the final closing of the transaction. While working-capital adjustments are ubiquitous in non-simultaneous sign-and-close transactions based on some valuation for the seller's working capital post-closing, purchase-price adjustments may be included to address any change in the value of the underlying assets between signing and closing. A purchase-price adjustment may be triggered by a new potential liability, such as a data breach that occurs between signing and closing, or upon request by the buyer in response to changes in valuation uncovered during due diligence. A prominent example of this is, of course, the Verizon/Yahoo acquisition discussed earlier.

Although most purchase-price adjustments are made in response to specific items impacting the financial statements of the company like working capital or EBITDA (earnings before interest, taxes, depreciation, and amortization), it may be appropriate to adjust the purchase price based on the occurrence of certain events during the gap period between signing and closing or in response to diligence discoveries. Events related to data privacy and security that may depress the value of the target company could include: (i) a data breach or other security incident requiring notification to data subjects or regulatory response; (ii) contractual or other limitations on the seller's ability to transfer valuable data to the buyer; (iii) inability on the buyer's part to use such data in ways that were anticipated when it made the initial offer of purchase; or (iv) identification during due diligence (or even post-closing, if the transaction documents permit) of data that is not collected, stored, used, or disclosed in a manner that is consistent with the company's policies or applicable law.

2. Indemnification

Sometimes, a purchase-price adjustment is not a feasible way to control for an issue that comes up during negotiation of the transaction. This may be particularly true where the underlying business will not be impacted by the issue. But there will likely be a tangible cost to addressing it, whether in legal fees, remediation measures, damage to brand or reputation, or regulatory penalties. Alternatively, if the issue is speculative and may never accrue any costs, but the buyer wants coverage on the chance that any such costs do accrue, a purchase-price adjustment may be hard to negotiate. In this instance, a special indemnity may provide the comfort the buyer requires to close the transaction without reducing the purchase price. A special indemnity can be structured so it is not subject to any basket or cap in place for the general indemnity. This will allow the buyer

to receive indemnity from the first dollar on any post-closing costs that are incurred by the company for data-related issues that may have accrued prior to closing. If the potential issue never materializes or otherwise does not result in any harm to the buyer, the special indemnity impacts neither party. But the buyer still maintains coverage for the length of the term of the special indemnity.

B. Post-Closing Operational Issues

It is important for the buyer to consider post-closing operational issues early in the transaction and consider them carefully during the drafting of the transaction documents. Issues like transferability of data, evaluation of IT infrastructure and data mapping, separation and integration of data, and harmonization of privacy and security policies should be considered as the transaction is proceeding, and may even be important for the buyer to understand when deciding whether to acquire the seller's business operations or assets in the first instance. It is important for the buyer to make an up-front determination regarding whether the data held by the seller can be used in the way the buyer contemplates and the extent to which the systems being purchased will create synergies or headaches for the buyer. In addition, as soon as practical after the closing of the transaction, the buyer should undertake to determine whether the data transferred as part of the transaction is consistent with the agreement, including its representations and warranties.

1. Identification and Confirmation of Data Transferred

While many transactional documents typically have long schedules of assets transferred, it is atypical for such documents to include a listing of the data, much less data maps identifying the data, its physical location, the hardware associated with the data, and other information necessary to access or query such data, including passwords, encryption keys, instruction

manuals, and field listings. Often, some or all of the IT personnel necessary to ascertain that information are no longer available or accessible post-transaction. Similarly, data may often be transferred but without the necessary hardware or software to access and manipulate the data.

Thus, as a threshold matter, the buyer will want to understand exactly what type of data it now owns as a result of the acquisition and what data, if any, is merely custodial or transient to its systems. This process can be a formal undertaking done through an inventory of the data or can be as informal as a perusal of a file share, depending on factors such as the volume, value, and risk associated with the information. Inventorying the data will simplify the process of understanding what data the buyer has, how it can be transferred or used, and whether it can be easily combined with the buyer's existing data. This process also should involve reviewing and, to the extent necessary, merging the buyer's and seller's respective record retention schedules, as well as identifying and taking appropriate steps to protect data coming from the seller that is subject to a litigation hold.[35]

2. Segregation of Data

The commingling of data once done is difficult to undo. Accordingly, prudence—as well as legal, technical, and practical reasons—dictates that a buyer should not immediately merge acquired data into its operations. Examples of data that require caution before merging are: (i) internal individual data (such as employee data); (ii) external individual data (such as customer or consumer data); (iii) data sets used specifically in performing a service (such as mapping data); (iv) data held by the company

35. *See* ILWU-PMA Welfare Plan Bd. of Trs. v. Conn. Gen. Life Ins. Co., No. C 15-02965 WHA, 2017 WL 345988 (N.D. Cal. Jan. 24, 2017) (sanctioning company for loss of data transferred during sale of business).

as custodian for a third party (such as data hosted by a service provider for corporate clients); and (v) transient data (such as data being processed or transmitted through the company's servers but to which the company has no ownership or other rights). The buyer should carefully consider and develop a strategy for the transfer, migration, use, and disposition of the acquired data.

3. Right to Use and Transfer Data

Purchasing a company does not automatically allow the buyer to use or transfer to itself or its affiliates (in the event of a stock sale or merger) the data owned by the target company. Transfer of any data outside the confines of the corporate entity that owns it, as well as use of the data by any affiliate or third party, may be subject to pre-existing obligations, whether contractually or through stated policies, such as a publicly available privacy policy at the point of collection. Whether already undertaken as part of the due-diligence process, it is important to review any pertinent existing privacy policies (including historically applicable policies) prior to the transfer or use of any consumer data obtained through an acquisition. If these policies limit the seller's ability to transfer the data, such restrictions likely will continue to apply post-closing, and the data may be required to remain within the acquired company or risk regulatory action. In addition, if the uses to which the buyer plans to put the information post-closing differ materially from those permitted under the seller's policies in effect at the time of collection, the buyer may have to obtain consent from the data subjects for such new uses.

4. Contractual Restrictions

Restrictions on the data may arise from promises made between the company and its users through the publication of a privacy policy. But restrictions may also exist through direct

contract between the company and its clients, customers, or vendors. Pay particular attention to any contractual arrangements that may limit the buyer's use of data held by the company post-closing, especially if the company is a custodian of data owned by others. Before putting any data collected or stored by an acquisition target to use, the buyer should review any agreements that may govern the use, retention, and disclosure of the data to ensure that no data is being treated in a way that conflicts with the company's contractual obligations. If there are any use restrictions inherent in such agreements that are not part of the existing data-use policy of the post-acquisition company, the buyer may need to revise any policies to address such additional restrictions. If the data is required to be used or stored in a manner inconsistent with prior uses based on fundamental business needs post-closing, the buyer may need to renegotiate certain agreements to provide for these new uses. As further discussed below, all acquired data should remain segregated from the buyer's data until the buyer has had a chance to: (i) understand the scope of the data in the company's systems; (ii) review the pertinent use and transfer policies for the data; (iii) cull any low-value data; and (iv) structure a plan to handle the data on a going-forward basis.

5. Statutory and Regulatory Restrictions

Beyond contractual provisions, many types of data are subject to statutory and regulatory restrictions to include data privacy, state security, and export control. The fact that data was acquired in a transaction does not give the acquiring party the unfettered right to either access or use the data. For example, in the European Union, personal and private data of the employee is just that—property of the employee. It is a violation of the employee's human rights to process that data, for example, without notice and permission. The recognition and application of these rights are being expanded under, for example, the

General Data Protection Regulation (GDPR). Accordingly, the buyer should undertake careful consideration of these and other statutory and regulatory rights ***before*** it accesses, transfers, or uses the acquired data. Be careful if the buyer intends to physically transfer the data from one country (for example, where the seller or data resides) to another country (for example, where the buyer or its facilities reside).

6. Data Separation

Not all transactions involve a transfer of all data from the seller to the buyer. Divestitures in particular present thorny issues that generally are not present where the entirety of a business is changing hands. Because a divestiture ultimately is a sale by a parent of some portion of its assets and operations (e.g., a subsidiary) to a third party, the data that is transferred must be viewed through that same lens—that is, the parent is selling the data to a third party.

From the parent's standpoint, if it neglects to take reasonable measures to protect data that is not part of the subsidiary's operations and, therefore, should not be transferred as part of the divestiture, it risks running afoul of myriad data protection laws and regulations, even if the data remains entirely contained within the subsidiary and is not breached or transferred to other areas of the buyer's enterprise. And if the subsidiary experiences a breach that results in the parent's data being exfiltrated, or potentially even if the subsidiary merely transfers the data to other areas of the buyer's business, then cue the usual parade of horribles (e.g., civil litigation, regulatory enforcement). A similar analysis applies in the context of privilege waiver. If the parent fails to take appropriate measures to prevent privileged information from being transferred to the buyer as part of the divestiture, then it could be found in subsequent litigation to have waived privilege by transferring the information to a third party without taking reasonable steps to protect it.

On the subsidiary/buyer side, similar issues and risks exist. By failing to take reasonable steps to excise data that isn't part of the subsidiary's operations, the subsidiary and buyer are on the receiving end of a data transfer that potentially violates data protection laws. Again, this can be problematic regardless of a further transfer or data breach. A class of consumers, for example, might argue the transfer of data that was not properly part of the subsidiary itself was a breach because it was an unauthorized transfer. In the event of an external breach, this too can trigger a parade of horribles. Another issue for the subsidiary/buyer is that if it takes or receives protected data, it also assumes all of the legal and compliance obligations that attach to that data (e.g., obligations under some regimes to destroy data after expiration of purpose, and requirements to maintain certain types of information in secure environments).

A well-designed and executed framework for data separation is important because the parties need to understand the security infrastructure differences between the organizations and evaluate not only where data is located currently and what security measures are in place to protect different tiers of information, but also how those measures differ between the organizations and why. There may be infrastructure challenges that the parties need to fully understand and map out before data is migrated from one system to another. If not done pre-closing, a post-closing review of the full universe of relevant systems to be integrated (or divested if there is a spin-out or other split in systems) can assist the parties to understand the scope and landscape being considered for integration, migration, or separation. In addition, a review can help determine where policies can be harmonized and can help the parties understand what data should be integrated and what data should remain segregated.

7. Deletion of Data

Once the data has been inventoried and its existing limitations understood, the buyer can then determine whether any of the data is low-value data that should be deleted rather than combined with buyer's existing data. The Compliance, Governance and Oversight Counsel estimates that approximately 70 percent of average enterprise data is redundant, outdated, or trivial (ROT), and of little or no value to the business that stores it.[36] If the data has no legal or regulatory reason for its retention and is otherwise redundant, outdated, or trivial to the business of the purchaser, the purchaser should not pay to store it and risk its compromise through a security breach. Consideration should be given to purging data that can be identified as ROT before the integration process begins and before such data is integrated into the information systems of the buyer. Data deletion, however, is not without considerable risk unless undertaken in a defensible manner that takes into consideration legal, regulatory, and business requirements to maintain the data.

C. Best Practices for Data Integration

It is also important for the buyer to consider data integration strategies and best practices to ensure the business operates smoothly after the deal closes. If possible, the buyer should anticipate potential hurdles and roadblocks to integration and address these issues in the early stages of the transaction. The following are some best practices to consider when planning for integration after the transaction closes.

---

36. Deidre Paknad, *Defensible Disposal: You Can't Keep All Your Data Forever*, FORBES (Jul. 17, 2012, 10:40 P.M.), https://www.forbes.com/sites/ciocentral/2012/07/17/defensible-disposal-you-cant-keep-all-your-data-forever/#362f67bd6bb3.

1. Summarizing Limitations and Permissions

It is unlikely the legal or compliance officers who review the permissions around the data will be the same persons completing the technical process to integrate the data on the systems or using the data once it's been integrated. Once the review is completed, a memorandum should be prepared that summarizes the inventory of data and any limitations or restrictions to use, combine, and disclose the data acquired at closing. The memorandum will not only assist with planning and executing the data integration, but it also can serve as a "use guide" going forward when questions arise whether certain data can be used in certain business operations. Information that the use guide contains can be relevant to operations, marketing, IT, and many other areas of the business.

2. Leveraging Institutional Knowledge

As part of the integration process, the buyer may want to involve the seller's officers and personnel (as well as vendors, SaaS providers, and cloud providers) originally associated with the information to the extent possible. If the acquisition is structured as a stock sale, much of the institutional knowledge will likely now be captured by employees of the buyer. If the sale is structured as an asset sale, or in the case where certain knowledge resides in the chain above the target company, a transition-services agreement may be in place to assist with the transfer and integration of data. The buyer in that instance has maximum leverage in negotiating a transition-services agreement pre-closing. The buyer personnel should be informed of the transition assistance being provided and given an opportunity to capture as much institutional knowledge as possible from outgoing knowledge-holders.

If there will be redundancy in job duties and not all personnel will be transitioning to the business post-closing, those

employees taking over the duties of the departing ones should meet with their counterparts to determine the current practices in place regarding operations and data handling. They could then prepare written memoranda outlining the existing practices to smooth the transition. If emotions are raw or the systems to be merged are complex, it may make sense to engage a third party to consult on the integration and help streamline the combination of business processes.

3. Integration Meetings and Training

As part of the integration process, IT personnel and stakeholders for the various data types should meet so that all parties understand: (i) what data might be changing or is being added; (ii) who is responsible for the oversight and use of newly acquired data; (iii) how the data fits into the existing business operations; and (iv) whether any special procedures need to be adopted to handle newly acquired data. Employees who are expected to take on new responsibilities in managing data or privacy matters surrounding data need to be aware of these obligations and properly trained on the handling of information and the timeframes for compliance associated with any responsibilities.

4. Updating, Adapting, or Revising Policies and Procedures

It is a mistake to assume that data acquired as part of a transaction will fit neatly within the four corners of the buyer's policies and practices to include: (i) data privacy; (ii) data security; (iii) information governance; (iv) confidential information handling; and (v) information technology. Pay careful attention to whether and how such policies and practices require revision, adjustment, or adoption to fit the needs of the information that is to be acquired. This consideration is especially true when acquiring a new line of business (e.g., products, markets,

customers) that is not second nature to the buyer. Give particular consideration from a data security perspective to the acquisition of not only data, but also hardware associated with that data, or to providers or vendors with which the buyer has no prior business dealings.

5. Developing a Data-Transition Plan

Transitioning data from one entity to another may not be as simple as copying the data to a new location. Certain data may require physical safeguards to be properly maintained, applications that require additional licenses for full compliance, or additional equipment to be installed. The data-transition process should be reviewed in the aggregate with existing information, software, and systems to determine what overall schema will work best for the ongoing business. A sizeable acquisition of data may present an opportunity for the buyer to undertake a defensible deletion initiative, do a fresh security assessment, or otherwise find efficiencies and prospective compliance opportunities with respect to how it handles its data. If the target company processes, owns, or is custodian for a large data cache, then it may make sense to bundle the transition with other actions that may improve the buyer's compliance and cause long-run cost savings that can even recoup the entire amount spent on the integration.

6. Knowing When Not to Integrate

Integration is not the only option when it comes to handling post-closing data issues. As part of the due diligence, the buyer should closely examine the data in question, the universe of policies in place with both entities, and the reasons for and against integration. To the extent that the transaction is intended to combine two separate businesses into one business (to achieve operational efficiencies with economies of scale, to expand product offerings to existing customers, or even to roll

customers onto a new service), the ability to transfer data between organizations and to consolidate systems and policies typically will be desirable for the buyer.

There are situations, however, where it may make sense to forego integration altogether. For example, the seller is to operate independently to develop its own products and maintain its own customer base. Or the buyer purchased the seller with an exit strategy in mind, such as a portfolio company that may be sold after only a few years. In all scenarios, the buyer should remain aware of the potential pitfalls of transferring data from one business to another. It should avoid any transfers that might contravene the existing policies of the seller, are otherwise prohibited by the seller's public privacy disclosures, or violate existing agreements the seller has with third parties.

7. Recognizing Opportunities for Improvement and Advancement

As mentioned, an acquisition presents opportunities for operational improvements and advances. In any significant deal, substantial resources are allocated for due diligence, professional services, and post-deal integration. Business functions across the enterprise are focused on the many streams of work required to integrate successfully the new operations into existing ones. Critical human resources are still employed or otherwise available. And perhaps most importantly, as noted above, the seller's data is still separate from the buyer's data; it has not yet been integrated into the buyer's information systems. As a result, it can be assessed, analyzed, and acted upon without first needing to be identified and filtered from a larger set where it is commingled with the buyer's existing data. In short, many of the dynamics inherent in the acquisition process create ripe conditions for tackling many of the challenges inherent in that same process. Initiatives that might otherwise struggle in competition for funding, staffing, and other resources often can achieve

liftoff in their own right or by "piggybacking" on other related initiatives.

This pre-integration period of time provides an extra opportunity to not only review, analyze, and consolidate the data between the entities, but also to potentially find a structural solution superior to the one currently used by either entity. A buyer already investing in the integration process can take this opportunity to revise further its internal practices to a level that may bring it future cost savings in the form of enhanced economies of scale, reduced risk of security incidents, and streamlined systems that are less costly to maintain. The very real cost savings on a going-forward basis may justify the expenditure post-merger to reinvent the data management and security infrastructure of the transaction parties.

D. Stage Three Summary

The buyer should give consideration to the following issues that may arise during the closing or post-closing time period and, if needed, implement the appropriate measures:

- Whether the transaction should include a mechanism for allocating information-based risks, such as a purchase-price adjustment or indemnity provision
- A method for the identification and confirmation of the data acquired
- How the buyer intends to use and transfer the data, and any limitations that may exist (whether contractual, regulatory, statutory, or by virtue of the seller's existing privacy policies) on the buyer's ability to acquire, transfer, or use the subject data
- Whether the data being acquired is necessary to the buyer's operations, and how the buyer

will integrate the data into its operations on a going-forward basis

- Whether and to what extent data should remain segregated during the deal process and post-closing
- Under what circumstances it is necessary or appropriate to delete data that does not need to be transferred
- Creation of a memorandum summarizing the data acquired and any limitations or restrictions on its use, combination, and disclosure
- Development of a mechanism for capturing institutional knowledge and a plan for data integration, including training of relevant personnel
- Undertaking a holistic review of the data-transition process to determine how data will be integrated with existing information, software, and systems to determine what overall schema will work best for the purchaser's business going forward

APPENDIX A:
DIFFERENT CATEGORIES AND TYPES OF DATA IMPLICATED IN THE DEAL ANALYSIS

GENERAL CATEGORIES OF DATA	
CATEGORY	**DESCRIPTION**
Employee Data	Employee data includes Personally Identifiable Information (PII) of employees, such as names, addresses, and social security numbers. It includes banking and payroll information, such as salary data. This data can also include background check information and other sensitive information such as employee reviews, performance metrics, and disciplinary actions. Employee data is often particularly sensitive and thus triggers a range of regulatory requirements, including requirements relating specifically to background checks.
Customer Data	Customer data includes PII of customers, such as names and email addresses. It may also include customer preferences, such as purchase history or internet browsing habits, and customer account and billing information. Customer data is often the most valuable digital asset in an M&A transaction, but the uses to which the buyer can put acquired customer data can be impacted substantially by the acquisition target's privacy statements and privacy policies.

CATEGORY	DESCRIPTION
Intellectual Property (IP)	The IP that companies maintain will vary greatly in quantity and quality, and therefore IP is an example of how data classification is simple on the surface yet not so—it requires further stratification. Identifying all IP is not the same as classifying all IP, because different types of IP are afforded different legal protection and require different obligations of the holder of the asset. For example, the validity of a trade secret requires its holder to employ efforts that are reasonable under the circumstances to maintain its secrecy. Yet trade secrets are not the only type of IP to gain value as a result of secrecy. Thus, classification frameworks should consider other forms of IP, such as know-how and database contents.
Operational Data	Operational data may include the know-how referenced above. It may also include accounting data, human resources and labor data, information concerning competitors, customers, and suppliers, market projections, and other information the business relies on to make decisions and operate on a day-to-day basis. Operational data may also include workflows and processes employed by a business.

CATEGORY	DESCRIPTION
Structured Data	Structured data is raw data that is stored in a data platform (a database) that organizes the raw data points in a meaningful way and enables the user to generate reports summarizing the underlying digital information. The database may be commercially available (off the shelf), entirely custom-built, or a hybrid of the two. The usefulness and value of structured data relies on access to the database that organizes and reports on the underlying information.
Unstructured Data	Unstructured data is data lacking a designated pattern and may be considered as a subset of the other classifications. Unstructured data is often difficult to value and may include images, files, and text documents. Typically, unstructured data derives value from further processing and analysis.

CATEGORY	DESCRIPTION
Personally Identifiable Information (PII)	PII is defined by the National Institute of Standards and Technology (NIST) as "(1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."[37] Common examples of PII include names (e.g., full name, alias, maiden name), personal identification numbers (e.g., driver's license number, financial account number, credit card number), addresses (e.g., street address, workplace, email address), or personal characteristics (e.g., facial images, fingerprints, handwriting).

37. U.S. DEP'T OF COMMERCE, NAT'L INST. OF STANDARDS & TECH., COMPUT. SEC. DIV., SPECIAL PUBL'N 800-122, GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII) (April 2010), http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf. To "distinguish" an individual means to identify an individual (e.g., name, passport number, social security number, biometric information). To "trace" an individual means to process sufficient information to make a determination about a specific aspect of an individual's activities or status (e.g., an audit log of an individual's recorded actions). And "linked" information means information about or related to an individual that is logically associated with other information about the individual (e.g., data from two different access-controlled databases), versus "linkable" information that is about or related to an individual for which there is a possibility of logical association with other information about the individual (e.g., data from one access-controlled database can be paired with information from an unrelated system, such as a public information database).

Particular Types of Data

I. Healthcare

A. Qualifying Data

- Qualifying data in this category includes: individually identifiable health information, Protected Health Information, and Electronic Protected Health Information.

- "'Individually identifiable health information' means any information, including demographic information collected from an individual, that: (A) is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual, and [either] (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual."[38]

- "Protected Health Information" (PHI) means individually identifiable health information, that is: (i) transmitted by electronic media; (ii) maintained in electronic media; or (iii) transmitted or maintained in any other form or medium, with certain exclusions for education and employment

38. 42 U.S.C. § 1320d(6).

records.[39] "Electronic Protected Health Information" (ePHI) means "electronic protected health information that is created, received, maintained, or transmitted by or on behalf of the health care component of the covered entity."[40]

B. Entities Covered

- Health Insurance Portability and Accountability Act (HIPAA) applies to covered entities and business associates. Covered entities are health plans, healthcare clearinghouses, and healthcare providers.[41] A business associate is a person or entity that uses PHI to perform certain functions or services on behalf of the covered entity.[42]

C. Applicable Laws

- HIPAA prohibits the unauthorized disclosure of PHI by covered entities to certain third parties.[43] The Health Information Technology for Economic and Clinical Health (HITECH) Act extends criminal enforcement and civil liability to covered entities and business associates who, without

39. 45 C.F.R. § 160.103.

40. 45 C.F.R. § 164.105(a)(2)(i)(D).

41. 45 C.F.R. § 160.103.

42. *Id.*

43. *See* 45 C.F.R. § 164.502(e); a broader set of guidelines and rules established by the U.S. Department of Health and Human Services must also be consulted.

authorization, obtain or disclose PHI.[44] Furthermore, the U.S. Department of Health and Human Services (HHS) promulgated (i) the HIPAA Privacy Rule, which establishes national standards for the protection of PHI, and (ii) the HIPAA Security Rule, which requires a national set of security standards for the confidentiality, integrity, and availability of ePHI that an entity creates, receives, maintains, or transmits. The recently issued Omnibus Final Rule expands the definition of "business associate" to generally any entity that creates, receives, maintains, or transmits PHI on behalf of a covered entity (e.g., subcontractors, health information organizations, electronic medical records vendors) and sets both permissible uses of and security requirements for PHI by business associates, as well as defining liability for impermissible use—i.e., business associates are directly liable for impermissible uses and disclosure of PHI.[45] Moreover, under the Final Rule, business associates must conduct a risk analysis of any potential security risks and vulnerabilities to ePHI.

- HIPAA preempts state law only when state law is less stringent.[46] For example, HHS' rules do not restrict the use or disclosure of de-identified health information; however, state laws vary widely in

44. *See* 42 U.S.C. §§ 17935, 17939.; *see also* Kara J. Johnson, *HITECH 101*, AM. BAR ASS'N (June 5, 2012), http://www.americanbar.org/groups/young_lawyers/publications/the_101_201_practice_series/hitech_101.html.

45. *See* 45 C.F.R. §§ 160, 164.

46. *See* 45 C.F.R. § 160.203(b).

their level of protecting de-identified health information.

D. M&A Impacts

- In healthcare M&A transactions, entities can disclose only the minimum PHI necessary to complete the transaction.[47] Healthcare audits are common, and it is important to consider appropriate security, technical, and physical safeguards early in the M&A process. Parties should analyze all business associate agreements. Business associates that operate under a patient authorization, instead of a business-associate agreement, can incur liability to the target company and the potential buyer because a covered entity cannot rely on patient authorization forms to transfer data when what is required is a business-associate agreement.

- Accordingly, a thorough HIPAA due-diligence review should determine: (i) the type of health information (e.g., PHI and ePHI) collected by the target; (ii) who the target discloses that health information to; (iii) how the health information is transferred to any third parties; and (iv) the target's policies and agreements relating to such information. Representations and warranties that drive the disclosure of these categories of information are highly recommended.

47. *See* 45 C.F.R. § 164.502(b).

II. Biometric Data

A. Qualifying Data

- Biometric data typically refers to either (i) measurable human biological and behavioral characteristics that can be used for identification, or (ii) the automated methods of recognizing an individual based on those characteristics. Examples include facial images, fingerprints, and retinal scans.[48] Many jurisdictions have varying definitions of biometric data, so parties should carefully analyze the rules with respect to the jurisdictions to which they are subject.

B. Entities Covered

- Any entity that collects, processes, or retains biometric data will likely be subject to the additional requirements that attach to biometric data. In practice, the industries most likely to have biometric data include life sciences, pharmaceutical, and medical companies, along with healthcare and technology companies. However, some employers now collect biometric data on their employees, potentially expanding the scope of industries subject to these concerns dramatically.

C. Applicable Laws

- Any entity that collects, processes, or retains biometrics should consult both federal agency

48. Michael P. Daly et al., *Biometrics Litigation: An Evolving Landscape*, PRAC. L. THE J. (April/May 2016).

guidance (e.g., the FTC and the Equal Employment Opportunity Commission (EEOC)) and state laws regarding its security and privacy—recognizing that the regulatory landscape around biometrics is quickly evolving. While biometric data lacks a federal regulatory framework, state laws have raised increased scrutiny of biometric data protection (e.g., in Illinois biometric data is considered to be PII); however, there is heavy debate around what qualifies as a biometric identifier. Illinois's Biometric Information Privacy Act was the first in the country to consider biometric identifiers in a commercial setting; it defines "biometric identifier" as "a retina or iris scan, fingerprint, or scan of hand or face geometry," specifically excluding physical descriptions or photographs.[49] Similarly, in Texas the Capture or Use of Biometric Identifier statute defines "biometric identifier" as a "retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry," with no specific exclusions to physical descriptions, but excludes photographs or information derived from a photograph.[50] In other states, many healthcare organizations consider it

49. 740 ILL. COMP. STAT. 14/10; *see* 740 ILL. COMP. STAT. 14/20 (noting that statute creates a private right of action for "any person aggrieved" by violation of statute, providing for statutory damages of $1,000 for negligent violation, up to $5,000 for intentional or reckless violation, along with attorneys' fees and costs under 740 ILL. COMP. STAT. 14/20).

50. TEX. BUS. & COM. CODE ANN. § 503.001(a); *see* TEX. BUS. & COM. CODE ANN. § 503.001(d) (noting no private rights of action under statute, but civil penalties can be brought by Texas Attorney General for up to $25,000 per violation).

best practice to engage in heightened security practices when dealing with biometrics.

- The rapid rise in private-sector biometric technology use has been seen not only in technology services (such as facial recognition software used in social media tagging), but also with health and fitness tracking devices (such as smartwatches and apparel). The major concern with this type of data is that unlike passwords or personal identification numbers (PINs), individuals generally cannot change their biometric features, and thus may not prevent access in the case of a data breach. The use of biometric screening has been part of heavy federal privacy scrutiny by the FTC and EEOC where it involves consumer recognition and screening tests that are deemed unfair or deceptive practices under Section 5 of the Federal Trade Commission Act, or are otherwise in violation of the Americans with Disabilities Act.[51] The area has been the subject of increased class-action litigation.[52]

D. M&A Impacts

- Parties to an M&A transaction need to recognize whether biometrics are collected from a product or service offering, or have been stored and retained in the standard course of business (e.g., for internal access control security and employee or customer data). As class-action activity for breaches of biometric data picks up, potential

51. Daly et al., *supra* note 48.

52. *Id.*

liability exposure can be far reaching and expensive. And privacy and security requirements for the collection and retention of biometrics are ever-evolving, so it is important in the due-diligence phase to keep up with regulatory and jurisdiction-specific requirements.

III. Financial Data

A. Qualifying Data

- Qualifying data in this category includes: Non-public Personal Information (NPI), Federal Tax Information (FTI), and Cardholder Data. "NPI" means personally identifiable financial information (i) provided by a consumer to a financial institution; (ii) resulting from any transaction or any service performed for the consumer; or (iii) otherwise obtained by the financial institution.[53] "FTI" includes any return or return information received from the Internal Revenue Service (IRS) or secondary sources, such as the Social Security Administration, Federal Office of Child Support Enforcement, or Bureau of Fiscal Service, by a state, county, or municipal agency or a contractor providing services to such an agency.[54] FTI includes any information, including PII, created by the recipient that is derived from return or return

53. 15 U.S.C. § 6809(4); Federal Final Model Privacy Form Under the Gramm-Leach-Bliley Act, 74 Fed. Reg. 62,890, 62,892 n.18 (Dec. 1, 2009).

54. *See* INTERNAL REVENUE SERV., PUBL'N 1075, TAX INFORMATION SECURITY GUIDELINES FOR FEDERAL, STATE AND LOCAL AGENCIES (Sept. 2016), https://www.irs.gov/pub/irs-pdf/p1075.pdf [hereinafter IRS Pub. 1075].

information.[55] "Cardholder Data" includes the primary account number, cardholder name, expiration date, and service code; "Sensitive Authentication Data" includes "full track data" (magnetic-stripe data or equivalent on a chip), CAV2/CVC2/CVV2/CID, PINs/PIN blocks; "Cardholder Data Environment" is comprised of people, processes, and technologies that store, process, or transmit cardholder data or sensitive authentication data; and "System Components" includes network devices, servers, computing devices, and applications (e.g., Domain Name System (DNS) servers, network firewalls, and virtual machines).[56]

B. Entities Covered

- Numerous entities are subject to the rules covering the data protection and privacy of financial data. The primary entities subject to these rules are financial institutions. "Financial institutions" refers broadly to companies that are "engaging" in offering financial products or services to individuals, like loans, financial or investment advice, or insurance, but excludes certain entities (e.g., those subject to the Commodity Futures Trading Commission).[57] Also, companies that

55. *See id*.

56. PAYMENT CARD INDUS. SEC. STANDARDS COUNCIL, PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD: REQUIREMENTS AND SECURITY ASSESSMENT PROCEDURES (version 3.2.1 May 2018), https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1557430674216 (hereinafter PCI DSS Version 3.2.1).

57. *See, e.g.*, 15 U.S.C. § 6809(3); 15 U.S.C. § 6801.

provide support to state or local governments that include the handling or processing of Federal Tax Information will likely be subject to the rules covering financial data.

- In addition, companies that in any way handle credit card information are subject to the Payment Card Industry Data Security Standard (PCI DSS). Specifically, PCI DSS applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process, or transmit cardholder data or sensitive authentication data, and to entities that accept credit cards or otherwise use credit card data. Note that PCI DSS may also apply to payment application vendors if the vendor stores, processes, or transmits cardholder data, or has access to such cardholder data.[58]

C. Applicable Laws

- The data protection and privacy of financial information have long been subject to a variety of federal, state, and industry-based statutes, rules, and guidelines, involving everything from the encryption of data to privacy disclosures to consumers under the Gramm-Leach-Bliley Act (GLBA). GLBA limits how financial institutions use specific types of NPI from consumers—i.e., their information-sharing practices.[59] Under the GLBA's

58. *See* PCI DSS Version 3.2.1, *supra* note 56.

59. 15 U.S.C. §§ 6801–6809.

Financial Privacy Rule, a financial institution may only disclose consumers' NPI in connection with a sale, merger, or transfer of a business with affiliated third parties.[60] "Customers" (consumers who are in a customer relationship with the institution) must be provided a reasonable opportunity to direct the financial institution not to share NPI about them (i.e., an opt-out) with non-affiliated third parties other than as permitted by the statute (e.g., for everyday business processing purposes or as part of government requests).[61]

- The privacy of NPI also translates to compliance with the Fair Credit Reporting Act (FCRA), more broadly. The FCRA applies to entities that use credit reporting agencies to determine a person's credit worthiness, character, mode of living, or general reputation.[62] It mandates that companies provide policies to reasonably ensure consumers of accurate data, and provides a reasonable process for consumers to correct inaccurate information.[63] Some state laws also establish stringent privacy standards, such as California's Financial Information Privacy Act, which requires affirmative consent from consumers for companies to share certain information with affiliated parties.[64]

60. 15 U.S.C. § 6802(e)(7).

61. *See* Federal Final Model Privacy Form Under the Gramm-Leach-Bliley Act, 74 Fed. Reg. at 62,892.

62. *See* 15 U.S.C. § 1681.

63. *See* 15 U.S.C. § 1681b.

64. *See* CAL. FIN. CODE §§ 4050–4060.

- The GLBA further outlines how financial institutions must safeguard NPI. The GLBA's Safeguards Rule makes specific financial regulatory agencies, such as the FTC, responsible for establishing standards "relating to administrative, technical, and physical safeguards (i) to insure the security and confidentiality of customer records and information; (ii) to protect against any anticipated threats or hazards to the security or integrity of such records; and (iii) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."[65] It should be noted that the Safeguards Rule (i) is applicable to entities that are not subject to the Privacy Rule (e.g., student loan operators), and (ii) requires that specific confidentiality and security requirements are met when handling NPI (e.g., having a written information security plan).[66]

- Notably, encryption standards are often required for handling certain financial data. The IRS has issued security controls under I.R.C. § 6103 for tax returns that involve FTI.[67] The IRS similarly provides guidance on how certain entities collecting FTI can comply with respect to email, data

65. 15 U.S.C. § 6801(b).

66. *See Financial Institutions and Customer Information: Complying with the Safeguards Rule*, FED. TRADE COMM'N (April 2006), https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying.

67. *See* IRS Pub. 1075, *supra* note 54.

transfers, mobile devices, and databases.[68] Similarly, the Financial Industry Regulatory Authority (FINRA) issues rules for financial institutions to comply with Security and Exchange Commission regulations by adopting written policies and procedures to protect customer information, defining duties to conduct information security operations, and preserving electronically stored records using encryption.[69] FINRA has been active in bringing enforcement actions against financial institutions that do not adopt encryption standards.[70] Similarly, certain states have their own data encryption laws for financial data, which also implicate state-level data-breach statutes. State Attorneys General often impose heavy penalties if a data breach is not properly disclosed.[71]

---

68. *See Encryption Requirements of Publication 1075*, INTERNAL REVENUE SERV., https://www.irs.gov/uac/encryption-requirements-of-irs-publication-1075 (last updated Jul. 18, 2018).

69. *See, e.g.*, *Cybersecurity*, FIN. INDUS. REG. AUTH., http://www.finra.org/industry/cybersecurity (last visited May 9, 2019).

70. FINRA recently brought an enforcement action against a broker-dealer that lost a laptop with unencrypted consumer data, ordering it to pay fines, even without a showing of a known identity theft or customer financial loss. *See* Jody Godoy, *Sterne Agee Settles With FINRA Over Laptop Privacy Breach*, LAW360 (May 26, 2015, 3:57 P.M.), http://www.law360.com/articles/659794/sterne-agee-settles-with-finra-over-laptop-privacy-breach ("[T]he firm failed to take appropriate technological precautions to protect customer and highly sensitive information[.] . . . There were no [written security protocols] to ensure that the firm's most sensitive customer and proprietary information stored on laptops were being adequately safeguarded by appropriate technology, such as encryption." (final alteration in original)).

71. *See, e.g.*, LB835, 104 Leg., 2d Sess. (Neb. 2016).

- Entities that process financial data through payment systems, both within a brick-and-mortar and online retail setting, must follow certain industry-based guidelines. The Payment Card Industry Security Standards Council issues the PCI DSS, which requires that all entities that process, store, or transmit Cardholder Data or Sensitive Authentication Data maintain a secure Cardholder Data Environment. PCI DSS version 3.2 was published in April 2016 and calls for stronger encryption standards and multifactor authentication.[72]

D. M&A Impacts

- Several financial laws, regulations, and industry guidelines can affect an M&A transaction in the privacy and data security context. Target companies should have standards and written policies in place that comply with the GLBA's Financial Privacy Rule governing NPI, as well as any rules established by an appropriate financial regulatory agency, including states, and, where applicable, must be mindful of the FCRA. The processing of FTI and payment data must undergo further scrutiny both during and after an M&A transaction. Buyers should insist on very robust representations driving the disclosure of all agreements and data pertaining to these data types.

72. *See* PCI DSS Version 3.2.1, *supra* note 56.

IV. Energy Data

A. Qualifying Data

- Qualifying data in this category includes "Bulk Electric System Cyber Information," which means "information about the BES [Bulk Electric System] Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System."[73] For example, this would include security procedures or information about the BES Cyber Systems, Physical Access Control Systems, and Electronic Access Control or Monitoring Systems that are not publicly available and could be used to allow unauthorized access or unauthorized distribution. It would exclude pieces of information that by themselves do not pose a threat or could not be used to allow unauthorized access to BES Systems, such as device names, individual IP (Internet Protocol) addresses without context, ESP (Electronic Security Perimeter) names, or policy statements.

- Note the following definitions. "BES Cyber System" means "[o]ne or more BES Cyber Assets logically grouped by a responsible entity to perform one or more reliability tasks for a functional entity."[74] "BES Cyber Asset" relates to any "Cyber Asset that if rendered unavailable,

---

73. *Glossary of Terms Used in NERC Reliability Standards*, N. AM. ELEC. RELIABILITY CORP. (Mar. 8, 2019), http://www.nerc.com/files/glossary_of_terms.pdf.

74. *Id*.

degraded, or misused would, within 15 minutes of its required operation, misoperation, or non-operation, adversely impact one or more Facilities, systems, or equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the [BES]."[75] "Cyber Asset" means "[p]rogrammable electronic devices, including the hardware, software, and data in those devices."[76]

B. Entities Covered

- The entities and industries most likely to be concerned with this category of data include electric utilities and energy producers. More specifically, these entities include Bulk Electric Systems and other entities subject to Federal Energy Regulatory Commission (FERC) regulation.

C. Applicable Laws

- With rising concerns over critical infrastructure protection and electric grid reliability, energy producers and utilities, in general, are subject to a variety of FERC (or the U.S. Nuclear Regulatory Commission (NRC)) and industry-based guidelines regarding their data and industrial control systems. Recently, FERC issued a final rule adopting seven revised Critical Infrastructure Protection (CIP) Reliability Standards and physical

75. *Id*.

76. *Id*.

controls addressing cybersecurity.[77] Industry guidelines to comply with these rules have been developed by the North American Electric Reliability Corporation (NERC) regarding CIP Reliability Standards and have been approved by the FERC.[78] Facilities regulated by the NRC, however, follow their own set of cybersecurity rules particular to nuclear considerations.[79]

D. M&A Impacts

- Data involving a BES Cyber System is considered part of critical infrastructure. M&A due diligence should consider whether a target electric, nuclear, or other energy-producing company complies with the security protocols promulgated by the

77. The seven reliability standards are: CIP-003-6 (Security Management Controls), CIP-004-6 (Personnel and Training), CIP-006-6 (Physical Security of BES Cyber Systems), CIP-007-6 (Systems Security Management), CIP-009-6 (Recovery Plans for BES Cyber Systems), CIP-010-2 (Configuration Change Management and Vulnerability Assessments), and CIP-011-2 (Information Protection). Revised Critical Infrastructure Protection Reliability Standards, 81 Fed. Reg. 4,177, 4,177 (Jan. 26, 2016).

78. *See Cyber Security Standards Transition Guidance*, N. AM. ELEC. RELIABILITY CORP. (Apr. 11, 2013), https://www.nerc.com/pa/comp/Resources/ResourcesDL/Cyber_Security_Standards_Transition_Guidance.pdf.

79. *See* 10 C.F.R. § 73.54; *NRC Regulatory Guide 5.71: Cyber Security Programs for Nuclear Facilities*, U.S. NUCLEAR REG. COMM'N (Jan. 2010), http://www.nrc.gov/docs/ML0903/ML090340159.pdf. The NRC uses the following terms: "critical digital asset" (CDA) to mean "[a] subcomponent of a critical system that consists of or contains a digital device, computer or communication system or network;" "critical system" (CS) means "[a]n analog or digital technology based system in or outside of the plant that performs or is associated with a safety-related, important-to-safety, security, or emergency preparedness function[,]" (e.g., equipment, communication systems, networks). *Id.* at 35.

FERC, NRC, or any other specially commissioned industry group. Acquiring entities should be sure they understand the compliance footing of the acquired entity because coming into compliance may be a significant liability that could impact the economic return of the transaction.

V. Telecommunications Data

A. Qualifying Data

- Qualifying data in this category includes "Customer Proprietary Network Information" (CPNI). CPNI includes customers' telephone call-detail records and logs, network subscription and services, and other subscriber information used for billing.[80]

B. Entities Covered

- The entities most traditionally concerned with this category of data were telecommunications carriers. Increasingly, however, the entire mobile industry, including hardware and software companies and internet service providers (ISPs), are concerned with this data set.

C. Applicable Laws

- Traditionally, only telecommunications carriers were subject to Federal Communications Commission (FCC) regulations, mostly regarding CPNI privacy. But as the FCC becomes more

80. 47 U.S.C. § 222(h)(1); *see* 47 C.F.R. §§ 64.2001–.2011.

active in regulating mobile networks—often overlapping with FTC jurisdiction—its regulatory reach has also expanded to include the scrutiny of privacy and security of the broader industry (e.g., smartphone manufacturers). Traditional carriers have long been subject to privacy rules over certain data that they collect from customers. Under the Telecommunications Act, the FCC is tasked with regulating how telecommunications companies collect, use, and share CPNI that includes customers' telephone call-detail records and logs, network subscription and services, and other subscriber information used for billing.[81]

- The FCC recently promulgated rules to protect broadband consumer privacy—a step that expands the FCC's reach from phone carriers to include ISPs, along with smartphone hardware and software companies.[82] The rules deal largely with how ISPs collect and use information regarding their customers' online activities. They also establish cybersecurity requirements for how ISPs protect CPNI among other types of information, including the implementation of risk management practices and audits.[83] For example, the FCC and FTC have initiated parallel regulatory

81. *See* 47 C.F.R. § 64.2001–.2011.

82. *See FCC Releases Proposed Rules to Protect Broadband Consumer Privacy*, FED. COMMC'NS COMM'N, https://www.fcc.gov/document/fcc-releases-proposed-rules-protect-broadband-consumer-privacy (last visited May 9, 2019).

83. *See* Press Release, Fed. Commc'ns Comm'n, FCC Proposes to Give Broadband Consumers Increased Choice, Transparency and Security for Their Personal Data (March 31, 2016), https://docs.fcc.gov/public/attachments/DOC-338679A1.pdf.

assessments into mobile security risks and vulnerabilities.

D. M&A Impacts

- While parties to an M&A transaction involving telecommunications carriers are required to comply with the FCC's privacy guidance, companies whose practices may touch on telecommunication issues as part of their core or ancillary practices may need to consider the FCC's emerging role in setting additional privacy and security standards. An acquirer should be aware that by purchasing one of these companies, it could end up entering a world of regulation with which they are unfamiliar.

APPENDIX B:
SAMPLE REPRESENTATIONS AND WARRANTIES

In an information economy, it is increasingly important to understand the information security and privacy protections that target companies across industries have in place at the time of an acquisition, whether in a stock deal or asset purchase. Traditionally, representations and warranties relating to information security and privacy have been "flat," meaning they make a general statement about the acquired assets or business that is required to be true. The parties then negotiate over the language of the representation or warranty, adding or subtracting qualifiers such as knowledge, duration of time, and materiality. Because we believe that the information practices and procedures of companies and their compliance with a myriad of industry-specific laws, regulations, and guidelines require a more nuanced approach, we provide sample representations and warranties focused on driving disclosure where practicable.

These sample representations and warranties are for use in an acquisition and adopt disclosure-focused schedules detailing the seller's practices, policies, and third-party contracts, along with the type of data that it collects, uses, or discloses subject to the transaction. Below are nine critical areas in an acquisition, with examples and recommended disclosure provisions: (1) Compliance with Information Security and Data Privacy Laws; (2) Information Security Measures and Standards; (3) User Privacy and Information Security Policies;[84] (4) Information Security and Data Privacy Third-Party Contractual Obligations; (5) Data Access Policies; (6) Information Security and Data Privacy Complaints and Investigations; (7) Security Breaches and Unauthorized Use of Personal Information; (8) Effect of the Transaction on Personal Data; and (9) Cybersecurity Insurance.

84. This provision relates to both consumer data and employee data.

The following sample representations and warranties are neutral in nature and should be modified, where applicable, to align with the buyer's interests. These provisions are not industry-specific and are drafted to work for a broad range of companies. Accordingly, they may need to be modified depending on the industry in which the target business operates. Where appropriate, counsel should consult with industry specialists to ensure relevant industry concerns and issues are adequately addressed.

1. Compliance with Information Security and Data Privacy Laws.

a. Sample contractual language:

i. Compliance with Laws. Except as set forth on Schedule [ ], the Company is and for the past [ ] years has been in compliance, in all material respects, with all (i) Information Security and Data Privacy Laws, and (ii) Foreign Information Security and Data Privacy Laws.

b. Pertinent defined term(s):

i. "Information Security and Data Privacy Laws" means the following laws, to the extent applicable to the Company and solely to the extent related to the collection, use, disclosure, and protection of personal data: (a) the Fair Credit Reporting Act (FCRA) of 1970, as amended; (b) the Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM); (c) the Privacy Act of 1974, as amended; (d) the Family Educational Rights and Privacy Act (FERPA) of 1974, as amended; (e) the Right to Financial Privacy Act of 1978, as amended; (f) the Privacy Protection Act of 1980, as amended; (g) the Cable Communications Policy Act of 1984, as

amended; (h) the Electronic Communications Privacy Act (ECPA) of 1986, as amended; (i) the Video Privacy Protection Act (VPPA) of 1988, as amended; (j) the Telephone Consumer Protection Act (TCPA) of 1991, as amended; (k) the Driver's Privacy Protection Act of 1994, as amended; (l) the Communications Assistance for Law Enforcement Act of 1994, as amended; (m) the Telecommunications Act of 1996, as amended; (n) the Health Insurance Portability and Accountability Act (HIPAA) of 1996, as amended; (o) the Children's Online Privacy Protection Act (COPPA) of 1998, as amended; (p) the Financial Modernization Act (Gramm-Leach-Bliley Act (GLBA)) of 2000, as amended; (q) state laws governing the use of electronic communications, e.g., email, text messaging, telephone, paging, and faxing; (r) state laws governing the use of information collected online, state laws requiring privacy disclosures to consumers, state data-breach notification laws, state laws investing individuals with rights in or regarding data about such individuals and the use of such data, and any state laws regarding the safeguarding of data, including encryption; and (s) any relevant federal or state guidelines or recommended best practices for information security and data privacy, including, but not limited to, the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework) and Federal Trade Commission (FTC) privacy guidelines.[85]

85. The defined term of Privacy Laws listed above provides myriad privacy-related laws that may apply to a host of regulated industries. Parties to

ii. "Foreign Information Security and Data Privacy Laws" shall mean (a) the Directive 95/46/EC of the Parliament and of the Council of the European Union of 24 October 1995 on the protection of individuals with regard to the collection, use, disclosure, and processing of personal data and on the free movement of such data and any other applicable laws relating to the processing of personal data, including Directive 2002/58/EC as amended and all related regulations, regulatory codes of practice and guidance issued from time to time, including from the European Commission, and other relevant data protection supervisory authorities; (b) the corresponding national rules, regulations, codes, orders, decrees, and related rulings of the member states of the European Union; (c) the Personal Information Protection and Electronic Documents Act (Canada) and Canada's Anti-Spam Legislation; and (d) any rules, regulations, codes, orders, decrees, and related rulings concerning personal data and the privacy, data protection, or data-transfer issues regarding the same implemented in Canada or other non-U.S. countries.[86]

---

a transaction are encouraged to customize the Privacy Laws definition to align with their given industry (e.g., healthcare, telecommunications, retail).

86. International law should also be considered when complying with data security laws. Particularly, when transferring data of European Union (EU) citizens, the seller should comply with the European Union Privacy Directive (Directive 95/46/EC) and must comply with model contracts, binding corporate rules, or other standards when transferring personal data outside the EU. Please note that foreign privacy standards as used in cross-border data transfers with the EU are undergoing significant revisions as per the EU-U.S. Privacy Shield Framework.

2. Information Security Measures and Standards.

a. Sample contractual language:

i. Information Security Measures. Schedule [ ] sets forth a true and complete list of the Company's information security and data protection policies, programs, and procedures that: (i) include administrative, technical, personnel, organizational, and physical safeguards designed to protect the security, confidentiality, and integrity of transactions, data, and other information in the Company's Information Systems, and (ii) are designed to protect against unauthorized or unlawful access to the Company's Information Systems and the systems of any third-party service providers that have access to the Information Systems. The Company has at all times been in compliance with the policies, programs, and procedures set forth on Schedule [ ].

b. Pertinent defined term(s):

i. "Information Systems" means the computer software, computer firmware, computer hardware (whether general purpose or special purpose), telecommunications, equipment, controlled networks, peripherals, and computer systems, including any outsourced systems and processes under the Company's control, and other similar or related items of automated, computerized, and/or software systems that are owned, licensed, leased, or controlled by the Company and used or relied on in connection with the Company's business, but excluding the public Internet.

3. User Privacy and Information Security Policies.

a. Sample contractual language:

i. User Privacy Policy. Schedule [ ] sets forth a true and complete list of each of the Company's privacy policies regarding the collection, storage, use, and distribution of Personal Information. Each privacy policy of the Company has commercially reasonable information security and data protection controls in place, consistent with general industry practice based on the type of data and degree of risk associated with Personal Information, designed to protect the security and confidentiality of Personal Information (i) against any threats or hazards to the security and integrity of Personal Information and (ii) against any unauthorized access to or use of Personal Information contrary to this Agreement or any applicable Privacy Laws. The Company is in compliance, in all material respects, with its stated privacy policies set forth in Schedule [ ], and has maintained such compliance, in all material respects, for the past [ ] years.

ii. Information Security Policy. Schedule [ ] contains a true and complete list of all of the Information Systems that are material to the operation of the business of the Company or the business of the Company's customers, not including off-the-shelf products. If such Information Systems are operated or hosted by an outsourcer or other third-party provider, the identity and contact information for the third-party provider is disclosed on Schedule [ ]. None of the Information Systems depend upon any technology or information of any third party (other than the public Internet). Such Information Systems

are sufficient for the conduct of the Company's business as currently conducted and as anticipated to be conducted by the Buyer. The Company uses commercially reasonable means, consistent with industry practice and state of the art technology generally available to the public, to protect the security and integrity of all the Information Systems set forth in Schedule [ ]. As set forth on Schedule [ ], the Company has implemented and maintains information security and data protection policies, programs, and procedures to ensure the security of the Information Systems. Furthermore, the Company's use of the Information Systems does not exceed the scope of the rights granted to the Company with respect to those rights, including any applicable limitation upon the usage, type, or number of licenses, users, hardware, time, services, or systems.

b. Pertinent defined term(s):

   i. "Personal Information" means any information that relates to an identified or identifiable individual, including name, address, telephone number, email address, username and password, photograph, government-issued identifier, persistent-device identifier,

or any other data used or intended to be used to precisely identify an individual.[87, 88]

ii. *See* 2(b)(i), *supra*, for an example definition of "Information Systems."

4. Information Security and Data Privacy Third-Party Contractual Obligations.

a. Sample contractual language:

i. Contractual Compliance. Schedule [ ] sets forth a true and complete list of each agreement and Contract with a third party that provides the Company with consumer data, including privacy policies relating to data privacy, security, or breach notification (including provisions that impose conditions or restrictions on the collection, use, disclosure, transmission, destruction, maintenance, storage, or safeguarding of Personal Information). Schedule [ ] sets forth each Contract in which a Security Breach of the

87. Companies may also handle Personally Identifiable Information (PII). PII is defined by the NIST as being "(1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." *Glossary*, NAT'L INST. OF STANDARDS & TECH., https://csrc.nist.gov/glossary/term/personally-identifiable-information (last visited May 9, 2019). Common examples of PII include names (e.g., full name, alias, maiden name), personal identification numbers (e.g., driver's license number, financial account number, credit card number), addresses (e.g., street address, workplace address, email address), or personal characteristics (e.g., facial images, fingerprints, handwriting).

88. Personal Information relates to both consumer data and employee data. Even for companies that do not possess consumer PII, these representations and warranties will be relevant to any employee data that will be assumed or transferred in connection with a stock or asset purchase.

Information System would result in a material breach of the terms of agreement. Schedule [ ] sets forth each Contract that requires the Company to notify any affected individual in the case of a Security Breach of the Information Systems. The Company is in compliance in all material respects with the terms of each of the Contracts listed on Schedules [ ], [ ], and [ ] and has maintained such compliance, in all material respects, for the past [ ] years. The Company includes in each of its Contracts with third parties that process, store, or otherwise handle Personal Information on behalf of the Company, contractual provisions that the third parties will comply with the Company's Information Security and Data Privacy policies, as set forth in Schedules [ ] and [ ], respectively, and all applicable Information Security and Data Privacy Laws in connection with their activities for the Company[, except as set forth in Schedule [ ], and has included such contractual provisions, in all material respects, for the past [ ] years.

b. Pertinent defined term(s):

   i. "Security Breach" means any act or omission that compromises either the security, confidentiality, or integrity of Personal Information, or compromises the physical, technical, administrative, or organizational safeguards put in place by the Company that relate to the protection of the security, confidentiality, or integrity of Personal Information.
   ii. *See* 1(b)(i) and 1(b)(ii), *supra*, for example definitions of "Information Security and Data Privacy Laws" and "Foreign Information Security and Data Privacy Laws."

iii. *See* 3(b)(i), *supra*, for an example definition of "Personal Information."

5. Data Access Policies.

a. Sample contractual language:

i. Data Access Policies. Schedule [ ] contains a true and complete list of the Company's data-access policies and procedures, setting forth (i) the transit of the Company's data and data flows, including, but not limited to, the Company's network topology, databases, document management systems, and any cross-border data transfers outside of the Territory; (ii) the Company's data-classification system and methodology; (iii) the Company's data collection and retention processes; and (iv) the requirements for granting or revoking access to Personal Information contained in the Company's Information Systems. The Company is currently in compliance with each of the data-access policies and procedures set forth on Schedule [ ] and has maintained such compliance, in all material respects, for the past [ ] years. The Company has taken commercially reasonable steps to protect and maintain the integrity and confidential nature of the Personal Information provided to the Company in reliance on the Company's data-access policies, in all material respects, for the past [ ] years.

b. Pertinent defined term(s):

i. *See* 3(b)(i), *supra*, for an example definition of "Personal Information."

ii. *See* 2(b)(i), *supra*, for an example definition of "Information Systems."

6. Information Security and Data Privacy Complaints and Investigations.

a. Sample contractual language:

i. Information Security and Data Privacy Litigation. Except as set forth in Schedule [ ], to the Company's knowledge, there are no pending or threatened claims, charges, investigations, violations, settlements, civil or criminal enforcement actions, lawsuits, or other court actions against the Company that allege either (i) a material security breach of information security, including, but not limited to, a network intrusion, incident involving the Company's Personal Information, or a data breach of the Company's Information Systems; or (ii) a violation of any Person's privacy, personal, or confidential rights under the Company's information security or data privacy practices, other than those listed in Schedules [ ] and [ ], or any Information Security and Data Privacy Laws.[89]

b. Pertinent defined term(s):

i. *See* 3(b)(i), *supra*, for an example definition of "Personal Information."
ii. *See* 2(b)(i), *supra*, for an example definition of "Information Systems."
iii. *See* 1(b)(i) and 1(b)(ii), *supra*, for example definitions of "Information Security and Data Privacy Laws"

89. In the event that a known material issue exists, buyers may require a purchase-price adjustment or, alternatively, a line-item indemnity. *See* Sections IV(B)–(C), *supra,* for a discussion on those considerations. The magnitude and severity of any identified issues will dictate whether a purchase-price adjustment or a special indemnity is a more suitable risk-shifting alternative.

and "Foreign Information Security and Data Privacy Laws."

7. Security Breaches and Unauthorized Use of Personal Information.

a. Sample contractual language:

i. Unauthorized Access and Security Breaches. To the Company's knowledge, and except as set forth on Schedule [ ], there has been no breach of the Information Systems or security of any personally identifiable or confidential data, including any unauthorized access to, acquisition of, disclosure of, or loss of data possessed or controlled by the Company, except in each case as would not, individually or in the aggregate, reasonably be expected to have a Material Adverse Effect, and the Company has not received any written notices or complaints from any Person with respect to any breach.

b. Pertinent defined term(s):

i. *See* 2(b)(i), *supra*, for an example definition of "Information Systems."

8. Effect of the Transaction on Personal Data.

a. Sample contractual language:

i. Effect of the Transaction. Neither (i) the execution, delivery, or performance of this Agreement, (ii) the consummation of any of the transactions contemplated by this Agreement (or any of the other ancillary agreements), nor (iii) the Buyer's possession or use of the Personal Information or any data or information in the Company's possession, will result in any breach or violation of any internal privacy

policy of the Company [as listed in Schedule [ ]], Contract [as listed in Schedule [ ]], or any Information Security and Data Privacy Laws pertaining to the collection, use, disclosure, transfer, or protection of Personal Information, except in each case as would not, individually or in the aggregate, reasonably be expected to have a Material Adverse Effect. Upon the Closing of this Transaction, the Buyer will continue to have the right to use such Personal Information on identical terms and conditions as the Company enjoyed immediately prior to the Closing.[90]

b. Pertinent defined term(s):

i. *See* 3(b)(i), *supra*, for an example definition of "Personal Information."

ii. *See* 1(b)(i) and 1(b)(ii), *supra*, for example definitions of "Information Security and Data Privacy Laws" and "Foreign Information Security and Data Privacy Laws."

9. Cybersecurity Insurance.

a. Sample contractual language:

i. Insurance. Schedule [ ] sets forth a true and complete list of all current policies or binders of fire, liability, workers' compensation, property, casualty, errors and omissions, employment practices, crime,

90. To ensure compliance with this representation, the parties should consider whether any constraints on the target company's ability to transfer the data exist. Constraints will often be in the form of pre-existing contractual restrictions and found in the target company's existing privacy policies. Even if the target company has valid ownership rights to certain data, the buyer may not have unrestricted use of—or transferability rights to—that data.

cybersecurity, and other forms of insurance owned or held by the Company (collectively, the "Insurance Policies"). True and complete copies of the Insurance Policies have been made available to the Buyer. The Insurance Policies are in full force and effect. The Company has not received any written notice of cancellation of, premium increase with respect to, or alteration of coverage under any of the Insurance Policies. All premiums due on the Insurance Policies have either been paid or, if due and payable prior to Closing, will be paid prior to Closing in accordance with the payment terms of each Insurance Policy. All of the Insurance Policies (a) are valid and binding in accordance with their terms; (b) are, to the Company's knowledge, provided by carriers who are financially solvent; and (c) have not been subject to any lapse in coverage. There are no claims related to the business of the Company pending under any of the Insurance Policies for which coverage has been questioned, denied, or disputed, or for which there is an outstanding reservation of rights. The Company is not in default under, nor has it otherwise failed to comply with, in any material respect, any provision contained in any Insurance Policy. The Insurance Policies are of the type and in the amounts customarily carried by Persons conducting a business similar to the Company, and are sufficient for compliance with all applicable Laws, including Information Security and Data Privacy Laws and Contracts to which the Company is a party or by which it is bound.

b. Pertinent defined term(s):

i. *See* 1(b)(i) and 1(b)(ii), *supra*, for example definitions of "Information Security and Data Privacy Laws" and "Foreign Information Security and Data Privacy Laws."

APPENDIX C:
DUE-DILIGENCE REQUESTS

In connection with the potential acquisition and subject to the mutual nondisclosure agreement, please provide us with the following materials. If certain materials have already been provided, are unavailable, or are generally inapplicable, please indicate so in your response to this request. Please note that our due-diligence investigation is ongoing, and we will submit supplemental due-diligence requests as necessary.

Unless otherwise indicated, any responsive documents should be made available for all periods subsequent to [DATE] and should include all amendments, supplements, or other ancillary documents.

DATA PRIVACY AND SECURITY		
Request	**Response**	**Status**
I. Data		
a. Describe and identify the location of: i. Consumer PII ii. Employee PII iii. Financial information iv. HIPAA data v. Aggregated/de-identified consumer information		
b. Identify and generally describe trade secret information and other proprietary know-how.		
c. List and describe databases material to the organization.		
d. List and describe other data repositories.		

DATA PRIVACY AND SECURITY		
Request	**Response**	**Status**
II. Hardware		
a. List and describe all in-house servers, Network Attached Storage (NAS) document management systems, data warehouses, and other hardware and computing assets belonging to the organization.		
b. List and describe all owned personal computers.		
c. List and describe encryption technologies employed on owned hardware.		
d. Provide details of any plans for significant software or IT systems upgrades within the next 12 months, indicating for each planned upgrade the status of completion or negotiation of related agreements and an estimate of the associated capital expenditures.		
e. Provide details of any material failures or interruptions in the use of the organization's IT systems in the past 12 months, indicating for each item the status of remediation and the actual or anticipated impact on the organization's business.		

DATA PRIVACY AND SECURITY		
Request	**Response**	**Status**
III. Software		
a. Provide a list describing all proprietary technology and computer software owned or being developed by or for the organization.		
b. Provide a list describing all: i. material third-party computer software used by the organization or incorporated into any software or product of the organization; and ii. open-source, freeware, or other software having similar licensing or distribution models used by the organization or incorporated into any software or product of the organization.		
c. Provide details (and copies where available) of material support agreements relating to the organization's software/hardware (including maintenance, disaster recovery, and outsourcing arrangements).		

DATA PRIVACY AND SECURITY		
Request	**Response**	**Status**
d. Provide details of any significant errors or performance issues experienced by the organization in the previous 12 months in connection with the organization's software/hardware, and steps that the organization has taken to resolve those errors or performance issues.		
e. Provide copies of all agreements relating to the provision of IT, data, or internet-related products or services to or by the organization.		
IV. Policies		
a. Describe the organization's collection, use, transmission, storage, or disposal of personal, financial, and health information of its customers or other individuals.		
b. Provide copies of all current and historical privacy and data protection, retention, storage, classification, destruction, or security policies and practice manuals of the organization, including, without limitation, all privacy policies and procedures for the organization's use and disclosure of customer/client or personal information.		

DATA PRIVACY AND SECURITY		
Request	**Response**	**Status**
c. Provide details of any training that is given to the employees on data protection, and the appointment of data protection officers.		
d. Provide copies of any other documentation and information regarding the organization's collection, use, storage, or disposal of customer or personal information.		
e. Describe and furnish copies of the organization's trade-secret policies and the measures taken to protect trade secrets and proprietary know-how.		
f. Provide details of any backup, business-continuity, and disaster-recovery plans and procedures, facilities management, and ongoing support arrangements.		
g. Provide copies of customer-facing website privacy policies and terms of use.		
h. Provide copies of all current and historical breach notification and response plans and procedures.		

DATA PRIVACY AND SECURITY		
Request	**Response**	**Status**
V. Agreements; Vendors		
a. Provide copies of all agreements that the organization has with any service providers and other vendors that (i) receive from or on behalf of the organization any customer or personal information that is subject to any data privacy or security requirements, or (ii) have access to the organization's networks.		
b. List and describe all hosting, cloud-computing, or collaboration services.		
c. Provide details regarding any data processor appointed by the organization and copies of all such agreements.		
d. Provide details of any agreements under which the organization has been appointed a data processor and copies of any applicable agreements.		
e. Provide details of any agreements entered into by the organization or its subsidiaries relating to the transfer of personal data out of the European Economic Area.		

DATA PRIVACY AND SECURITY		
Request	**Response**	**Status**
f. Provide copies of all agreements that the organization has with any third parties that act as the organization's agents or contractors and that receive customer or personal information subject to any statutory or regulatory data privacy or security requirements from or on behalf of the organization. Please provide copies of any reports or audits (internal or external, and including any SAS 70 and SSAE 16 audits) that have been performed on the information security program(s) of such third parties.		
VI. Litigation; Enforcement		
a. List and describe (including an estimate of the amount of the organization's contingent liability) any claims, charges, arbitrations, grievances, actions, suits, investigations, or proceedings involving the IT or data assets of the organization or its affiliates in connection with the organization currently outstanding, outstanding at any time within the last five (5) years, or pending, threatened, or contemplated.		

DATA PRIVACY AND SECURITY		
Request	**Response**	**Status**
b. List, describe, and provide a copy of all unsatisfied or outstanding judgments, writs, injunctions, decrees, awards, or orders of any court or other governmental agency or body relating to or affecting the IT or data assets of the organization.		
c. Provide a summary of all reports to and correspondence with governmental agencies involving the data of the organization.		
d. Provide copies of all of the organization's notifications to and requests for authorization from the relevant supervisory authority under applicable national data protection law.		
e. Provide details of any complaints, notices, or other correspondence relating to the organization from the relevant national supervisory authority or any other party in relation to data protection, and copies of all material correspondence.		

DATA PRIVACY AND SECURITY		
Request	**Response**	**Status**
f. Provide details of any audits or investigations (internal or external, including any SAS 70 and SSAE 16 audits) relating to the information security practices of the organization (or any service providers or other vendors that receive customer or personal information from or on behalf of the organization), and copies of any reports prepared by or for the organization concerning the implementation of information security program(s) by the organization or such service providers or other vendors.		
g. Provide details of any complaints, claims, proceedings, or litigation relating to the organization's information security practices, and copies of any notices, pleadings, correspondence, or other relevant documents.		
h. Provide details of any actual or potential data and information security breaches, unauthorized use or access of the organization's IT systems or data, or data and information security issues affecting the organization in the past 5 years.		

DATA PRIVACY AND SECURITY		
Request	**Response**	**Status**
i. Provide details of any actual or potential hacking, viruses, or other attacks on the organization's websites or social media sites in the past 5 years, indicating for each item the status of remediation and the actual or anticipated impact on the organization's business.		
j. Describe any insurance coverage for business losses related to the organization's computer systems.		
k. List and describe any known lapses in insurance coverage or insurance claims made or pending with respect to the insurance policies relating to the organization's computer systems.		

THE SEDONA CONFERENCE COMMENTARY ON LEGAL HOLDS, SECOND EDITION: THE TRIGGER & THE PROCESS

A Project of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1)

Author:
The Sedona Conference

Drafting Team:

Jeffrey Goreski
Brad Harris
Taylor M. Hoffman
Laura A. Hunt
Henry J. Kelston
Geoffrey C. Klingsporn
Corey Lee
Robert L. Levy
J. Alex Lovo
Anthony S. Lowe
Kathy K. Malamis
Leeanne Mancari
Jana Mills
Jesse Weisshaar

WG1 Steering Committee Liaisons and Editors-in-Chief:
Kevin F. Brady
Timothy M. Opsitnick
Gina Trimarco

Drafting Team Leaders:
John Tredennick
Gina Trimarco

Staff Editors:
David Lumia
Susan McClain

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference Working Group 1. 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 Legal Holds, Second Edition: The Trigger & The Process*, 20 SEDONA CONF. J. 341 (2019).

PREFACE

Welcome to the final, June 2019, version of The Sedona Conference *Commentary on Legal Holds, Second Edition: The Trigger & The Process*, a project of The Sedona Conference Working Group on Electronic Document Retention and Production (WG1). 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, and intellectual property rights. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

In 2007, The Sedona Conference published, for public comment, the First Edition of the *Commentary on Legal Holds: The Trigger & The Process*, which provided practical guidelines for determining when the duty to preserve relevant information arises as well as the scope of preservation. In 2010, The Sedona Conference published its final, post-public comment version of the First Edition, which reflected the evolution of law and best practices as well as informal and formal suggestions and comments that The Sedona Conference received since the 2007 public comment version was published. After the 2015 amendments to the Federal Rules of Civil Procedure, updating the 2010 *Commentary* was a topic of dialogue at both the Annual and Midyear WG1 Meetings in 2016. The subsequently formed Legal Holds drafting team presented redlined drafts to the WG1 membership and entertained feedback at both the Annual and Midyear Meetings in 2017. The guidelines and commentary in this Second Edition account for the 2015 amendments emphasizing proportionality in discovery and sharpening the analysis of sanctions for the loss of discoverable electronically stored information (ESI), developments in state and federal case law on preservation and spoliation, new and novel sources of ESI requiring preservation and collection, and advances in electronic

document management technology. The Second Edition also includes new guidance on how organizations should address data protection laws and regulations that may affect an organization's ability to implement legal hold data preservation measures outside of the United States. Finally, this Second Edition incorporates the knowledge and guidance embodied in *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, which was published in October 2017. This Second Edition was first published for public comment in December 2018. Where appropriate, the comments received during the public comment period have now been incorporated into this final version of the *Commentary on Legal Holds, Second Edition: The Trigger & The Process*.

The Sedona Conference acknowledges the efforts of Drafting Team Leaders John Tredennick and Gina Trimarco, both of whom were invaluable to driving this project forward. Gina also serves as one of the Editors-in-Chief and Steering Committee Liaisons, along with Kevin F. Brady and Timothy M. Opsitnick—we are thankful for their service. For their efforts and commitments in time and attention to this project, we are grateful to our drafting team members: Jeffrey Goreski, Brad Harris, Taylor M. Hoffman, Laura A. Hunt, Henry J. Kelston, Geoffrey C. Klingsporn, Corey Lee, Robert L. Levy, J. Alex Lovo, Anthony S. Lowe, Kathy K. Malamis, Leeanne Mancari, Jana Mills, and Jesse Weisshaar. Finally, we thank Thomas Y. Allman, Erick Drobinski, Philip Favro, Ruth Anne French-Hodson, Ted S. Hiser, Will Hoffman, Charles R. Ragan, David C. Shonka, Ariana J. Tadler, and Kenneth J. Withers, as well as The Honorable Xavier Rodriguez, all of whom contributed to this project, either initially through their research efforts or later at the editorial stage.

We encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series

is open to all. The Series includes WG1 and several other Working Groups in the areas of international electronic information management, discovery, and disclosure; patent damages and patent litigation best practices; data security and privacy liability; trade secrets; and other "tipping point" issues in the law. 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
June 2019

TABLE OF CONTENTS

I. INTRODUCTION

Information lies at the core of civil litigation and our legal discovery system. Accordingly, the law has developed rules regarding the way information should be treated in connection with litigation. One of the principal rules is that when an organization reasonably anticipates litigation (as either the initiator or the target of litigation), the organization has a duty to undertake reasonable actions to preserve paper documents, electronically stored information (ESI), and tangible items that are relevant to the parties' claims and defenses and proportional to the needs of the case.[1] Separate obligations may be imposed by statutes or other rules when an investigation is reasonably anticipated.[2] The use of a "legal hold" has become a common means by which organizations initiate meeting their preservation obligations.

This *Commentary* provides practical guidelines for determining (a) when the duty to preserve discoverable information arises, and (b) once that duty is triggered, what should be preserved and how the preservation process should be undertaken.

Commentary Terminology

Before diving into the substance of this *Commentary*, a brief explanation is in order about the terms used throughout.

---

1. FED. R. CIV. P. 26(b)(1). *See* FED. R. CIV. P. 37(e); The Sedona Conference, *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Production*, 19 SEDONA CONF. J. 1, 93–96 (2018) [hereinafter *The Sedona Principles, Third Edition*].

2. *Id.* at 93. *See In re* Delta/Airtran Baggage Fee Antitrust Litig., 770 F. Supp. 2d 1299, 1307–08 (N.D. Ga. 2011) (recognizing that preservation obligations apply to government investigations). This *Commentary* applies the legal hold standard to government investigations in civil contexts. We note that separate preservation obligations may be imposed by statutes when a government investigation is reasonably anticipated. Criminal investigations are outside the scope of this *Commentary*.

- "Legal hold" refers to the process by which an organization seeks to satisfy an obligation to preserve, initially by issuing a communication designed to suspend the normal disposition of information pursuant to a policy or through automated functions of certain systems. The term "legal hold notice" is used when referring to the actual communication.
- The term "legal hold" is used rather than "litigation hold" (or other similar terms)[3] to recognize that a legal hold may apply in non-litigation circumstances (e.g., pre-litigation, government investigation, or tax audit).
- "Discoverable information" refers to information that is relevant to the parties' claims and defenses and proportional to the needs of the case.[4] This phrase is used in lieu of the phrases "potentially relevant information" and "relevant information," from earlier versions of this *Commentary* (and in other Sedona Conference publications), to clarify that both relevance and proportionality apply to preservation decisions.

---

3. *See* The Sedona Conference, *The Sedona Conference Glossary: E-Discovery & Digital Information Management (Fourth Edition)*, 15 SEDONA CONF. J., 305, 336–37 (2014).

4. *Cf.* FED. R. CIV. P. 26(b)(1). The definition of "discoverable information" is not meant to imply that the duty to preserve does not extend to privileged information because it does. *See* EPAC Techs., Inc. v. Thomas Nelson, Inc., No. 3:12-CV-00463, 2016 WL 11339512, at *11, n.28 (M.D. Tenn. Jan. 29, 2016) ("[T]he duty to preserve applies to relevant, potentially-privileged material, even if such material is ultimately exempt from discovery."); Taylor v. Mitre Corp., No. 1:11-cv-01247, 2012 WL 5473715, at *6 (E.D. Va. Sept. 10, 2012).

- "Litigation" refers primarily to civil litigation. State or federal statutes may impose obligations in the face of criminal proceedings or government investigations.
- Where appropriate, the term "organization" includes natural persons, government agencies, and other legal entities, for example, corporations.

A. Legal Framework for the Duty to Preserve

The preservation obligation typically arises from the common-law duty[5] to avoid spoliation of relevant evidence that may be used at trial[6] and is not explicitly defined in the Federal Rules of Civil Procedure. Nonetheless, the Federal Rules and state counterparts governing the scope and conduct of discovery provide a framework for interpreting the duty to preserve, which the guidelines set forth below interpret and apply.

1. Requiring Early Consideration of Preservation

In 2006, Rule 26(f)(2) was amended to require discussion of "issues about preserving discoverable information" when the parties meet and confer prior to the Scheduling Conference required by Rule 16(b). The Advisory Committee intended that,

---

5. *See* Robert Keeling, *Sometimes Old Rules Know Best: Returning to Common Law Conceptions of the Duty to Preserve in the Digital Information Age*, 67 CATH. U. L. 67 (2018) (providing a historical background of the common law duty to preserve and comparing to the application of today's standard).

6. *See, e.g.*, Silvestri v. Gen. Motors Corp., 271 F.3d 583 (4th Cir. 2001) (applying the federal common law of spoliation); Armory v. Delamirie, (1722) 93 Eng. Rep. 664 (K.B.) (*Armory* is recognized as the origin of the doctrine of spoliation. A chimney sweep found a jewel, took it to a jeweler to be appraised, and the jeweler subsequently lost it. The chimney sweep sued the jeweler for the loss of the jewel, and the court held that he was entitled to an inference that the stone was "of the finest water.").

by encouraging early discussion, parties would reach agreement on reasonable preservation steps.

In 2015, Rule 26(f)(3)(C) was amended to require that the parties' views on preservation of ESI be included in the discovery plan. In addition, Rule 16(b)(3)(B)(iii) now explicitly permits a scheduling order to address ESI preservation. The Committee noted that "[o]nce litigation has commenced, if the parties cannot reach agreement about preservation issues, promptly seeking judicial guidance about the extent of reasonable preservation may be important," and "[p]reservation orders may become more common."

2. Proportionality and Accessibility

In 2015, Rule 26(b)(1) was amended to clarify that proportionality must be analyzed when determining the proper scope of discovery.[7] Under the amended Rule and subject to possible limitations for inaccessible ESI,[8] "[p]arties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense and *proportional* to the needs of the case . . . ."[9]

---

7. FED. R. CIV. P. 26(b)(1).

8. FED. R. CIV. P. 26(b)(2)(B) provides that information stored in sources that are not reasonably accessible because of undue burden or cost are not initially discoverable; a court, however, may order that such information be produced for "good cause." Moreover, the 2006 advisory committee note to the Rule cautions that identification of ESI as not reasonably accessible does not relieve the party of its duty to preserve evidence. In addition, *The Sedona Principles, Third Edition* warns that unilateral preservation decisions are not without risk. *Supra* note 1, at 96–97.

9. FED. R. CIV. P. 26(b)(1) (emphasis added). *See* FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment ("Another factor in evaluating the reasonableness of preservation efforts is proportionality. The court should be sensitive to party resources; aggressive preservation efforts can be extremely costly, and parties (including governmental parties) may have limited staff

3. Requiring Reasonable Efforts—Not Perfection

The principle that an organization has a duty to preserve discoverable information in the anticipation or conduct of litigation is easy to state. Its application in practice, however, often requires careful analysis and difficult decisions. Nonetheless, each day, organizations must apply the principle to real-world circumstances, first confronting the issue of whether an obligation is triggered, and then determining the scope of their obligation.

The 2015 Amendments to the Federal Rules of Civil Procedure provide a measure of comfort and guidance on these fronts, as they were intended to reduce both the costs generally associated with ESI discovery and fears about making preservation decisions that might be second-guessed in later spoliation motion practice.[10] The Rules recognize that the situation described in 1993 as an information "explosion" has been exacerbated by the geometric increase in the volume of information (90 percent of the data in the world has been generated over the last two years[11]), as well as the variety of constantly emerging data types, and the speed with which they evolve.

In particular, amended Rule 37(e) regarding the failure to preserve ESI imposes sanctions "only if the lost [ESI] should

---

and resources to devote to those efforts."). *See also* Little Hocking Water Assn., Inc. v. E.I. Du Pont de Nemours & Co., 94 F. Supp. 3d 893, 918 (S.D. Ohio 2015) ("[T]he scope of the duty to preserve is a highly fact-bound inquiry that involves considerations of proportionality and reasonableness.") (quoting Tracy v. NVR, Inc., No. 04-cv-6541L, 2012 WL 1067889, at *29 (W.D.N.Y. Mar. 26, 2012)).

10. *See* FED. R. CIV. P. 26(b)(1) and FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment.

11. Bernard Marr, *How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read*, FORBES (May 21, 2018), https://www-forbes-com.cdn.ampproject.org/c/s/www.forbes.com/sites/bernard-marr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/amp/.

have been preserved in the anticipation or conduct of litigation and the party failed to take reasonable steps to preserve it."[12] Further, the Rule prohibits severe sanctions unless a "party acted with the intent to deprive another party."[13]

In addition, "[d]ue to the ever-increasing volume of electronically stored information and the multitude of devices that generate such information, perfection in preserving all relevant electronically stored information is often impossible."[14] Thus, the "rule recognizes that 'reasonable steps' to preserve suffice; it does not call for perfection."[15] *The Sedona Principles, Third Edition*[16] similarly suggests that preservation obligations require "reasonable and good faith efforts," and that it is "unreasonable to expect parties to take every conceivable step or disproportionate steps to preserve each instance of relevant electronically stored information."[17]

While the amended Rule 37(e) by its terms only applies to ESI, the proposition that preservation requires reasonableness and good faith has been broadly applied—even outside the

12. FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment. The note also advises that "it is important not to be blinded to [the reality that preservation decisions may be based on limited information] by hindsight arising from familiarity with an action as it is actually filed." *Id*.

13. FED. R. CIV. P. 37(e)(1) and (2).

14. FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment.

15. *Id.* ("This rule recognizes that 'reasonable steps' to preserve suffice; it does not call for perfection."); Agerbrink v. Model Service LLC, No. 14 Civ. 7841, 2017 WL 933095, at *5 (S.D.N.Y. Mar. 8, 2017) ("The standard for evaluating discovery is reasonableness, not perfection.").

16. *See supra* note 1, Principle 5 and Cmts. 5.d. and 5.e., at 106–09.

17. *Id*. at Principle 5. *But see* Franklin v. Howard Brown Health Center, No. 17 C 8376, 2018 WL 4784668 (N.D. Ill. Oct. 4, 2018) (holding that defendant failed to take reasonable steps to preserve relevant emails and instant messages when its counsel neglected to oversee the preservation process after perfunctorily issuing litigation hold).

context of ESI—by numerous courts.[18] The amended Rule 37(e) refines the old concept of "good faith," explaining in the Advisory Committee Notes that "the 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."[19]

---

18. *See, e.g.*, Chin v. Port Auth. of N.Y. & N.J., 685 F.3d 135, 161–63 (2d Cir. 2012); Snider v. Danfoss, LLC, 15 CV 4748, 2017 WL 2973464 (N.D. Ill. July 12, 2017); Rimkus Consulting Grp., Inc. v. Cammarata, 688 F. Supp. 2d 598, 613 (S.D. Tex. 2010) ("Whether preservation or discovery conduct is acceptable in a case depends on what is reasonable"); Witt v. GC Servs. Ltd. P'ship, 307 F.R.D. 554, 568 (D. Colo. 2014) ("The court does not expect perfection and will not 'infer nefarious intent or bad faith' from 'ordinary discovery errors.'") (citation omitted); Fisher v. Ciba Specialty Chems. Corp., No. 03-0566-WS-B, 2007 WL 987457, at *3 (S.D. Ala. Mar. 30, 2007) ("The rules of discovery do not demand perfection, clairvoyance, or miracle workings in the production of documents.").

For hard-copy documents and tangible things, federal courts continue to apply circuit-specific case law—including the use of inherent authority—to allegations of spoliation of such evidence. *E.g.*, EEOC v. GMRI, Inc., No. 15-20561-civ, 2017 WL 5068372, at *2 (S.D. Fla. Nov. 1, 2017) (applying Rule 37(e) to alleged spoliation of email and Eleventh Circuit common law to alleged spoliation of paper documents); Jimenez v. Menzies Aviation Inc., No. 15-cv-2392, 2016 WL 3232793 (N.D. Cal. June 13, 2016) (not applying amended Rule 37(e) when addressing loss of hard-copy documents). Likewise, state courts continue to apply state-specific law to ESI spoliation claims. In both cases, most courts will take into consideration at least: (1) the party's obligation to preserve, (2) the party's culpability in losing the information, and (3) the effect that losing such information has on the opposing party's case. Moody v. CSX Transp., Inc., 271 F. Supp. 3d 410, 426–32 (W.D.N.Y. 2017) (In a personal injury action, the defendant railroad did not take reasonable steps to preserve train's event recorder data, but sanctions for the destruction of a laptop containing the relevant data would be limited under Rule 37(e), despite the plaintiff's argument that the laptop was "physical evidence" as opposed to "electronically stored information.").

19. FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment.

Thus, whenever an organization makes a preservation decision, or a court analyzes a claim of spoliation, the guiding principle is reasonableness under the circumstances. Whether a party issued a legal hold notice and, if so, when, how, and to whom, are all important factors, although not dispositive, in determining the reasonableness of the party's preservation efforts.

B. Triggering the Duty to Preserve

The duty to preserve discoverable information is certainly triggered when a complaint is served. The duty to preserve, however, may arise earlier, if an organization is bringing the action or is the target of the action. The touchstone is "reasonable anticipation" or "reasonably foreseeable."[20] The standard is an objective one, "asking not whether the party in fact reasonably foresaw litigation, but whether a reasonable party in the same factual circumstances would have reasonably foreseen litigation."[21]

Determining if a duty to preserve has been triggered is fact-specific and not amenable to a one-size-fits-all or checklist approach.[22] Instead, a number of factors should be considered,

---

20. *See* Alter v. Rocky Point Sch. Dist., No. 13-1100, 2014 WL 4966119, at *8 (E.D.N.Y. Sept. 30, 2014) ("The duty to preserve arises, not when litigation is certain, but rather when it is 'reasonably foreseeable.'") (quoting Byrnie v. Town of Cromwell Bd. of Educ., 243 F.3d 93, 107 (2d Cir. 2001)); *In re* Abilify (Aripiprazole) Prod. Liab. Litig., No. 16-MD-2734, 2018 WL 4856767, *3–6 (N.D. Fla. Oct. 5, 2018) (finding that defendant did not reasonably anticipate litigation and rejecting plaintiffs' assertion that industry-wide events created a "reasonable anticipation of litigation" and a duty to preserve).

21. Micron Tech., Inc. v. Rambus Inc., 645 F.3d 1311, 1320 (Fed. Cir. 2011); *see also* Storey v. Effingham Cnty., 2017 WL 2623775, at *3 (S.D. Ga. June 16, 2017).

22. *Micron Tech., Inc.*, 645 F.3d at 1320 ("When litigation is 'reasonably foreseeable' is a flexible fact-specific standard that allows a district court to

including the level of knowledge within the organization about the claim and the risk to the organization posed by the claim. *See infra* Guidelines 1 and 4, and associated commentary. Weighing these factors will enable an organization to decide when litigation is reasonably anticipated and when a duty to take affirmative steps to preserve discoverable information has arisen.

C. Implementing the Legal Hold

Once the duty to preserve is triggered, an organization must decide what to preserve and how to preserve it. In some circumstances, the duty to preserve requires only identifying and preserving only a modest amount of information. In other circumstances, the scope of the information is broader, and the sources of the information may not be immediately known.

The proportionality principle applies to all efforts to plan and implement preservation, and in the assessment of those efforts.[23] In *Rimkus Consulting v. Cammarata*, the court noted that "[w]hether preservation or discovery conduct is acceptable in a case depends on what is *reasonable,* and that in turn depends on whether what was done—or not done—was *proportional* to that case and consistent with clearly established applicable standards."[24] Similarly, the Seventh Circuit Council on eDiscovery

exercise the discretion necessary to confront the myriad factual situations inherent in the spoliation inquiry.").

23. *See, e.g.*, FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment (One "factor in evaluating the reasonableness of preservation efforts is proportionality."); Hon. Joy Flowers Conti & Richard N. Lerrieri, *E-Discovery Ethics: Emerging Standards of Technological Competence*, FED. LAW. 28, 31 (Oct./Nov. 2015) ("Proportionality is a guiding principle in determining the breadth and extent of the preservation required" under the Federal Rules.).

24. 688 F. Supp. 2d 598, 613 (S.D. Tex. 2010) (emphasis in original).

and Digital Information[25] provides, in Principle 2.04 (Scope of Preservation), that "[e]very party to litigation and its counsel are responsible for taking reasonable and proportionate steps to preserve relevant and discoverable ESI within its possession, custody or control." [26, 27]

As has been noted by several courts, there is no broad requirement to preserve *all* information. "Must a corporation, upon recognizing the threat of litigation, preserve every shred of paper, every email or electronic document, and every backup tape? The answer is clearly, 'no.' Such a rule would cripple large corporations."[28]

---

25. Formerly the "7th Circuit E-Discovery Pilot Program," https://www.ediscoverycouncil.com/.

26. 7th Circuit Electronic Discovery Committee, *Principles Relating to the Discovery of Electronically Stored Information*, Principle 2.04, 7TH CIRCUIT COUNCIL ON EDISCOVERY AND DIGITAL INFORMATION (2d ed. Jan. 2018), https://www.ediscoverycouncil.com/sites/default/files/7thCircuitESIPilot-ProgramPrinciplesSecondEdition2018.pdf.

27. *See also* FED. R. CIV. P. 26(b)(1). Notably, the scope of discovery under Rule 26(b)(1)—as amended in December 2015—no longer includes "any matter relevant to the subject matter involved in the action" or information "reasonably calculated to lead to the discovery of admissible evidence." FED. R. CIV. P. 26(b)(1) (2006). The former phrase was removed because "[p]roportional discovery relevant to any party's claim or defense suffices," and the latter phrase was removed because it had "been used by some, incorrectly, to define the scope of discovery." FED. R. CIV. P. 26 advisory committee's note to 2015 amendment. *See also* Cole's Wexford Hotel, Inc. v. Highmark Inc., 209 F. Supp. 3d 810, 817–23 (W.D. Pa. 2016); *In re* BARD Filters Prod. Liab. Litig., 317 F.R.D. 562, 563–64 (D. Ariz. 2016).

28. Zubulake v. UBS Warburg, 220 F.R.D. 212, 217 (S.D.N.Y. 2003); *see also, e.g.*, *In re* Ethicon, Inc. Pelvic Repair Sys. Prod. Liab. Litig., 299 F.R.D. 502, 517 (S.D.W. Va. 2014) (It is "uniformly agreed that a corporation under a duty to preserve is not required to keep 'every shred of paper, every e-mail or electronic document, and every backup tape' . . . [as] such a requirement 'would cripple large corporations.'") (quoting *Zubulake*, 220 F.R.D. at 217).

The typical legal hold notice focuses on key custodians and data stewards,[29] directing them to take steps to preserve discoverable information and to prevent losses due to routine business or systems operations.

Identifying and preserving discoverable information can be a complex process. It may include creating teams to identify the sources, custodians, and data stewards of discoverable information, to define what needs to be preserved, and to coordinate with outside counsel. When ESI is at issue, personnel with particular knowledge and expertise, and the use of specific processes and technology, may be needed.[30] For large preservation efforts, a process that is planned, systemized, and scalable is useful, although *ad hoc* manual processes may be appropriate for cases involving a small number of key custodians and identifiable issues.

D. Role of Counsel

Regardless of the process employed, counsel (both in-house and outside) usually play important roles in an organization's

29. *I.e.*, persons responsible for maintaining and operating relevant computer systems, files, or databases. *See The Sedona Principles, Third Edition*, *supra* note 1, Cmt. 5.d., at 105.

30. *See, e.g.*, The Sedona Conference, *Database Principles Addressing the Preservation and Production of Databases and Database Information in Civil Litigation*, 15 SEDONA CONF. J. 171 (2014); Leidig v. Buzzfeed, Inc., 16 Civ. 542, 2017 WL 6512353 (S.D.N.Y. Dec. 19, 2017) (In a defamation suit, the plaintiffs failed to take reasonable steps to collect and preserve web-based evidence, including screenshots, email, and metadata; the court, however, noted the plaintiffs' lack of technical sophistication and "amateurish" preservation efforts, did not find intent to deprive, and limited remedies to evidentiary preclusions and instructions.).

efforts to satisfy its preservation obligation.[31] The traditional role of counsel is to advise the client of its duty to preserve discoverable information in the client's possession, custody, or control and the possible consequences if the information is not preserved.[32] But numerous decisions hold that counsel also owe an independent duty to monitor and supervise or participate in a party's efforts to comply with the duty to preserve.[33]

---

31. *See* EPAC Techs. v. HarperCollins Christian Publ'g., Case No. 3:12-cv-00463, 2018 WL 1542040, at *22 (M.D. Tenn. March 29, 2018) ("Counsel must take an active and primary role in implementing a litigation hold.").

32. ABA CIVIL DISCOVERY STANDARDS, Standard 10 (2004) ("This Standard is . . . an admonition to counsel that it is counsel's responsibility to advise the client as to whatever duty exists, to avoid spoliation issues."). *See also* Turner v. Hudson Transit Lines, Inc., 142 F.R.D. 68, 73 (S.D.N.Y. 1991) (The preservation obligation runs first to counsel, who has a duty to advise, with "corporate managers" having the responsibility to convey that information to the relevant employees.).

33. FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment (recognizing counsel's role in matters related to preservation: "It is important that counsel become familiar with their clients' information systems and digital data . . . to address these issues."); *cf.* Sunderland v. Suffolk Cty., No. CV 13-4838, 2016 WL 3264169, at *3 (E.D.N.Y. June 14, 2016) (It is counsel's obligation to "supervise and oversee the search for and production of electronically stored information and documents."); Browder v. City of Albuquerque, 187 F. Supp. 3d. 1288, 1295 (D.N.M. 2016) ("Counsel must go beyond mere notification and 'take affirmative steps to monitor compliance,'. . . to continually ensure that the party is preserving relevant evidence."); Phoenix Four, Inc. v. Strategic Res. Corp., No. 05 Civ 4837, 2006 WL 1409413, at *5 (S.D.N.Y. May 23, 2006) ("Counsel has the duty to properly communicate with its client" to ensure adequate preservation, which "would involve communicating with information technology personnel and the key players in the litigation to understand how electronic information is stored."); Zubulake v. UBS Warburg, 229 F.R.D. 422, 432 (S.D.N.Y. 2004) ("A party's discovery obligations do not end with the implementation of a 'litigation hold'—to the contrary, that's only the beginning. Counsel must oversee compliance with the litigation hold, monitoring the party's efforts to retain and produce the relevant documents."). *See also* State of Cal. Standing Comm. on Prof'l Responsibility

Following that logic, counsel's duty does not end with issuance of a legal hold notice but remains in effect as long as the client's duty to preserve exists.

E. Benefits of Implementing a Proper Legal Hold

If a party takes reasonable steps to implement a legal hold and preserve discoverable ESI, under the 2015 Amendments to Rule 37(e), that party should not be sanctioned, or have curative measures imposed upon it, even if discoverable information is lost.[34] Instead, the curative measures in Rule 37(e)(1) and (2) apply *only if* (i) the ESI was subject to a preservation obligation,[35] (ii) the organization failed to take "reasonable steps" to preserve

---

and Conduct Formal Op. No. 2015-193, *available at* https://www.calbar.ca.gov/Portals/0/documents/ethics/Opinions/CAL%202015-193%20%5B11-0004%5D%20(06-30-15)%20-%20FINAL.pdf.

34. *The Sedona Principles, Third Edition* takes the position, contrary to the express terms of Rule 37(e), that sanctions may be imposed against an incompetent spoliator, i.e., if information is lost due to the efforts of one intending to deprive a party of the use of that information in litigation even though it is otherwise restored or replaced; and there is some authority for this position. *Supra* note 1, Cmt. 14.d., at 197. *See, e.g.*, Cat3, LLC v. Black Lineage, Inc., 164 F. Supp. 3d 488, 2016 WL 154116 (S.D.N.Y. 2016); Hon. James C. Francis IV and Eric P. Mandel, *Limits on Limiting Inherent Authority: Rule 37(e) and the Power to Sanction*, 17 SEDONA CONF. J. 613 (2016). *See also* Tera Brostoff, *Reports of Death of Inherent Judicial Authority Exaggerated?*, BLOOMBERG BNA (Nov. 15, 2016) ("'37(e) didn't take action to make inherent authority unavailable. . . . [Rather, under amended rules,] [y]ou couldn't say to yourself that I don't like the fact that with 37(e) you can't get specific serious sanctions, and so I'm going to use inherent authority instead.' [In other words,] inherent authority can't be used merely to circumvent 37(e).") (quoting Judge Paul W. Grimm (D. Md. and former Federal Rules of Civil Procedure Advisory Committee member)).

35. FED. R. CIV. P. 37(e). *See also, e.g.*, Marten Transp., Ltd. v. Plattform Adver., Inc., No. 14-cv-02464, 2016 WL 492743, at *10 (D. Kan. Feb. 8, 2016) (denying sanctions under Rule 37(e) when plaintiff had no duty to preserve ESI at issue until after its destruction).

the ESI,[36] (iii) as a result, the ESI was lost,[37] and (iv) "the information cannot be restored or replaced through additional discovery."[38] And sanctions under Rule 37(e)(2) are available only if the ESI was destroyed "with the intent to deprive another party of the information's use in the litigation."[39]

F. Other Preservation Obligations

Preservation obligations also may arise and be enforced pursuant to statutes or regulations.[40] Criminal penalties at the

---

36. FED. R. CIV. P. 37(e). *See also, e.g.*, Best Payphones, Inc. v. City of New York, 1-CV-3924, 1-CV-8506, 3-CV-0192, 2016 WL 792396, at *5 (E.D.N.Y. Feb. 26, 2016) ("[T]he Court cannot find that [the party] acted unreasonably as is required for the Court to issue sanctions under Rule 37(e)."); *but see* GN Netcom v. Plantronics, Inc., No. 12-1318, 2016 WL 3792833 (D. Del. July 12, 2016) (sanctions imposed for senior executive's bad-faith destruction of evidence); GN Netcom v. Plantronics, Inc., No. 12-1318, 2017 WL 4417810 (D. Del. Oct. 5, 2017) (pre-trial order with "stipulated facts" and permissive adverse inference instruction); GN Netcom v. Plantronics, Inc., No. 12-1318, 2018 WL 273649 (D. Del. Jan. 3, 2018) (court refuses to grant new trial after jury found for defendant despite permissive adverse inference).

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

38. *Id. See also, e.g.*, Eshelman v. Puma Biotech., 2017 WL 2483800 (E.D.N.C. June 7, 2017); Fiteq Inc. v. Venture Corp., No. 13-cv-01946, 2016 WL 1701794, at *3 (N.D. Cal. Apr. 28, 2016) (refusing to award sanctions under Rule 37(e) when plaintiff failed to offer "persuasive evidence to show that the ESI was not 'restored or replaced through additional discovery'").

39. FED. R. CIV. P. 37(e)(2).

40. *See* Byrnie v. Town of Cromwell Bd. of Educ., 243 F.3d 93, 108–09 (2d Cir. 2001) ("Several courts have held that destruction of evidence in violation of a regulation that requires its retention can give rise to an inference of spoliation."). However, some record retention regulations that create preservation obligations are not necessarily enforceable for the benefit of private parties. *See* Zubulake v. UBS Warburg LLC, 217 F.R.D. 309, 322 n.70 (S.D.N.Y. 2003) (plaintiff was not an intended beneficiary of 17 C.F.R. § 240.17a-4, the U.S. Securities and Exchange Commission rule mandating retention of communications by members, brokers, or dealers); EEOC v. Jetstream Ground

federal and state level may also be invoked in specific cases within the coverage of those laws.[41] An order entered in another case or a party's own information-retention protocols may also give rise to preservation obligations.[42] However, "court[s] should be sensitive . . . to the fact that such independent preservation requirements may be addressed to a wide variety of concerns unrelated to the current litigation. The fact that a party had an independent obligation to preserve information does not necessarily mean that it had such a duty with respect to the litigation, and the fact that the party failed to observe some other preservation obligation does not itself prove that its efforts to preserve were not reasonable with respect to a particular case."[43]

Servs., Inc., 878 F.3d 960 (10th Cir. 2017) (In a Title VII action, the defendant disposed of relevant employment records contrary to a federal regulation, but the destruction did not require the imposition of an adverse inference jury instruction or other severe sanction, as no intent to deprive was found, and substitute testimonial evidence obviated prejudice.).

41. *See, e.g.,* 18 U.S.C. § 1519 (Sarbanes-Oxley Act § 802).

42. FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment. *See, e.g.*, Williams v. Kohl's Dep't. Stores, Inc., No. 3:12-cv-01385, 2014 U.S. Dist. LEXIS 78084, at *29 (D. Or. Mar. 31, 2014) (holding that, while "a company's internal policy, by itself, does not create a legal duty to preserve evidence . . . a *company's* internal policy may reflect that a certain type of incident is likely to give rise to litigation"); Coale v. Metro-N. R.R. Co., No. 3:08-cv-01307, 2016 WL 1441790, at *2 (D. Conn. Apr. 11, 2016) ("[N]o rule dictates that an entity's self-imposed obligation to preserve evidence for internal purposes creates an automatic obligation to preserve that *evidence* for purposes of litigation. Nevertheless, in this case . . . , the Court has little difficulty in holding that the [defendant's Incident Investigation and Reporting] Manual's discrete requirements may be construed as obligations to preserve evidence for purposes of litigation.").

43. FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment.

G. Non-Party Subpoenas

Prior sections addressed a *party's* duty to preserve discoverable information when a lawsuit or government investigation is reasonably anticipated. In a lawsuit, a non-party may receive a subpoena commanding the production of documents, information, or tangible things. The subpoenaed non-party then must decide whether the receipt of such a subpoena triggers a duty to preserve and, if not, what obligation for the non-party is triggered by receipt of the subpoena.

A non-party receiving a subpoena may not have a copy of the operative pleadings in the matter and may know little or nothing about the dispute. In that situation, the non-party would be unlikely to understand the scope of discovery (including relevance and proportionality) without some discussion with party counsel.[44]

44. In rare circumstances, the subpoena recipient may have knowledge of the principal dispute and may have a reasonable expectation of being made a party to the lawsuit. In those circumstances, a duty to preserve discoverable information arises (employing the same standards discussed in Guidelines 1–4, *infra*). *Cf*. *In re* Napster, Inc. Copyright Litig., 462 F. Supp. 2d 1060, 1068–69 (N.D. Cal. 2006). The *Napster* court found no circumstances existed at the time a venture capital firm received a non-party subpoena to create a reasonable expectation that *the specific venture capital firm* would be named as a party in any pending or future litigation. *Id*. at 1068. Instead, the court held that the venture capital firm's duty to preserve relevant ESI attached *one month after service of the subpoena* when, in the court's view, there was a "clear indication . . . that the recording industry would be targeting [downloading service's] investors" and the venture capital firm "should have reasonably believed that litigation against it was probable." *Id*. at 1069. A complaint against the venture capital firm was not filed until almost three years later—April 2003. *Id*. at 1065.

Rule 45, which governs subpoenas issued in federal court matters, says nothing about preservation.[45] However, the Rule does require that the party issuing the subpoena[46] (and the court on any ensuing motion[47]) takes steps to avoid imposing undue burden or expense on the subpoenaed person, and that the subpoenaed person respond in one of three ways—produce the requested information, object to the subpoena, or move to quash.

This does not mean that the non-party can destroy or discard information responsive to the subpoena, because the non-party may be subject to contempt sanctions if it "fails without adequate excuse to obey the subpoena or order related to it."[48] The receipt of a subpoena, however, usually does not trigger implementation of a preservation protocol as described elsewhere in this Commentary.

If the non-party serves a timely objection, performance is suspended and "acts may be required only as directed" in a court order. In the event of a motion to quash or a motion to compel over objections, the court may find the subpoena facially overbroad and inconsistent with the issuing attorney's obligation to protect the non-party from undue burden or expense. In other cases, a court may conclude that the requests exceed the relevant and proportional discovery scope for the matter. And, in some cases, a court may order the subpoena enforced as prepared and served on the non-party, in which case the non-party must produce the information responsive to the subpoena as served.

---

45. Rule 45 was last amended as relevant to this discussion in 2006, in connection with the original ESI amendment package. Preservation was not mentioned in the main discovery rules until the 2015 amendments.

46. *See* FED. R. CIV. P. 45(d)(1), and advisory committee's note to 1991 amendment.

47. *See* FED. R. CIV. P. 45(d)(2)(B)(ii) and (3)(B) and (C).

48. *See* FED. R. CIV. P. 45(g).

Once a responsive production is provided (either in the absence of timely objection or motion, or after court order), there is no ongoing duty for the non-party to retain documents and ESI.[49] The non-party may wish to inform the subpoenaing party that it considers its duty to respond to the subpoena to have been fulfilled, and that going forward it intends to manage the subpoenaed information consistent with its internal policies and procedures. If the non-party gave such notice, it would then be incumbent upon the subpoenaing party to inform the non-party of any desire for prolonged retention beyond the timeframe disclosed by the non-party (for example, to retain originals of specific information for potential trial use), and the subpoenaing party may have to shoulder the costs associated with the desire for prolonged retention.[50]

---

49. *See* FED. R. CIV. P. 45(d), (e), & (g). *See also* The Sedona Conference, *Commentary on Non-Party Production & Rule 45 Subpoenas*, at 7–8, THE SEDONA CONFERENCE (Apr. 2008), https://thesedonaconference.org/publication/Commentary_on_Non-Party_Production_and_Rule_45_Subpoenas ("The duration of a non-party's duty to ***preserve*** is not coextensive with a party's duty to preserve. In the ordinary course, a non-party subpoena recipient's duties should terminate once the non-party has produced, in conformity with their discovery obligations, either: (i) all information responsive to the subpoena; (ii) all information responsive to the subpoena except information excluded pursuant to timely objections by the producing party pursuant to Rule 45(c)(2)(B); or (iii) information responsive to the subpoena and satisfying any agreement with the party issuing the subpoena (i.e., after the issuance of the subpoena, the recipient and the issuer may negotiate and agree to a narrower scope of production that will satisfy the party.)") (emphasis added).

50. In some cases in which the commencement of discovery is delayed, generally due to a statutory stay, or lengthy pre-discovery motion practice, such as securities actions subject to the Private Securities Litigation Reform Act of 1995 (PSLRA), courts have issued orders, based upon specific evidentiary showings, permitting the issuance of so-called preservation subpoenas to a non-party requiring preservation of relevant documents or ESI. *See, e.g.*, *In re* Smith Barney Transfer Agent Litig., No. 05 Civ. 7583(WHP), 2012 WL 1438241, at *3 (S.D.N.Y. Apr. 25, 2012). Such court orders, however,

In some cases, a non-party to litigation may have a special, affiliated, or contractual relationship with a party, obligating the non-party to provide information to that party upon reasonable notice and request. The party may be deemed to have actual or constructive control of discoverable information in the possession of the non-party, and may have an obligation to notify the non-party to preserve information. Regardless of whether notice is provided, such non-parties need to consider these relationships and their related obligations when deciding whether a duty to preserve discoverable information is triggered.

In sum, where there is no "special relationship" with a party and there are no grounds to reasonably anticipate becoming a party to the action, the non-party receiving a subpoena has an affirmative obligation to (i) not destroy knowingly responsive documents and ESI; and (ii) after negotiation of the scope of the subpoena or resolution of objections, undertake reasonable collection of responsive documents and ESI. If expeditious collection is not possible, the non-party may choose to issue an appropriately tailored legal hold until its production obligations to the subpoena have been fulfilled (at which time the hold may be terminated). The non-party receiving the subpoena has *no obligation to* (i) suspend ordinary information management policies and procedures; (ii) issue legal hold notices; and (iii) absent extraordinary circumstances, preserve documents and ESI after collection and production.[51]

---

presumably include Rule 45 protections against undue burden and expense by requiring the subpoenas to avoid overbroad requests and to properly tailor preservation to the scope of discovery required by the circumstances, including relevance and proportionality.

51. The non-party may wish to keep the relevant and responsive materials at least through production and, ideally, until receiving confirmation that the original documents will not be needed for trial.

II. THE GUIDELINES

The Sedona Conference offers the following guidelines to help a party meet its duty to preserve discoverable information and to provide pragmatic suggestions and a framework for creating a set of preservation procedures.[52] *The guidelines are not intended to be, and should not be, used as an all-encompassing "checklist" or set of rules to be followed mechanically.* Instead, they should guide organizations in articulating policies to implement legal holds tailored to their needs.

The guidelines are illuminated by illustrations of hypothetical situations. These illustrations are intended to impart an understanding of the applicable analytical framework. If other factors were added to the illustrations, a different analysis and result might be required. In short, the illustrations should not be considered the sole basis for reaching a particular result, as all factors in any particular circumstance must be considered.

Guideline 1: A reasonable anticipation of litigation arises when an organization is on notice of a credible probability that it will become involved in litigation, seriously contemplates initiating litigation, or when it takes specific actions to commence litigation.

Guideline 2: Adopting and consistently following a policy governing an organization's preservation

52. James S. Kurz & Daniel D. Mauler, *A Real Safe Harbor: The Long-Awaited Proposed FRCP Rule 37(e), Its Workings, And Its Guidance For ESI Preservation*, 62 FED. L. 62, 65–66 (Aug. 2015) (suggesting that this *Commentary* provides guidelines for "designing processes that provide an ESI preservation solution that should meet the . . . Rule 37(e) 'reasonable steps' standard").

obligations are factors that may demonstrate reasonableness and good faith.

Guideline 3: Adopting a procedure for reporting information relating to possible litigation to a responsible decision maker may assist in demonstrating reasonableness and good faith.

Guideline 4: Determining whether litigation is or should be reasonably anticipated should be based on a good-faith and reasonable evaluation of relevant facts and circumstances.

Guideline 5: Evaluating an organization's preservation decisions should be based on the good faith and reasonableness of the decisions (including whether a legal hold is necessary and how it should be implemented) at the time they are made.

Guideline 6: Fulfilling the duty to preserve involves reasonable and good-faith efforts, taken as soon as is practicable and applied proportionately, to identify persons likely to have information relevant to the claims and defenses in the matter and, as necessary, notify them of their obligation to preserve that information.

Guideline 7: Factors that may be considered in determining the scope of information that should be preserved include the nature of the issues raised in the matter, the accessibility of the information, the probative value of the

information, and the relative burdens and costs of the preservation effort.

Guideline 8: In circumstances where issuing a legal hold notice is appropriate, such a notice is most effective when the organization identifies the custodians and data stewards most likely to have discoverable information, and when the notice:

(a) communicates in a manner that assists persons in taking actions that are, in good faith, intended to be effective;
(b) is in an appropriate form, which may be written, and may be sent by email;
(c) provides information on how preservation is to be undertaken, and identifies individuals who can answer questions about preservation;
(d) includes a mechanism for the recipient to acknowledge that the notice has been received, read, and understood;
(e) addresses features of discoverable information systems that may make preservation of discoverable information more complex (e.g., auto-delete functionality that should be suspended, or small sections of elaborate accounting or operational databases);
(f) is periodically reviewed and amended when necessary; and

(g) is followed up by periodic reminder notices, so the legal hold stays fresh in the minds of the recipients.[53]

Guideline 9: An organization should consider documenting the procedure of implementing the legal hold in a specific case when appropriate.

Guideline 10: Compliance with a legal hold should be regularly monitored.

Guideline 11: Any legal hold process should include provisions for releasing the hold upon the termination of the duty to preserve, so that the organization can resume adherence to policies for managing information through its useful life cycle in the absence of a legal hold.

Guideline 12: An organization should be mindful of local data protection laws and regulations when initiating a legal hold and planning a legal hold policy outside of the United States.

53. *See The Sedona Principles, Third Edition, supra* note 1, Cmt. 5.d., at 103–04.

III. COMMENTARY

Guideline 1: A reasonable anticipation of litigation arises when an organization is on notice of a credible probability that it will become involved in litigation, seriously contemplates initiating litigation, or when it takes specific actions to commence litigation.

In many instances, there is no ambiguity about when the duty to preserve arises. For example, the receipt of a summons or complaint or the receipt of a formal notice that an organization is the target of a government investigation puts an organization on notice that it has a duty to preserve information. However, other events may trigger a duty to preserve only when considered in the context of an organization's history and experience or the facts of the case.

For instance, an insurer's receipt of a claim from an insured often will not indicate the probability of litigation, as the insurer is in the business of paying claims often without litigation. On the other hand, the occurrence of an accident[54] or the receipt of

54. *Compare, e.g.*, Browder v. City of Albuquerque, 187 F. Supp. 3d. 1288, 1296 n.3 (D.N.M. 2016) ("The Court would find that litigation was 'reasonably foreseeable' the moment the City became aware that a police officer was involved in a fatal traffic accident.") *and* Williams v. Kohl's Dep't. Stores, Inc., No. 3:12-cv-01385, 2014 U.S. Dist. LEXIS 78084, at *29–30 (D. Or. Mar. 31, 2014) ("Courts have routinely found that a defendant is on notice of possible litigation simply by virtue of the fact that an accident occurred on the premises.") *with* McCabe v. Wal-Mart Stores, Inc., No. 2:14-cv-01987, 2016 WL 706191, at *2 (D. Nev. Feb. 22, 2016) ("While all slip-and-fall incidents may not result in litigation, the incident report made at the scene by [plaintiff] is sufficient to trigger Wal-Mart's duty to preserve relevant evidence.") *and* Harrell v. Pathmark, No. 14-5260, 2015 WL 803076, at *4 (E.D. Pa. Feb. 26, 2015) ("Even in a highly litigious community or culture, just because a person falls in a grocery store does not mean that litigation is imminent. . . . While the incident itself did cause [defendant's employee] to create an incident

a preservation notice letter from an opposing party may give rise to a credible probability of litigation, depending on the circumstances. In most circumstances, service of a subpoena on an organization will not trigger a duty to preserve information unless, at the time the organization receives the subpoena, it reasonably anticipates that the organization will become a party to that litigation.

Plaintiff Claims: On the plaintiff's side, seeking advice of counsel, sending a cease-and-desist letter, or taking specific steps to commence litigation may trigger the duty to preserve. The activities of the plaintiffs prior to litigation came under close examination in *Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC*[55] and *Rimkus Consulting Grp., Inc. v. Cammarata*.[56] The test of when the duty to preserve is triggered is often based on when the plaintiff "determined [that] legal action was appropriate."[57] Thus, in *Best Payphones, Inc. v. City of N.Y.*, a plaintiff was held to be under a duty to preserve evidence once it decided to bring an action.[58]

Defense Claims: On the defendant's side, credible information that it is the target of legal action may be sufficient to trigger the duty to preserve. The degree to which litigation must be certain is debatable. In *Goodman v. Praxair Servs., Inc.*, the court refused to require an unequivocal notice of impending

---

report, nothing about it was so immediately dramatic to create an objectively foreseeable likelihood of litigation.").

55. 685 F. Supp. 2d 456, 475 (S.D.N.Y. 2010), *abrogated in part by* Chin v. Port Auth. of N.Y. & N.J., 685 F.3d 135 (2nd Cir. 2012).

56. 688 F. Supp. 2d 598, 611, 641 (S.D. Tex. 2010).

57. Milenkamp v. Davisco Foods Int'l, Inc., 562 F.3d 971, 981 (9th Cir. 2009) (no duty to preserve since destruction of evidence occurred "by the time" that plaintiffs determined legal action was appropriate).

58. Nos. 1-CV-3924, 1-CV-8506, 3-CV-0192, 2016 WL 792396, at *4 (E.D.N.Y. Feb. 26, 2016).

litigation.[59] In *Apple Inc. v. Samsung Elecs. Co., Ltd.*, a presentation among senior executives in which Apple informed Samsung that it believed Samsung was infringing its patents was held to trigger Samsung's duty to preserve.[60]

However, there are circumstances when the threat of litigation is not credible, and it would be unreasonable to anticipate litigation based on that threat. For example, in *Cache LaPoudre Feeds, LLC v. Land O'Lakes, Inc.*, a letter referencing potential "exposure" but also mentioning the possibility of amicable resolution was held not to trigger the obligation to preserve, since a mere possibility of litigation does not necessarily make it likely.[61]

This guideline provides that a duty to preserve is triggered *only* when an organization concludes (or should have concluded), based on credible facts and circumstances, that litigation or a government investigation is probable. Whether litigation can be reasonably anticipated should be based on a good-faith and reasonable evaluation of the facts and circumstances as they are known at the time.

---

59. 632 F. Supp. 2d 494, 510 n.7 (D. Md. 2009) ("[W]here, as here, [a] letter openly threatens litigation, then the recipient is on notice that litigation is reasonably foreseeable and the duty to preserve evidence relevant to that dispute is triggered.").

60. 881 F. Supp. 2d 1132, 1145 (N.D. Cal. 2012). In *Phillip M. Adams & Assocs., L.L.C. v. Dell, Inc.*, 621 F. Supp. 2d 1173 (D. Utah 2009), the duty to preserve was held to have been triggered many years before suit was filed because of mere awareness of similar litigation involving others in the industry.

61. 244 F.R.D. 614, 623 (D. Colo. 2007) ("[A] party's duty to preserve evidence in advance of litigation must be predicated on something more than an equivocal statement of discontent."); *see also* Hixson v. City of L.V., No. 2:12-cv-00871, 2013 WL 3677203, at *5 (D. Nev. July 11, 2013) ("It is not reasonably foreseeable [*sic]* that every internal employment complaint may result in litigation if not resolved to the employee's satisfaction.").

A reasoned analysis of the available facts and circumstances is necessary to conclude whether litigation or a government investigation is "reasonably anticipated." That determination is fact-specific and should be made by an experienced person who can make a reasoned judgment.

Of course, later information may require an organization to reevaluate its determination and may result in a conclusion that (a) litigation that previously had not been reasonably anticipated (and consequently did not trigger a preservation obligation) is then reasonably anticipated or (b) new information alters the scope of the preservation obligation for anticipated or pending litigation.[62] Conversely, new information may enable an organization to determine that it should no longer reasonably anticipate a particular litigation and is, consequently, no longer subject to a preservation obligation. A party that obtains new information, after the initial decision is made, should reevaluate the situation as soon as practicable. Parties and counsel should give careful consideration to documenting their analysis.[63]

---

62. *See, e.g.*, Marten Transp., Ltd. v. Plattform Adver., Inc., No. 14-cv-02464, 2016 WL 492743, at *10 (D. Kan. Feb. 8, 2016) (Although plaintiff's duty to preserve was triggered by correspondence between counsel in 2013, it did not include a key employee's internet browser history until 2015, when defendant first made allegations to which the history was potentially relevant.); *In re* Pradaxa (Dabigatran Etexilate) Prods. Liab. Litig., No. 3:12-md-02385, 2013 WL 6486921, at *1 (S.D. Ill. Dec. 9, 2013), *mandamus granted on other grounds, In re* Pet. of Boehringer Ingelheim Pharms. Inc.,745 F.3d 216 (7th Cir. 2014) ("[W]hile the defendants may have been able to justify adopting a narrow litigation hold as to *some* employees prior to June 2012, they cannot justify failing to adopt a company-wide litigation hold as of June 2012—when they knew nationwide Pradaxa product liability litigation was imminent.") (emphasis in original).

63. *See, e.g.*, Stevenson v. Union Pac. R.R. Co., 354 F.3d 739, 749–50 (8th Cir. 2004) (affirming the imposition of sanctions against defendant that selectively preserved evidence that was favorable to its litigation position and

To help understand when the duty to preserve arises, one should consider when the duty does *not* arise. For example, a vague rumor or indefinite threat of litigation does not trigger the duty; nor does a threat of litigation that is not credible or not made in good faith. A lack of credibility may arise from the nature of the threat itself, past experience regarding the type of threat, the person who made the threat, the legal basis upon which the threat is purportedly founded, or any similar facts.

Another issue to be considered is what constitutes notice to the organization. For corporations, this can be a complicated issue. If one employee or agent of the organization learns of facts that might lead one to reasonably believe litigation will be forthcoming, should that knowledge be imputed to the organization as a whole, thereby triggering its preservation obligations? Often, the answer will depend on the nature of the knowledge, the potential litigation,[64] and the agent. Generally, an organization is considered to "'know' what its employees know—at least, what employees know on subjects within the scope of their duties."[65]

Organizations that become aware of a credible threat from which litigation could arise may have a duty to make a reasonable inquiry or undertake a more detailed investigation regarding the facts related to the "threat." Whether an inquiry or

failed to preserve an audio recording that was likely material to plaintiff's claims).

64. Attorneys and organizations should be cognizant of the possibility of arguments that the labeling of information as attorney work product (either at the time of creation or in later logs) is tantamount to admitting a preservation obligation existed at the time the information was created because both doctrines depend on a reasonable anticipation of litigation.

65. NECA-IBEW Rockford Local Union 364 Health & Welfare Fund v. A&A Drug Co., 736 F.3d 1054, 1059 (7th Cir. 2013). Some courts require that the knowledge be "material" to the employee's duties. *See, e.g.*, Huston v. Proctor & Gamble Paper Prods. Corp., 568 F.3d 100, 107 (3d Cir. 2009).

detailed investigation is warranted will be fact-driven and based on reasonableness and good faith. Thus, while there may be no duty to affirmatively disprove allegations associated with a threat before concluding that it lacks credibility, the facts and circumstances may suggest the prudence of making an inquiry before reaching such a conclusion.[66]

ILLUSTRATIONS

Illustration i: An organization receives a letter that contains a vague threat of a trade secret misappropriation claim. The letter does not specifically identify the trade secret. Based on readily available information, it appears that the information claimed to be the misappropriated trade secret had been publicly known for many years. Furthermore, the person making the threat had made previous threats without initiating litigation. Given these facts, the recipient of the threat could reasonably conclude that there was no credible threat of litigation, and the organization had no duty to initiate preservation efforts.

Illustration ii: An organization receives a demand letter from an attorney on behalf of a client that contains a specific threat of a trade secret misappropriation claim. Furthermore, the organization is aware that others have been sued by the attorney's client on similar claims. Given these facts, there is a credible threat of litigation, and the organization has a duty to preserve discoverable information. The client's duty to preserve arises no later than the date of the decision to send the letter, and, in some circumstances, may arise earlier.

66. *See* Stallings v. Bil-Jax, Inc., 243 F.R.D. 248, 252 (E.D. Va. 2007) (Although plaintiff's letter was vague, it provided "some notice" of possible litigation and defendant "had ample time to make a timely request for additional information regarding the nature of the incident referred to in the letter.").

Illustration iii: An organization learns of a report in a reputable news source that includes sufficient facts, consistent with information known to the organization, concerning the possibility of an impending government investigation of the organization for a possible violation of law. Under these circumstances, a government investigation (and possibly litigation) can reasonably be anticipated, and a preservation obligation has arisen.

Illustration iv: An event occurs that, in the experience of the organization, typically results in litigation. Examples of such events may include a plant explosion with severe injuries, an airplane crash, or an employment discrimination claim. The experience of the organization when these events or claims arose in the past would be sufficient to give rise to a reasonable anticipation of litigation.

Illustration v: A cease-and-desist letter for misuse of a trademark is received by a business. The recipient replies with an agreement to comply with the demand and, in fact, does comply. The recipient does not have a reasonable basis to anticipate litigation and does not have an obligation to preserve discoverable information. However, the duty to preserve on the part of the sender arises no later than the date of the decision to send the letter.

Guideline 2: Adopting and consistently following a policy governing an organization's preservation obligations are factors that may demonstrate reasonableness and good faith.

A policy[67] setting forth a procedure[68] for determining whether the duty to preserve information has arisen can help ensure that the decision is made in a defensible manner. As stated in *The Sedona Principles*, *Third Edition*, such a policy can be part of a larger information governance ("IG") program, although "an organization's compliance with discovery obligations cannot be judged by the state or lack of its IG program."[69] Any policies that provide for management of an organization's information should include provisions for implementing procedures to preserve discoverable information in ongoing or reasonably anticipated litigation, or relevant for government investigations or audits.[70] The nomenclature used (e.g., "legal hold" or "information governance") is not important; what is important is that the organization have explicit and consistent policies and procedures to guide compliance with its preservation obligations.[71]

Organizations will have different policies depending on their size, business needs, culture, and other structural factors.

---

67. Policy refers to the general statement of a course of action which may be operational, aspirational, or a combination of both. Operational in this context means that the course of action can be executed without further articulation.

68. Procedure refers to a plan of action to implement a policy. Although a policy statement may incorporate procedures, procedures should not be used as a synonym for policy. *See also* the definition of Process, *infra* note 72.

69. *See The Sedona Principles, Third Edition, supra* note 1, Cmt. 1.b., at 59–64; *see also id*., Cmt. 5.b., at 99.

70. *Id*.

71. *See id*. at 100.

The key is to have a process[72] that is followed.[73] In cases where the preservation efforts are likely to be challenged, it can be helpful to memorialize the steps taken to follow that process, so the organization can demonstrate its compliance with the process. A defined policy and evidence of compliance should provide strong support if the organization is called upon to demonstrate the reasonableness of its decision-making process.

ILLUSTRATIONS

Illustration i: Upon receipt of an anonymous threat of litigation sent to a corporation's ombudsman, the ombudsman consults the legal hold policy. The policy provides criteria for an assessment of the threat and whether the issues raised by it, including the circumstances surrounding its receipt, indicate the potential for litigation or government investigation. It also provides for a preliminary evaluation of the allegations before determining whether a legal hold should be implemented. Based on the policy, the ombudsman concludes that the corporation does not reasonably anticipate litigation and memorializes that decision in a memorandum to the file. In a subsequent challenge, the corporation can demonstrate that it considered its legal hold policy and the likelihood of litigation occurring, and it exercised reasonable and good-faith judgment in determining that litigation was not reasonably anticipated.

Illustration ii: A citizen complaint is forwarded to the city attorney for a medium-sized municipality. Following her standard practice (which has been consistently followed and was developed and memorialized in consultation with city officials),

72. Process refers to the articulation of the steps employed to implement a procedure.

73. *See The Sedona Principles, Third Edition, supra* note 1, Cmt. 5.b., at 100, and Cmt. 1.b., at 62 n.31 ("[O]rganizations must not only communicate what the IG policy is, but why it is important to follow the policy.").

the city attorney considers the type of complaint, seriousness of the alleged behavior, and history of past similar complaints, among other factors. After determining that the city does not reasonably anticipate litigation based on the complaint, she memorializes that decision in an email to the city agency that initially forwarded the complaint. In a subsequent challenge, the city can use the existence of its consistent process (and the existence of the email, although its content may be privileged) to demonstrate the reasonableness and good faith of the city's decision regarding preservation.

Guideline 3: Adopting a procedure for reporting information relating to possible litigation to a responsible decision maker may assist in demonstrating reasonableness and good faith.

In any organization—but particularly large organizations—individuals within the organization may have information indicating a threat of litigation that the organization's decision makers do not have. An organization should consider how to communicate that information to persons charged with evaluating the threat and, if warranted, instituting legal holds. The particulars of such a procedure will vary from organization to organization, based on the nature of the business, the way the business is conducted, and the culture of the organization.

One important consideration is the threshold for reporting. A procedure for reporting information should discourage spurious or trivial reports, while still encouraging the candid flow of information to appropriate decision makers. The reporting threshold, like other particulars of the procedure, will vary among organizations. Generally, the threshold for reporting should be lower than the threshold for determining whether a legal hold is warranted. Legal hold determinations require an understanding and application of the law; a reporting threshold need not.

To be effective, any such procedure should be simple and practical, and individuals within the organization should be trained on how to follow the procedure. The organization should periodically evaluate the effectiveness of its procedure, including the frequency with which it is used, and the quality of the information being received.

ILLUSTRATIONS

Illustration i: Westerberg Products (Westerberg) is a large corporation with tens of thousands of employees and offices throughout the United States. Westerberg establishes an internal compliance website through which employees can submit information regarding matters they believe may become subjects of litigation. The information received via the website is forwarded to the legal department, which is charged with determining whether and when to implement a legal hold. All Westerberg employees are trained on how to use the website and are periodically reminded that they should use it to report any concerns. A member of the legal department is assigned to make an annual evaluation of the effectiveness of the procedure. Westerberg can use these procedures to demonstrate its good-faith efforts to ensure it is aware of information that may lead it to conclude there is a reasonable anticipation of litigation.

Illustration ii: Stinson Software (Stinson) is a small software developer with eight employees. Every month, all eight employees attend a staff meeting, and a regular topic of discussion is whether any employee is aware of any ongoing threats to the company, including possible claims or demands that might result in litigation by or against the company. Stinson's Chief Operations Officer follows up on any tips with Stinson's outside counsel. Stinson can use this procedure to demonstrate its good-faith effort to ensure it is aware of information that may lead it to conclude there is a reasonable anticipation of litigation.

Guideline 4: Determining whether litigation is or should be reasonably anticipated should be based on a good-faith and reasonable evaluation of relevant facts and circumstances.

Determining whether litigation is or should be reasonably anticipated—either on behalf of or against an organization—requires consideration of many factors. Depending on the nature of the organization, factors that may be pertinent include the following:

- The nature and specificity of the notice of potential claim or threat
- The person or entity making the claim
- The business relationship between the accused and accusing parties
- Whether the threat is direct, implied, or inferred
- Whether the party or counsel making the claim is known to be aggressive or litigious
- Whether a party who could assert a claim is aware of the claim
- The strength, scope, or value of a known, reasonably anticipated, or threatened claim
- Whether the organization has knowledge or information about similar claims
- The relevant experience in the industry with regard to such claims
- Reputable press or industry coverage of the issue, either directly pertaining to the organization or regarding complaints against others similarly situated
- Whether a party has retained counsel or is seeking advice of counsel in connection with defending against or filing a claim

- Whether an organization that is considering bringing a claim has begun to mark documents to indicate that they fall under the work-product doctrine
- Whether a potential claimant has sent or received a demand, cease-and-desist, or complaint letter

These factors are not exhaustive, and no single factor is necessarily determinative of what response is reasonable. All factors must be evaluated reasonably and in good faith.

ILLUSTRATIONS

Illustration i: A musician writes a song that sounds very similar to a famous song. Immediately, there are critical reviews and radio disc jockeys calling the song a "blatant rip-off." Although the copyright owners of the original song have not yet made any claim, the high-profile nature of the criticism is a consideration that may lead the musician's publisher to determine that a preservation obligation has arisen.

Illustration ii: A restaurant chain's central management office receives a series of anonymous emails purported to be from customers claiming food poisoning after the much-publicized introduction of a new dish. In the absence of any corroborating reports from the restaurants and with no specific details on which to act, the chain's counsel may reasonably conclude that litigation is not reasonably anticipated.

Guideline 5: Evaluating an organization's preservation decisions should be based on the good faith and reasonableness of the decisions (including whether a legal hold is necessary and how it should be implemented) at the time they were made.

The reasonableness of an organization's preservation decisions, such as whether to implement a legal hold and the scope of such a hold, should be made in light of the facts and circumstances reasonably known to it at the time of its decisions, and should not be evaluated on the basis of hindsight or information acquired after the decisions are made.[74] An organization seeking to determine whether a preservation obligation has arisen and the scope of any such obligation has no choice but to rely on the information available to it. Consequently, whether reasonable decisions were made should turn on what the organization knew or reasonably should have known at that time, and not on other circumstances of which the organization was unaware.[75]

---

74. Any subsequent judicial evaluation of an organization's legal hold implementation should be based on the good faith and reasonableness of the implementation at the time the hold was implemented. In doing so, proportionality considerations are relevant. FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment (One "factor in evaluating the reasonableness of preservation efforts is proportionality.").

75. *See* FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment (In deciding whether and when a duty to preserve arose in advance of litigation, "it is important not to be blinded . . . by hindsight arising from familiarity with an action as it is actually filed."); *see also* Marten Transp., Ltd. v. Plattform Adver., Inc., No. 14-cv-02464, 2016 WL 492743, at *10 (D. Kan. Feb. 8, 2016) (denying sanctions under Rule 37(e) because the party took reasonable steps to preserve relevant information; the party "had no knowledge or information from which it should have known that [the lost ESI] would become relevant in the case" before the ESI was lost); *In re* Delta/AirTran Baggage Fee Antitrust Litig., No. 1:09-md-2089, 2015 WL 4635729, at *10 (N.D. Ga. Aug. 3, 2015) ("The fact that, with perspective adjusted by hindsight and

ILLUSTRATIONS

Illustration i: The One, Inc. offers an online dating service that uses state-of-the-art software it licenses from Tech Savvy to "match" its couples. Tech Savvy also licenses its software to SO Finder, which runs its own online dating service. In January, SO Finder receives reports that many of its members are being matched to people whose characteristics align with their "dislike" and "can't stand" lists instead of with their "love" or "like" lists. After investigating, SO Finder determines that the mismatching is caused by a flaw in the software it licenses from Tech Savvy. The news of SO Finder's mismatching is kept out of the media, and the class action case brought by SO Finder's members is settled out of court by March. In April, The One, Inc., which had no knowledge of the suit against SO Finder or the subsequent settlements, disposes of certain information relating to its use of Tech Savvy's software, pursuant to its information management and data destruction policies. In May, The One, Inc. begins receiving complaints from its members about mismatching and is sued by its members a month later. Because The One, Inc. had no knowledge or reason to know of the problems with the software it licenses from Tech Savvy, its decision to dispose of information in April was not in violation of a duty to preserve.

Illustration ii: In January, Polly Pliff sues Farma Firm alleging that its product, Xpill, caused Pliff to develop a side effect about which Farma Firm failed to properly warn consumers. Xpill has been on the market for more than 10 years. Pliff's case is the first relating to Xpill brought against Farma Firm, and Farma Firm has no reason to believe there will be other such

---

over a year of discovery, it might have been helpful for Delta to preserve the data sources now at issue is insufficient to support a motion for sanctions if it is not shown that the duty to preserve reached this evidence to begin with.") (internal quotation omitted).

cases. Farma Firm acts promptly to issue a legal hold to key custodians, including Ron Rep, the sales representative who detailed Xpill to Pliff's prescribing doctor. Pursuant to Farma Firm's information governance policy, at the end of its fiscal year in March, Farma Firm destroys its sales representative detail call records that are more than five years old. Because of the legal hold issued to Ron Rep, records of his Xpill detail calls are retained, but records of Xpill detail calls by all other Farma Firm sales representatives are destroyed. In July, several new cases alleging claims similar to Pliff's are filed against Farma Firm by patients who received their Xpill prescriptions from doctors who had been detailed by other Farma Firm sales representatives. Because Farma Firm had no knowledge or reason to know of the relevance of detail call records for sales representatives other than Ron Rep when it destroyed such records in March, its decision to do so was reasonable and not in violation of a duty to preserve.

Guideline 6: Fulfilling the duty to preserve involves reasonable and good-faith efforts, taken as soon as is practicable and applied proportionately, to identify persons likely to have information relevant to the claims and defenses in the matter and, as necessary, notify them of their obligation to preserve that information.

After an organization determines it has a duty to preserve, it should begin to identify information to be preserved. The obligation to preserve requires reasonable and good-faith efforts.[76]

76. FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment ("A variety of events may alert a party to the prospect of litigation. Often these events provide only limited information about that prospective litigation, however, so that the scope of information that should be preserved may

But it is "unreasonable to expect parties to take every conceivable step or disproportionate steps to preserve all potentially relevant data."[77] The organization should consider the sources of information within its "possession, custody, or control"[78] that would likely include discoverable information. The most obvious of these sources are those that the organization has physically in its possession or custody—for example, file cabinets of documents in its office, and emails or office files on its servers (wherever located)—but also may include sources such as thumb drives, company-furnished laptops, and mobile devices used by employees for business purposes.[79]

Some sources of information within the possession or custody of third parties may also be deemed to be within the control of the organization because of contractual or other

---

remain uncertain. It is important not to be blinded to this reality by hindsight arising from familiarity with an action as it is actually filed.").

77. *The Sedona Principles, Third Edition, supra* note 1, Principle 5, at 93. *See also* Cmt. 5.e., at 108 ("Preservation efforts need not be heroic or unduly burdensome.").

78. *See* FED. R. CIV. P. 34 and its state equivalents; *see also, e.g.*, Lindholm v. BMW of N. Am., LLC, No. 3:15-CV-03003, 2016 WL 452315, at *3–4 (D.S.D. Feb. 5, 2016) (Plaintiffs were not entitled to discovery of information that was in the possession of defendant's non-party indirect subsidiary when the non-party was a separate legal entity and had no agency relationship with defendant.); *In re* NTL, Inc., Secs. Litig., 244 F.R.D. 179, 195 (S.D.N.Y. 2007) (Defendant was obliged to produce responsive records in the physical possession of a non-party when defendant had the legal right and practical ability to obtain the records.).

79. *See* Paisley Park Enters., Inc. v. Boxill, 330 F.R.D. 226 , 2019 WL 1036058 (D. Minn. Mar. 5, 2019) (holding that defendants violated their duty to preserve relevant information by failing to take affirmative steps to keep relevant text messages); NuVasive, Inc. v. Kormanis, 18-cv-0282, 2019 WL 1171486 (M.D.N.C. Mar. 13, 2019), *report and recommendation adopted*, 2019 WL 1418145 (M.D.N.C. Mar. 29, 2019) (finding that defendant should have disabled the automated destruction feature on his mobile phone to properly preserve relevant text messages).

relationships. Examples include information held by outsourced service providers, storage facility operators, and providers of software as a service (SaaS).[80] With respect to those sources, the organization should consider providing appropriate notice concerning the need to preserve material likely to be discoverable.

It must be noted that a mere delay in implementing a legal hold is not necessarily fatal. In *Rahman v. The Smith & Wollensky Restaurant Grp., Inc.*, the court concluded that "even assuming there was, in fact, no litigation hold" until late in the litigation, the plaintiff had failed to establish that there was "any gap" in production "attributable to the failure to institute [a] litigation hold at an earlier date."[81] The test is what was reasonable under the circumstances, with the goal of preserving discoverable information. Thus, there is no per se negligence rule, and if the organization otherwise preserved the information, there is no violation of the duty to preserve.[82]

---

80. Notably, the advent of "cloud computing" has increased substantially the number of organizations using third parties to host, manage, store, and dispose of electronic information in the course of business. *See generally* The Sedona Conference, *Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control,"* 17 SEDONA CONF. J. 467 (2016).

81. No. 06 Civ. 6198, 2009 WL 773344, at *6 (S.D.N.Y. Mar. 18, 2009) (emphasizing that the proof is directed at the failure to produce or destruction of relevant evidence, not, per se, the institution of a legal hold).

82. FED. R. CIV. P. 37(e); Matthew Enter., Inc. v. Chrysler Grp. LLC, No. 13-cv-04236-BLF, 2016 WL 2957133, at *1 (N.D. Cal. May 23, 2016) ("Rule 37(e) now provides a genuine safe harbor for those parties that take 'reasonable steps' to preserve their electronically stored information."); Chin v. Port Auth. of N.Y. & N.J., 685 F.3d 135, 162 (2nd Cir. 2012) ("We reject the notion that a failure to institute a 'litigation hold' constitutes gross negligence *per se*. . . . Rather, we agree that 'the better approach is to consider [the failure to adopt good preservation practices] as one factor' in the determination of whether discovery sanctions should issue.") (internal citations omitted).

ILLUSTRATION

Illustration i: Strummer Holdings (Strummer) is a large corporation that sends many of its historic documents to an offsite storage facility managed by Jones Storage. Typically, documents older than five years are sent to Jones Storage. At all times, Strummer retains all legal rights with respect to the documents and has the right to require their return from Jones Storage at any time. Jones Storage has standing instructions from Strummer to automatically destroy certain documents when they are 10 years old.

Strummer reasonably anticipates litigation relating to events that occurred nine years ago. As a result, its preservation obligations are triggered with respect to documents stored at Jones Storage that Strummer believes may include unique information. If Strummer does not take steps to ensure that the discoverable documents (if any) it has stored at Jones Storage are preserved, it may be subject to curative measures or sanctions under the court's inherent authority with respect to hard-copy documents. If ESI was destroyed and cannot be replaced, Strummer may be subject to curative measures or sanctions under Federal Rule of Civil Procedure 37(e).[83]

83. *See supra* notes 12–19 and accompanying text for a discussion of this Rule.

Guideline 7: Factors that may be considered in determining the scope of information that should be preserved include the nature of the issues raised in the matter, the accessibility of the information, the probative value of the information, and the relative burdens and costs of the preservation effort.

Determining the scope of preservation obligations typically involves an initial focus on information available in accessible or "active" sources.[84] "Only when electronically stored information is not available through such primary sources should parties move down a continuum of less accessible sources until the information requested to be preserved or produced is no longer proportional."[85] As noted earlier, there is no requirement to preserve *all* information.[86]

The Federal Rules and *The Sedona Principles, Third Edition* recognize the value of conferring with opposing parties about the preservation and production of ESI.[87] Rule 26(f) provides parties with the opportunity at the discovery planning stage to discuss and agree on a reasonable preservation scope. The Rules emphasize cooperative action,[88] as promoted by The Sedona

84. *See The Sedona Principles, Third Edition, supra* note 1, Principle 8, at 134.

85. *Id*.

86. Zubulake v. UBS Warburg, 220 F.R.D. 212, 217 (S.D.N.Y. 2003); *see also, e.g., In re* Ethicon, Inc. Pelvic Repair Sys. Prod. Liab. Litig., 299 F.R.D. 502, 517 (S.D.W. Va. 2014) (It is "uniformly agreed that a corporation under a duty to preserve is not required to keep 'every shred of paper, every e-mail or electronic document, and every backup tape' . . . [as] such a requirement 'would cripple large corporations.'") (quoting *Zubulake*, 220 F.R.D. at 217).

87. *See The Sedona Principles, Third Edition, supra* note 1, Principle 3, at 71.

88. FED. R. CIV. P. 1 advisory committee's note to 2015 amendment ("Effective advocacy is consistent with—and indeed depends upon—cooperative and proportional use of procedure."); *The Sedona Principles, Third Edition,*

Conference *Cooperation Proclamation*.[89] Parties are admonished to pay particular attention to the balance between the competing needs to preserve discoverable information and to continue routine business operations critical to ongoing activities.[90]

Unfortunately, it is not always feasible to secure prior agreement on preservation steps to be taken.[91] This is particularly true when preservation decisions must be made in the pre-litigation context, but it also can be a problem after commencement of litigation. In these circumstances, under the amended Federal Rules, the organization should base preservation decisions on its best judgment, made upon reasonable inquiry and in good faith, considering all the circumstances.[92] In some cases, this

---

supra note 1, Cmt. 3.b. at 76; *see also* Loop AI Labs Inc. v. Gatti, No. 15-CV-00798, 2016 WL 1273914, at *1 (N.D. Cal. Feb. 5, 2016) (noting that the parties' obligations under the discovery rules require cooperation and warning that "[o]bstructionist behavior will not be tolerated").

89. 10 SEDONA CONF. J. 331 (2009 Supplement) (calling for cooperative action by participants in relation to the discovery process).

90. FED. R. CIV. P. 26(f) advisory committee's note to 2006 amendment (parties' Rule 26(f) conference "discussion should pay particular attention to the balance between the competing needs to preserve relevant evidence and to continue routine operations critical to ongoing activities"); FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment ("[T]he prospect of litigation may call for reasonable steps to preserve information by intervening in that routine operation.").

91. For example, in rare cases, an organization may have questions about whether ephemeral data would be discoverable or could be preserved except by extraordinary measures not reasonably warranted. *See* Kenneth J. Withers, *"Ephemeral Data" and the Duty to Preserve Discoverable Electronically Stored Information*, 37 U. BALT. L. REV. 349, 377 (2008) ("By the time the parties sit down at the Rule 26(f) conference, the preservation issues surrounding ephemeral data may be moot and the fate of the responding party may already be sealed, if sanctions are later found to be warranted.").

92. *The Sedona Principles, Third Edition, supra* note 1, Cmt. 8.a., at 136. *The Sedona Principles, Third Edition* also notes that there are risks to making

may include the preservation of both historical and future data (if information created in the future is relevant to claims or defenses in the litigation).[93]

Key Factors to be Considered

There are numerous factors to be weighed when determining the scope of a particular hold.

Issues in Dispute: First, the scope of any legal preservation effort is bounded by the claims made or issues involved in the matter. There is no obligation to preserve data that falls outside those boundaries.[94]

Accessibility: A second factor is the accessibility of the information, especially when ESI is involved. Data that is not reasonably accessible may not need to be preserved.

"[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."[95] Consistent with the principle of proportionality embodied in the Federal Rules,[96] The Sedona Conference *Commentary on Preservation, Management and Identification of Sources of Information That Are Not Reasonably*

unilateral decisions, especially if an opportunity to confer has been avoided. *See id.*, Cmt. 5.a., at 96–97.

93. Courts have recognized that a duty to preserve applies to discoverable information that exists at the time the duty attaches, and that is created after the duty arises. *See, e.g.*, Zubulake v. UBS Warburg, 220 F.R.D. 212, 218 (S.D.N.Y. 2003).

94. *See* discussion and footnotes for Guideline 5, *supra* (preservation decisions based on good faith and reasonableness at the time they are made).

95. FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment.

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

Accessible[97] stated that in the absence of agreement, it may be "reasonable to decline to preserve" inaccessible sources if the party concludes that the "burdens and costs of preservation are disproportionate to the potential value of the source of data."[98]

For example, *Zubulake IV* concluded that "as a general rule," a "litigation hold does not apply to inaccessible backup tapes," which "may continue to be recycled."[99] *Zubulake IV* also established an exception: if the producing party "can identify where particular employee documents are stored on backup tapes, then the tapes storing the documents of 'key players' [i.e., custodians] to the existing or threatened litigation should be preserved if the information contained on those tapes is not

97. 10 SEDONA CONF. J. 281, 291 (2009). In determining accessibility, a combination of "media based factors" and "data complexity factors" should be used. *Id*. at 289.

98. *Id.* (proposing a "decision tree" form of analysis under which the burdens and costs of accessing and preserving are balanced against the "reasonably anticipated need and significance of the information"). *See also The Sedona Principles, Third Edition*, *supra* note 1 at 95–96; The Sedona Conference, *Commentary on Proportionality in Electronic Discovery*, 18 SEDONA CONF. J. 141, Principle 1, at 150 (2017) ("The burdens and costs of preserving relevant [ESI] should be weighed against the potential value and uniqueness of the information when determining the appropriate scope of preservation.").

99. Zubulake v. UBS Warburg, 220 F.R.D. 212, 217 n.22 (S.D.N.Y. 2003). *See also, e.g.*, Gen. Elec. Co. v. Wilkins, No. 1:10-cv-00674, 2012 WL 570048, at *5 (E.D. Cal. Feb. 21, 2012) (noting that backup tapes are generally considered to be inaccessible or at least not reasonably accessible due to undue burden and cost); United States ex rel. Carter v. Bridgepoint Educ., Inc., 305 F.R.D. 225, 241 (S.D. Cal. 2015) (suggesting that backup tapes are per se inaccessible).

otherwise available."[100] *The Sedona Principles, Third Edition* is in accord with this view.[101]

The logic of this conclusion is reinforced by the emphasis on proportionality in the amended Federal Rules, and which was presaged by earlier case law. For example, in *Escobar v. City of Houston*, the fact that the discoverable information had been preserved and was available from a more accessible source mitigated concern about the failure to preserve audio tapes.[102] Notably, the reasoning behind the general rule excluding

---

100. *Zubulake*, 220 F.R.D. at 218. *See also* Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC, 685 F. Supp. 2d 456, 480 n.99 (S.D.N.Y. 2010), *abrogated on other grounds by* Chin v. Port Auth. of N. Y. & N. J., 685 F.3d 135 (2nd Cir. 2012) ("I am not requiring that *all* backup tapes must be preserved. Rather, if such tapes are the *sole* source of relevant information (e.g., the active files of key players are no longer available), then such backup tapes should be segregated and preserved. When accessible data satisfies the requirement to search for and produce relevant information, there is no need to save or search backup tapes.") (emphasis in original); Forest Labs., Inc. v. Caraco Pharm. Labs., Ltd., No. 06-CV-13143, 2009 WL 998402, at *7 (E.D. Mich. Apr. 14, 2009) (announcing proceedings limited to assessing *Zubulake* exception on delayed decision to cease recycling backup media).

101. *The Sedona Principles, Third Edition, supra* note 1, Cmt. 5.h., at 112 ("Absent good cause, preservation obligations should not extend to disaster recovery storage systems."); *see id.* at Cmt. 8.a., at 136 ("[M]ere suspicion that a source may contain discoverable, but duplicative ESI is not sufficient to require preservation of that source 'just in case.'").

102. No. 04-1945, 2007 WL 2900581, at *17–19 (S.D. Tex. Sept. 29, 2007); *see also, e.g.*, West v. Talton, No. 5:13-CV-338, 2015 WL 6675565, at *2 (M.D. Ga. Nov. 2, 2015) (The routine destruction of backup tapes did not warrant spoliation sanctions where defendant still had access to the hard drive in question and could restore it and recover responsive emails.); *In re* Delta/AirTran Baggage Fee Antitrust Litig., 770 F. Supp. 2d 1299, 1310–11 (N.D. Ga. 2011) (Defendants' delay in preserving backup tape information was not sanctionable in part because defendants produced some documents from the time period at issue from alternate sources and plaintiffs had an opportunity to depose all key employees.).

inaccessible data (such as backup tapes) from preservation is not based simply on the expense of saving a tape—which, in isolation, is relatively slight. Instead, it is based upon principles of proportionality—i.e., the need for preservation of information balanced against the ultimate cost of later restoring data sources and culling them for particular content.[103]

Ultimately, "[a] party's identification of sources of ESI as not reasonably accessible does not relieve the party of its common-law or statutory duties to preserve evidence."[104] However, this observation should be read in conjunction with Rule 37(e), which allows for the imposition of sanctions or curative measures in the face of lost ESI *only* if the party "failed to take reasonable steps to preserve it."[105]

Probative Value: A third factor to consider in weighing preservation obligations is the nature of the information involved[106] and whether the data is unique and non-duplicative.[107]

---

103. *See, e.g.*, FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment (One "factor in evaluating the reasonableness of preservation efforts is proportionality."); Hon. Joy Flowers Conti & Richard N. Lerrieri, *E-Discovery Ethics: Emerging Standards of Technological Competence*, FED. LAW. 28, 31 (Oct./Nov. 2015) ("Proportionality is a guiding principle in determining the breadth and extent of the preservation required" under the Federal Rules.). *See also The Sedona Principles, Third Edition, supra* note 1, Cmt. 2.d., at 68 (noting the "full range" of considerations when assessing proportionality), and Cmt. 5.h., at 116 (referring to the role of "proportionality considerations" in preservation of backup tape).

104. FED. R. CIV. P. 26 advisory committee's note to 2006 amendment.

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

106. The Sedona Conference, *Commentary on BYOD: Principles and Guidance for Developing Policies and Meeting Discovery Obligations,* 19 SEDONA CONF. J. 495, Cmt. 3.d., at 534 (2018) ("The concept of proportionality also limits the scope of discovery of ESI on employee-owned devices.").

107. *See* Oracle America, Inc. v. Hewlett Packard Enter. Co., 328 F.R.D. 543 (N.D. Cal. 2018) (declining to impose sanctions on plaintiff after its Chief

Arguably, marginal or repetitive data falls outside the scope of proportionality and its probative value may be outweighed by the cost to preserve and produce information.[108]

Relative Burdens (Costs): A fourth factor to be considered in deciding whether to preserve data is the relative burden it will impose on the organization to preserve it. Data stored on backup tapes, for example, can be expensive to recover while the value of that data is marginal, often because it is substantively duplicative of data that exists from a more accessible source, or it is of lesser importance to the issues in dispute.[109]

Other Preservation Issues

There are several other issues to consider when making preservation decisions.

Transient or Ephemeral Data: Transient or ephemeral data not kept in the ordinary course of business (and that the organization may have no means of preserving) may not need to be preserved.[110] Absent a showing of special need, *The Sedona*

Executive Officer destroyed over 500 electronic documents given that plaintiff still maintained alternative sources of such information).

108. *See* The Sedona Conference, *Commentary on Proportionality in Electronic Discovery*, 18 SEDONA CONF. J. 141, Principle 1, at 150 (2017) ("The burdens and costs of preserving relevant [ESI] should be weighed against the potential value and uniqueness of the information when determining the appropriate scope of preservation.").

109. *Id.*

110. See Kenneth J. Withers, *"Ephemeral Data" and the Duty to Preserve Discoverable Electronically Stored Information*, 37 U. BALT. L. REV. 349, 377 (2008); *See* 7th Circuit Electronic Discovery Committee, *Principles Relating to the Discovery of Electronically Stored Information*, Principle 2.04(d), 7TH CIRCUIT COUNCIL ON EDISCOVERY AND DIGITAL INFORMATION (2d ed. Jan. 2018), https://www.ediscoverycouncil.com/sites/default/files/7thCircuitESIPilotProgramPrinciplesSecondEdition2018.pdf (deleted, slack, fragmented, unallocated, RAM, or ephemeral data among categories of ESI generally not discoverable); U.S. DIST. CT, DIST. OF DEL., DEFAULT STANDARD FOR DISCOVERY,

Principles, Third Edition states that a responding party should not be required to "preserve, review, or produce deleted, shadowed, fragmented, or residual [ESI]."[111]

Instant messages and other forms of chat are increasingly used by organizations for substantive communications, both internally and externally. In the past, such data was often labeled "ephemeral," because it was not retained as a general practice and in many cases did not persist in an easily recoverable form. More modern chat and messaging applications store their conversations in a form that can be maintained and more easily recovered. The data maintained in these applications may be appropriate for preservation and should not be deemed inaccessible in most cases.[112]

The same may be true for voicemail messages. In some cases, the voice message is stored temporarily as an audio recording, which by virtue of the recording application is neither permanent nor easily accessible. In others, the voice message is transcribed or transmitted via email with an audio copy attached. In the latter case, the data (recording or transcription) is not ephemeral and would not likely qualify as inaccessible.

INCLUDING DISCOVERY OF ELECTRONICALLY STORED INFORMATION (ESI), Sched. A, *available at* http://www.ded.uscourts.gov/sites/default/files/pages/Electronic%20Discovery%20Default%20Standard.pdf (last visited Nov. 6, 2018).

111. *The Sedona Principles, Third Edition, supra* note 1, Principle 9, at 144.

112. *See* Siras Partners LLC v. Activity Kuafu Hudson Yards LLC, 2019 N.Y. Slip Op. 03303, 2019 WL 1905478 (N.Y. App. Div. Apr. 30, 2019) (failure to preserve WeChat messages or to recover data from later-damaged phones constitutes gross negligence justifying adverse inference and spoliation sanction); *cf*. Monolithic Power Systems, Inc. v. Intersil Corp., No. 16-1125, 2018 WL 6075046, at *3 (D. Del. Nov. 19, 2018) ("Intersil's motion with respect to WeChat messages also must be denied. Intersil has not disproven MPS's representation that the WeChat messages were 'deleted in the ordinary course of business, prior to MPS's legal department becoming aware of the issue.'").

Snapshots or Mirror Images: Parties sometimes seek to compel creation of a "mirror image" of hard drives to preserve data pending forensic examinations.[113] Rule 34(a) recognizes the right to "test or sample" information, but that right does not create a "routine right of direct access" for such purposes.[114] Instead, such access is granted on a proper showing and perhaps with certain defined conditions.[115] *The Sedona Principles, Third Edition* recognizes that "Rule 34 inspections of electronic information systems are disfavored."[116]

In some cases, parties may wish to affirmatively create "snapshots" of data as a defensive measure.[117] For example, the

---

113. Bank of Mongolia v. M&P Global Fin. Servs., Inc., 258 F.R.D. 514, 520 (S.D. Fla. 2009) (expert appointed to "retrieve any deleted responsive files" in light of (i) discrepancies between defendants' discovery responses and their concession that not all documents had yet been produced and (ii) production of responsive documents from third-party sources).

114. FED. R. CIV. P. 34(a) advisory committee's note to 2006 amendment.

115. *See, e.g.*, Klayman v. City Pages, No. 5:13-cv-143-Oc-22PRL, 2014 WL 5426515, at *5 (M.D. Fla. Oct. 22, 2014) ("[C]onclusory and unpersuasive assertions are inadequate to meet [plaintiff's] burden of showing good cause to warrant a forensic examination."); *Bank of Mongolia*, 258 F.R.D. at 520–21 (establishing procedure for review of defendants' computer records to "minimize intrusion"); Covad Commc'ns v. Revonet, Inc., 258 F.R.D. 5, 9–10 (D.D.C. 2009) (ordering forensic imaging of email servers for purposes of "preserv[ing] information as it currently exists").

116. *The Sedona Principles, Third Edition*, *supra* note 1, Comment 6.d., at 127.

117. It should be noted that forensic collection is not, nor should it be, the default method of collection and preservation. Instead, the duty to collect and preserve forensically arises only if: (i) the facts known to the preserving party or which the party should reasonably know would establish the need; or (ii) the requesting party has specifically requested it, and the producing party has either agreed or notified the requesting party upon receiving the request that it will not comply, at which point the requesting party seeks judicial intervention and obtains an order compelling such preservation and collection. *See The Sedona Principles, Third Edition, supra* note 1, Comment 8.c., at 141 ("[w]hile [forensic data acquisition] clearly is appropriate in some

ability to access the hard drives of laptops issued to key employees upon their departure may be useful if it is the sole source of deleted information.[118] While doing so is an option, that action is not required unless there is a reasonable anticipation of litigation involving issues relating to that employee.

Collection vs. Preservation: If there are many custodians or there is ongoing business information subject to the legal hold, *collecting* data at the outset of the legal hold may not be feasible. Sequestering the data can be disruptive to the business or technically unworkable in such circumstances. As a result, it is important to distinguish between preserving information in place, and collecting and sequestering it. It is possible that a technical solution, such as placing a custodian's data on hold on the server side, may preserve both current and subsequently created discoverable information.

If collecting data at an initial stage is not warranted, reasonable, or feasible, communications and monitoring processes become more important. It is critical that recipients of hold notices understand their duty to preserve information and how to meet that duty. Training sessions on legal hold compliance can be a useful tool to foster the effectiveness of legal holds.

---

circumstances . . . , it should not be required unless circumstances specifically warrant the additional cost and burden and there is no less burdensome option available"; also noting the need for careful protocols to address such collections).

118. *See, e.g.*, Cache La Poudre Feeds v. Land O'Lakes, 244 F.R.D. 614, 629 (D. Colo. 2007) (failure to refrain from "expunging" former key employees' hard drives sanctioned where backup tapes were no longer available for use in seeking deleted email).

Guideline 8: In circumstances where issuing a legal hold notice is appropriate, such a notice is most effective when the organization identifies the custodians and data stewards most likely to have discoverable information, and when the notice:

(a) **communicates in a manner that assists persons in taking actions that are, in good faith, intended to be effective;**
(b) **is in an appropriate form, which may be written, and may be sent by email;**
(c) **provides information on how preservation is to be undertaken, and identifies individuals who can answer questions about preservation;**
(d) **includes a mechanism for the recipient to acknowledge that the notice has been received, read, and understood;**
(e) **addresses features of discoverable information systems that may make preservation of discoverable information more complex (e.g., auto-delete functionality that should be suspended, or small sections of elaborate accounting or operational databases;**
(f) **is periodically reviewed and amended when necessary; and**
(g) **is followed up by periodic reminder notices, so the legal hold stays fresh in the minds of the recipients.**

When preparing a legal hold notice, it is particularly important that it be understandable by diverse groups within an organization. Counsel should review relevant pleadings or

other documents and then describe the litigation in a way that will be understood by those with responsibility for preserving information.

The initial and subsequent hold notices and reminders should describe the matter at issue, provide specific examples of the types of information at issue, identify potential sources of information, inform recipients of their legal obligations to preserve information (and suspend disposition practices, whether manual or automated), and include a reference to the potential consequences to the individual and the organization for noncompliance.[119] It should be in a form—which may include email, written hard-copy, or, in limited cases, oral notice—that is appropriate to the circumstances. The notice should also inform recipients whom they should contact if they have questions or need additional information. Again, a legal hold notice must be adapted to conform to the facts and circumstances unique to each case.

Because of the distributed nature of an organization's information, it may be appropriate to communicate a legal hold notice not only to relevant data-generating or -receiving custodians, but also to appropriate data stewards, records management personnel, information technology (IT) personnel, and other personnel to preserve other information sources and repositories within the organization. For example, IT personnel or others may need to suspend auto-delete functions or records disposition function.

---

119. *See* N.M. Oncology and Hematology Consultants v. Presbyterian Healthcare Servs., No. 1:12-cv-00527, 2017 WL 3535293 (D.N.M. Aug. 16, 2017) (directed preservation of all relevant information, described forms of information to be retained, detailed 17 subject matters, directed suspension of auto-delete programs, solicited identity of additional persons with relevant information, and required acknowledgement).

In addition, the organization should consider whether a preservation notice should be sent to third parties, such as contractors or vendors, including those that provide information technology services.

Organizations should consider requiring confirmations of compliance with such legal hold notices as a means of verifying that recipients understand and agree to comply with their preservation duties and obligations.[120] Appropriate responses to legal hold notices and the organization's expectations for compliance with them should be documented and, depending on the organization's structure, included in its compliance programs.

Importantly, while the use of a written legal hold notice is often appropriate, it is simply one method of executing preservation obligations, not the only method. An organization should consider whether a written notice—or a formal legal hold notice in any form—is necessary to implement the hold effectively and preserve the requisite information. In some instances, a notice may not be necessary and, in fact, may be an encumbrance or source of confusion.[121] One example of when notices need not

120. *See The Sedona Principles, Third Edition, supra* note 1, Cmt. 5.d., at 105; Guideline 10, *infra*.

121. Orbit One Commc'ns, Inc. v. Numerex Corp., 271 F.R.D. 429, 441 (S.D.N.Y. 2010) ("[D]epending upon the circumstances of an individual case, the failure to [issue a written legal hold] does not necessarily constitute negligence, and certainly does not warrant sanctions if no relevant information is lost. For instance, in a small enterprise, issuing a written litigation hold may not only be unnecessary, but it could be counterproductive, since such a hold would likely be more general and less tailored to individual records custodians than oral directives could be. Indeed, under some circumstances, a formal litigation hold may not be necessary at all."). *See also* Bouchard v. U.S. Tennis Ass'n, 15 Civ. 5920, 2017 WL 3868801, *2 (E.D.N.Y. Sept. 5, 2017) (Failure to institute a "litigation hold" notice is only one factor; the "absence of a litigation hold is not dispositive" because the parties had fully complied

be issued to effectuate preservation is a situation in which sources of likely discoverable information are subject to retention for sufficiently long periods pursuant to the organization's information management or record retention policy such that they will be preserved for the duration of the litigation without the need for a formal legal hold. Another is when sources of discoverable information can be immediately secured without requiring preservation actions by employees; for example, a read-only system of record for all pertinent research-and-development and product-quality information harnessed by a document management system. Nevertheless, some organizations in these situations may prefer to take a conservative approach and issue a written legal hold notice despite a very low risk of disposition.

There are also circumstances where the collection of information prior to any notice may be prudent; for example, where the custodian is the subject of the litigation or government investigation and there is reason to believe that he or she might take steps to delete or destroy discoverable information if aware of the circumstances.

ILLUSTRATIONS

Illustration i: Lydon Enterprises (Lydon) obtains information that leads it to reasonably anticipate litigation. Lydon issues a written legal hold notice to certain employees. The notice describes in easily understandable terms the information that falls within the scope of the employees' preservation duties. The notice also explains how employees are expected to gather and preserve discoverable information. Whenever Lydon obtains new information regarding the litigation that could affect the scope of the legal hold, its in-house counsel reviews the notice.

---

with their preservation obligations by preserving the videotaped footage that was relevant to the accident.).

The notice is revised and reissued as necessary, and a periodic reminder is issued to all employees with preservation obligations. Compliance with the notice is periodically assessed. This legal hold is likely to be considered effective or reasonable.

Illustration ii: Jones, Inc., (Jones) obtains information that leads it to reasonably anticipate litigation. In-house counsel for Jones identifies 40 people who she thinks might have discoverable information and instructs her secretary to call them and tell them to hold any information relevant to the potential litigation, which she describes in general terms. The secretary calls the employees but is unable to answer many of their questions. In-house counsel does not follow up on any of the employee questions. No written hold notice is issued. Litigation does not occur until 18 months later; at that point, in-house counsel begins collecting discoverable information. This approach may or may not be reasonable, depending upon the circumstances, including whether discoverable information was lost because of the failure to issue a written legal hold or follow up with identified custodians, and the prejudice, if any, caused by the loss of such information.

Illustration iii: Acme Industries (Acme), which owns various properties, completes its financial accounting for 2008 and files its tax returns. Under its record retention policy and supporting schedules, tax-related papers are held for five years or until that tax year's audit is complete (whichever occurs later), and documentation supporting its financial reports is held for eight years. In 2010, Acme was audited by the IRS, and questions were raised about Acme's valuation of certain properties, but no litigation was filed. If Acme reasonably concludes that the information needed to respond to questions during the audit are being retained pursuant to the company's information management and retention policy, it need not issue a formal legal hold notice. If, however, litigation is later filed, either by the government or by Acme for a refund after an adverse agency

determination, and it is reasonably likely that information beyond the parameters of the retained records may be necessary to address claims or defenses in the action, Acme would then be well-advised to issue a legal hold notice and take other steps discussed above to ensure the preservation of discoverable information.

Guideline 9: An organization should consider documenting the procedure of implementing the legal hold in a specific case when appropriate.

When appropriate, an organization should consider documenting the steps taken to ensure the appropriate and defensible implementation of specific holds. The documentation should include sufficient information to demonstrate that the legal hold was implemented in a reasonable and good-faith manner should there be a need to defend the process. In most cases, the process of issuing and implementing the legal hold and following up to preserve the data will provide sufficient documentation. Appropriate documentation of the legal hold process may include the following:

- The date and by whom the hold was initiated, and a brief analysis of the triggering event
- The initial scope of information, custodians, sources, and systems involved, including reasons the hold was scoped with these parameters
- Information from custodians in response to questionnaires, interviews, checklists, or other means, noting additional sources of information

- Reasoning for subsequent scope changes as new custodians or data are identified or initial sources are eliminated
- Notices and reminders sent, confirmations of compliance received (if any), and handling of exceptions
- A master list of data stewards, custodians, or data "owners" involved in the preservation effort

While it may never be necessary to disclose this information, or disclosure may be made only to the court *in camera* to preserve privileged legal advice and work-product information, the availability of documentation will preserve for the organization the option of disclosing the information if a challenge to its preservation efforts is raised. Documentation also may prove a valuable resource when responding to discovery requests. If the organization chooses to memorialize legal hold implementation efforts, the possibility of this voluntary or forced disclosure should be considered when drafting. Additionally, while the contents of a legal hold notice are not typically discoverable, the recipients and the date of the notice are discoverable information.

Having documentation of legal hold processes and implementation efforts can be an effective method of demonstrating that an organization has taken reasonable steps to comply with its preservation obligations and of invoking the protections afforded by amended Rule 37(e).

Guideline 10: Compliance with a legal hold should be regularly monitored.

Organizations should develop ways to periodically monitor legal hold compliance. Some tools to accomplish this may include requiring periodic confirmations from custodians and

data stewards, and annual compliance training concerning negative consequences for noncompliance. Organizations may also consider employing technological tools, such as automated solutions and dedicated "legal hold" platforms, to facilitate and track employee compliance.

Organizations may also consider tailoring their monitoring processes depending on the recipient of the legal hold notice. For example, a recipient who is intimately familiar with the discoverable information may require more initial education but less instruction on implementing specific holds. An employee who has received several legal hold notices in the past may need less instruction on the importance of hold compliance but benefit from periodic reminders of which holds remain active. An employee who is receiving his or her first legal hold notice, particularly an employee who is not familiar with the U.S. litigation system, may benefit from more education on the implications of noncompliance. A one-size-fits-all approach is unlikely to be successful.

Organizations may also consider designating one or more individuals within the legal department to be responsible for issuing the legal hold notice, answering employee questions, and conducting training to maintain ongoing compliance with the notice. For smaller organizations, outside counsel may be retained to perform this oversight function. These individuals may also be tasked with following up with unacknowledged legal holds, either personally or through auto-generated requests for acknowledgement.

The effort to ensure affected employees comply with their preservation obligations is an ongoing process throughout the course of litigation.[122] This may include distributing periodic

122. Alabama Aircraft Indus. v. Boeing Co., 319 F.R.D. 730, 746 (N.D. Ala. 2017) (finding "sufficient circumstantial evidence . . . to conclude that

reminders of the legal hold, as well as issuing updated legal hold notices reflecting changes in the scope of the legal hold.[123] Also, if the organization learns that additional employees may have discoverable information, the legal hold notice should be sent to those employees.

Likewise, if the legal hold applies to information created on a going-forward basis and pertains to a matter that represents substantial benefits or risks to the organization, the organization may wish to consider additional means of ensuring compliance. For example, for holds requiring preservation of newly created information, organizations may consider periodic reminders to ensure ongoing compliance.

The argument has been made in some matters that sole reliance on individuals to comply with preservation notices is unreasonable.[124] For example, a special master in a case involving a massive legal hold questioned the efficacy of preservation requirements that relied on recipients to move emails to avoid automatic deletion.[125] Another court expressed the view that "it is *not* sufficient to notify all employees of a legal hold and expect that the party will then retain and produce all relevant information."[126] In *Pension Committee*, the same court noted that "not

---

Boeing's agents acted with an intent to delete (or destroy) ESI . . . by an affirmative act which has not been credibly explained," where defendant's preservation efforts were uneven, with some employees' email deleted instead of collected, two compact discs lost from the legal department, and the ESI of departing employees never preserved).

123. This parallels Guideline 8, Illustration i, *supra*, on communicating changes in the scope of the legal hold.

124. *E.g.*, Treppel v. Biovail Corp., 249 F.R.D. 111, 115–20 (S.D.N.Y. 2008) (noting inadequacies of mere notification to employees of a legal hold).

125. *In re* Intel Corp. Microprocessor Antitrust Litig., 258 F.R.D. 280, 282–85 (D. Del. 2008).

126. Zubulake v. UBS Warburg, 229 F.R.D. 422, 432 (S.D.N.Y. 2004) (emphasis in original).

every employee will require hands-on supervision from an attorney[. But] attorney oversight of the process, including the ability to review, sample, or spot-check the collection efforts is important."[127]

However, in most cases, a careful combination of notification as described above, collection, and individual action should enable parties to rely on the good-faith actions of their employees. For example, in *Concord Boat Corp. v. Brunswick Corp.*, the court held that "[t]he fact that Defendant allowed individual employees to use discretion whether to retain e-mail is simply not indicative of bad faith." This is consistent with Principle 6 of *The Sedona Principles, Third Edition*: "Responding parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own electronically stored information."[128]

Guideline 11: Any legal hold process should include provisions for releasing the hold upon the termination of the duty to preserve, so that the organization can resume adherence to policies for managing information through its useful life cycle in the absence of a legal hold.

An organization creating a legal hold process should include procedures for releasing the holds once the organization is no longer obligated to preserve the information that was subject to a legal hold. These release procedures should include a process for conducting a custodian and data cross-check, so the organization can determine whether the information to be released is subject to any other ongoing preservation obligations.

---

127. Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Secs., LLC, 685 F. Supp. 2d 456, 473 n.68 (S.D.N.Y. 2010).

128. *The Sedona Principles, Third Edition*, *supra* note 1, Principle 6, at 118.

Organizations may consider using automated software that can perform custodian, system, and data cross-checking and provide for efficient legal hold management.

When the organization is satisfied that the information is not subject to other preservation obligations, reasonable efforts should be made to provide notice that the legal hold has been terminated to the recipients of the original notice (and any modifications or updated notices) and to records management, IT, and other relevant personnel, as well as any third parties notified of their obligation to preserve. Organizations may wish to conduct periodic audits to ensure that information no longer subject to preservation obligations is not unnecessarily retained and is being appropriately disposed of in accordance with the organization's records and information management policy.[129]

Guideline 12: An organization should be mindful of local data protection laws and regulations when initiating a legal hold and planning a legal hold policy outside of the United States.

Data protection laws and regulations may affect an organization's ability to implement legal hold data preservation measures. Even within the United States, a patchwork of sectoral laws and regulations may govern how data is stored, managed, accessed, or disclosed, including for preservation

129. *See* The Sedona Conference, *Commentary on Information Governance, Second Edition*, 20 SEDONA CONF. J. 95, 139–42 (2019), *available at* https://thesedonaconference.org/publication/Commentary_on_Information_Governance (discussing the need to dispose of information "that no longer needs to be retained"). *See also* The Sedona Conference, *Principles and Commentary on Defensible Disposition*, 20 SEDONA CONF. J. 179 (2019), *available at* https://thesedonaconference.org/publication/Commentary_on_Defensible_Disposition.

purposes.[130] Outside the United States, this effect is amplified in countries—especially non-common law countries—where U.S.-style preservation and discovery is unknown, and stricter, more comprehensive data protection laws and regulations are in place.[131]

---

130. Examples of U.S. federal laws that affect data management include: The Health Insurance Portability and Accountability Act of 1996 (Pub. L. 104–191) (HIPAA) and Health Information Technology for Economic and Clinical Health Act of 2009 (Pub. L. 111–5) (HITECH) (healthcare data); the Gramm-Leach Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999 (Pub. L. 106–102, 113 Stat. 1338) (financial data); and the Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510–22 (ECPA) (electronic communications). At the state level, Massachusetts sets strict requirements for management of certain data types. *See* STANDARDS FOR THE PROTECTION OF PERSONAL INFORMATION OF RESIDENTS OF THE COMMONWEALTH, 201 C.M.R. 17.00. Moreover, case law may restrict an organization's ability to preserve privileged and personal employee data accessible from within the organization's systems. *See*, *e.g.*, Pure Power Boot Camp v. Warrior Fitness Boot Camp, 759 F. Supp. 2d 417 (S.D.N.Y. 2010); Stengart v. Loving Care Agency, Inc., 408 N.J. Super. 54 (App. Div. 2009), *aff'd as modified and remanded*, 201 N.J. 300 (2010).

131. *See, e.g.*, 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]. The GDPR, which applies to entities established in the European Union (EU) or that offer goods or services to or monitor the behavior of data subjects in the EU, is a comprehensive data privacy law that impacts how companies can process personal data. The GDPR regulates the ability of companies to process personal data or transfer it outside the EU, especially for purposes—like litigation or investigations—that were unforeseen when data are collected or obtained. *See* GDPR, arts. 13.3, 14.4, 49.1(e). Although the GDPR allows a company to process and transfer personal data for the "establishment, exercise or defence of legal claims" in certain situations, it imposes very strict criteria for doing so. *Id*.

In the European Union (EU), for example, personal data protection is considered a fundamental human right.[132] European laws and regulations are designed to protect this right, including the protection of an individual's workplace data. These laws and regulations may prohibit or restrict an organization from "processing" such data, including retaining it *in situ* outside of a routine schedule, or copying, moving, or otherwise targeting it, including for purposes of U.S. preservation.[133] Beyond preservation, data protection laws and regulations may affect the range of activity covered by the Electronic Discovery Reference Model (EDRM) (e.g., collection, processing, analysis, review, and production), because transferring and disclosing personal data outside of the EU (and certain other approved countries with similar protections) is also restricted or prohibited.[134]

"Personal data" is defined broadly to include information from which an individual can be identified, directly or indirectly, including, for example, email and Internet Protocol (IP) addresses.[135] Heightened protection is afforded to classes of

---

132. *See, e.g.*, GDPR, *supra* note 131, at Recital 1. Effective May 25, 2018, the GDPR replaced Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281), *available at* https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:31995L0046 [hereinafter EU Data Protection Directive].

133. "Processing" is defined as "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." GDPR, *supra* note 131, at art. 4(2).

134. *See generally* GDPR, *supra* note 131, at ch. V.

135. "Personal data" is defined as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference

sensitive personal data, including some information that may be found in Human Resource (HR) records.[136] Moreover, U.S.-style general waivers or consent may be deemed invalid in the employer/employee context.[137] The General Data Protection Regulation (GDPR) includes a range of penalties for violations, up to the higher of €20 million or 4 percent of total worldwide annual turnover (i.e., gross revenue) for the preceding year.[138]

Many countries outside the EU have data protection laws and regulations in place that may similarly restrict or prohibit U.S. preservation and discovery activity.[139] In addition to data

---

to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." GDPR, *supra* note 131, at art. 4(1).

136. Sensitive data is personal data that reveals "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership" and also includes "genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation." GDPR, *supra* note 131, at art. 9.

137. *See, e.g.*, Art. 29 Data Protection Working Party, *Guidelines on Consent Under Regulation 2016/679*, WP 259 (Adopted Nov. 28, 2017, revised and adopted Apr. 10, 2018), http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030. Although WP 29 ceased operations when the GDPR became effective in May 2018, its opinions continue to be authoritative. Indeed, the date the GDPR became effective, the European Data Protection Board (EDPB), which took over the functions of WP 29, issued Guidelines on the transfer of personal data that expressly endorsed WP 259. EDPB, *Guidelines 2/2018 on Derogations of Article 49 Under Regulation 2016/679*, https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en.

138. GDPR, *supra* note 131, at art. 83.

139. For a general overview and "heat map" of global data protection laws, *see* DLA Piper, *Data Protection Laws of the World, available at* https://www.dlapiperdataprotection.com/index.html#handbook/world-map-section (last visited Nov. 6, 2018).

protection laws, other laws that may affect an organization's ability to preserve data and implement a legal hold include local privacy laws, labor laws, laws designed to protect national sovereignty interests, "blocking statutes," telecom laws, and other industry-specific and sectoral laws.[140] Parties should consider the effect, if any, that these laws may have on their U.S. discovery obligations, including preservation.

To minimize conflicts between data protection laws and other laws limiting an organization's ability to manage data for U.S. preservation and discovery processes, an organization may implement checks and safeguards as outlined in several Sedona Conference publications, including the *International Principles on Discovery, Disclosure & Data Protection in Civil Litigation*;[141] *International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices*;[142] and *Practical In-House Approaches for Cross-Border Discovery & Data Protection*.[143] Such measures may include taking a tiered approach to preservation in the United States and elsewhere, and limiting the scope of preservation outside the United States to data that is necessary—and unique—for the specific legal purpose. Moreover, organizations should ensure

140. *See generally* The Sedona Conference, *International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition)*, THE SEDONA CONFERENCE (Jan. 2017), https://thesedonaconference.org/publication/International_Litigation_Principles.

141. *Id*.

142. The Sedona Conference, *International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices*, 19 SEDONA CONF. J. 557 (2018).

143. The Sedona Conference, *Practical In-House Approaches for Cross-Border Discovery & Data Protection: Principles, Commentary & Best Practices*, 17 SEDONA CONF. J. 397 (2016); *see also* Taylor Hoffman and James Sherer, *Cross-Border Legal Holds: Challenges and Best Practices*, PRAC. L. J., at 28–37 (Oct/Nov. 2017).

timely legal hold releases, i.e., hold the information only for the duration that it is necessary to undertake preservation efforts.[144]

ILLUSTRATION

Illustration i: Multinational Corporation ("MNC") is sued in U.S. Federal Court by a former employee alleging discrimination based on gender, religion, national origin, and a disability. Plaintiff's supervisors were based in France and Canada, and plaintiff was seconded by affiliated entities in both countries during her employment. Assessing its U.S. preservation duties pursuant to its global legal hold program, MNC preserves data specifically related to the plaintiff from plaintiff's supervisors, including communications with and about the plaintiff. MNC does not extend preservation further up the chain of command or to entire departments where plaintiff worked outside the United States. MNC documents steps taken to comply with U.S. preservation obligations and with local data protection and other relevant laws, and outlines preservation scope in the Rule 26(f) conference. MNC's actions should be an appropriate means to mitigate the potential conflict between non-U.S. data protection regulations and U.S. data preservation obligations.

144. *See* GDPR, *supra* note 131, at Recital 39.

THE BURDEN OF PRIVACY IN DISCOVERY*

*Robert D. Keeling & Ray Mangum***

Traditionally, the scope of discovery under Rule 26 of the Federal Rules of Civil Procedure and its state law analogues was defined exclusively in terms of relevance, with privilege providing but a narrow exception. Private matters by default were discoverable, even where the privacy interests were significant and the relevance only marginal. To obtain relief, a producing party was required to seek a protective order under Rule 26(c) and establish good cause. Beginning with the 1983 amendments, however, the scope of discovery under Rule 26(b) has been limited by a growing list of proportionality factors, which weigh both monetary and nonpecuniary burdens imposed upon the

---

* This article has been prepared for informational purposes only and does not constitute legal advice. This information is not intended to create, and the receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this without seeking advice from professional advisers. The views and opinions expressed in this article are those of the authors only and do not reflect in any way the views and opinions of any law firm, company, agency, or other entity to which the authors are affiliated.

** Robert Keeling is a partner at Sidley Austin LLP, an experienced litigator whose practice includes a special focus on electronic discovery matters, and co-chair of the firm's eDiscovery Task Force. He represents both plaintiffs and defendants in civil litigation throughout the nation and conducts internal investigations in the United States and throughout the world. Ray Mangum is an associate at Sidley Austin LLP who represents clients in a variety of government investigations and commercial disputes, with a particular focus on matters involving complex data analytics and eDiscovery issues. Special thanks to Michael Buschbacher for his careful research and thoughtful edits. Thanks also to Christopher Joyce and Kristen Bartolotta for their valuable assistance.

producing party against the likely value of the otherwise discoverable material. Although these proportionality factors began as an integral part of the definition of the scope of discovery, for more than two decades these limitations resided in a separate subsection of the Rule, resulting in considerable confusion and less-than-rigorous enforcement. The 2015 amendments to Rule 26(b)(1), however, were meant to resolve any doubt, returning the proportionality factors to their original place as part of the very definition of what is discoverable. To be within the scope of discovery, an inquiry now must be both relevant as well as proportional.

This emphasis on proportionality in discovery arrives at a time when the protection of privacy is of increasing concern in the United States and abroad. Recent advances in technology—smart phones and social media in particular—have allowed businesses to collect, store, and find ways to monetize far more personal data than ever before. With the rise of Big Data, however, there has been a growing and well-founded concern that personal information might be used unethically or exposed improperly. Protection of personal privacy has consequently become an important goal both in technological development—e.g., the increasing prevalence of "privacy by design" in communications programs such as "ephemeral" messaging systems—and in governmental regulation. To pick just two recent examples of the latter, the European Union's General Data Protection Regulation[1] (GDPR) and the California Consumer

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. (L119/1) *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679#PP3Contents.

Privacy Act[2] (CCPA) both impose sweeping requirements on businesses with the aim of increasing consumers' privacy and control over how their personal data is used.

The renewed prominence of the Rule 26(b) proportionality factors as part of the definition of the scope of discovery has provided a solid textual basis for giving weight to such privacy "burdens" in defining the scope of discovery. As a result, an emerging consensus of courts and commentators has concluded that privacy may—indeed, should—be considered as part of the proportionality analysis required under Rule 26(b)(1). As we aim to explain in this article, that conclusion is well founded not only in the text of Rule 26, but also in its historic underpinnings, which provide important context for more recent developments and continue to inform how judges and advocates should consider privacy concerns in discovery.

HISTORY OF PROPORTIONALITY AND THE SCOPE OF CIVIL DISCOVERY

The principle of proportionality in civil discovery is hardly new.[3] The Federal Rules of Civil Procedure have begun—since their inception—with a guiding command for courts to seek "to secure the just, speedy, and inexpensive determination of every action and proceeding."[4] In keeping with that aim, the scope of

2. CAL. CIV. CODE § 1798.100.

3. *See, e.g.,* Welty v. Clute, 1 F.R.D. 446, 446–47 (W.D.N.Y. 1940) (finding that it was unnecessary to grant a second deposition of plaintiff in addition to granting discovery); Waldron v. Cities Serv. Co., 361 F. 2d 671, 673 (2d Cir. 1966) (stating that a plaintiff "may not seek indefinitely . . . to use the [discovery] process to find evidence"); *see also* Daniel J. Solove & Woodrow Harzog, *The Ultimate Unifying Approach to Complying with all Laws and Regulations*, 19 GREEN BAG 2D 223 (2016) ("Be reasonable.").

4. ADVISORY COMMITTEE ON RULES FOR CIVIL PROCEDURE, REPORT OF THE ADVISORY COMMITTEE ON RULES FOR CIVIL PROCEDURE CONTAINING

discovery has always been cabined. The original Rule 26, which applied to depositions only, limited the "Scope of Examination" to matters "not privileged" and "relevant to the subject matter involved in the pending action."[5] Even prior to the adoption of the Federal Rules in 1938, courts applied principles of proportionality to the cases in their dockets.[6]

Yet an express proportionality limitation on the scope of discovery did not appear in the Federal Rules until 1983, when Rule 26(b)(1) was further amended.[7] The revised Rule required courts to consider a variety of proportionality factors, including whether "the discovery sought [was] unreasonably cumulative or duplicative" and whether "the discovery [was] unduly burdensome or expensive" in light not only of "the amount in controversy" but also of less-tangible and even nonpecuniary considerations such as "the needs of the case," the "limitations on the parties' resources," and "the importance of the issues at stake in the litigation."[8]

The revised Rule "recogni[zed] that the right of pretrial disclosure is subject to some limitation beyond relevance."[9] Yet it

---

PROPOSED RULES OF CIVIL PROCEDURE FOR THE DISTRICT COURTS OF THE UNITED STATES (1937).

5. *Id.* at 66 (Rule 26(b)).

6. *See* Hon. Elizabeth D. Laporte & Jonathan M. Redgrave, *A Practical Guide to Achieving Proportionality Under New Federal Rule of Civil Procedure 26*, 9 FED. CTS. L. REV. (ISSUE 2) 19, 24–25 (2015) ("Indeed, the concept of proportionality existed in practice long before being officially embodied in the Federal Rules.").

7. FED. R. CIV. P. 26(b)(1) (1983).

8. *Id.*

9. Edward D. Cavanagh, *The August 1, 1983 Amendments to the Federal Rules of Civil Procedure: A Critical Evaluation and a Proposal for More Effective Discovery through Local Rules*, 30 VILLANOVA L. REV. 767, 786 (1985); see also Arthur R. Miller, *Confidentiality, Protective Orders, and Public Access to the Courts*, 105 HARV. L. REV. 427, 459 (1991) ("A basic shift in discovery

was aimed most squarely at curbing the types of duplicative, excessive, "scorched earth" discovery practices prevalent at the time—i.e., at the problem of so-called "overdiscovery."[10] As the advisory committee's note to the 1983 amendment explained, the amended Rule sought to "prevent use of discovery to wage a war of attrition or as a device to coerce a party, whether financially weak or affluent."[11] In other words, the 1983 amendment was seen as limiting the depth rather than the breadth of discovery.[12]

Ten years later, in 1993, the scope of discovery was further refined when Rule 26(b) was again amended, this time in recognition that "[t]he information explosion of recent decades ha[d] greatly increased both the potential cost of wide-ranging discovery and the potential for discovery to be used as an instrument for delay or oppression."[13] Two additional proportionality factors were added: the first asked whether "the burden or expense of the proposed discovery outweighs its likely benefit," and the second considered "the importance of the proposed

---

philosophy was evidenced by the [1983] elimination of the sentence in Rule 26(a) stating that 'the frequency of use of [the discovery] methods is not limited.'").

10. *See, e.g.*, Am. Bar Ass'n Section of Litig., Comments on Revised Proposed Amendments to the Federal Rules of Civil Procedure 6–11 (1979) (unpublished) (discussing the reasoning for the proposed amendments to Rule 26, and noting that ample evidence existed to support the idea that "overuse" of discovery was a real problem).

11. FED. R. CIV. P. 26(b) advisory committee note to 1983 amendment.

12. *See* Cavanagh, *supra* note 9, at 786–87 n.93 (citing FED. R. CIV. P. 26(b)(1); AM. BAR ASS'N SECTION OF LITIG., REPORT OF THE SPECIAL COMMITTEE FOR THE STUDY OF DISCOVERY ABUSE *in* 92 F.R.D. 149 (1977); Maurice Rosenberg & Warren R. King, *Curbing Discovery Abuse in Civil Litigation: Enough is Enough,* 1981 B.Y.U. L. REV. 579 (1981); Hon. Mary M. Schroeder & John P. Frank, *The Proposed Changes in the Discovery Rules,* 1978 ARIZ. ST. L.J. 475 (1978).

13. FED. R. CIV. P. 26(b) advisory committee note to 1993 amendment.

discovery in resolving the issues."[14] These changes were intended to "enable courts to keep a tighter rein on the extent of discovery."[15] Unfortunately—out of a desire to avoid a larger renumbering of Rule 26(b) that would have resulted from other revisions—Rule 26(b)(1) was split into two subparagraphs, severing the proportionality limitations from the core definition of the scope of discovery.[16] As the 2015 advisory committee note observed, while not intended, this structural change to Rule 26 "could [have been] read to separate the proportionality provisions as 'limitations,' no longer an integral part of the (b)(1) scope provisions."[17] Indeed, in the years following the 1993 amendments, "[t]he Committee [was] told repeatedly that courts ha[d] not implemented these [proportionality] limitations with the vigor that was contemplated." In a minor effort to combat that trend, Rule 26(b)(1) was amended yet again in 2000 to add an "otherwise redundant cross-reference" to the proportionality factors then residing in Rule 26(b)(2).[18]

Most recently, in 2015, the scope of discovery under Rule 26(b) was amended to "restore[] the proportionality factors to their original place in defining the scope of discovery."[19] No longer are the proportionality considerations described as separate "limitations" on an inquiry governed solely by relevance.[20] Under the revised Rule 26(b)(1), proportionality once again stands on equal footing alongside relevance in defining the

14. FED. R. CIV. P. 26(b) advisory committee note to 2015 amendment.
15. FED. R. CIV. P. 26(b) advisory committee note to 1993 amendment.
16. *See* FED. R. CIV. P. 26(b) advisory committee note to 2015 amendment.
17. *Id.*
18. FED. R. CIV. P. 26(b) advisory committee note to 2000 amendment.
19. FED. R. CIV. P. 26(b) advisory committee note to 2015 amendment.
20. *Id.*

scope of discovery.[21] If it is not both relevant as well as proportional, it is not discoverable. At the same time, an additional proportionality factor was added— "the parties' relative access to relevant information"—and the growing list of proportionality factors was re-ordered to begin with the more-specific factors and to conclude with a general proportionality limitation whenever "the burden or expense of the proposed discovery outweighs its likely benefit."[22] While these changes did not add much new in substance, the increase in clarity and the emphasis on proportionality augured a significant practical effect on how discovery is actually conducted. As Chief Justice John Roberts put in his *2015 Year-End Report on the Federal Judiciary*, these changes "crystalize[d] the concept of reasonable limits on discovery through increased reliance on the common-sense concept of proportionality."[23]

PRIVACY IS A "BURDEN" UNDER RULE 26(b)(1)

"The Federal Rules of Civil Procedure were designed to effect a revolution in litigation by broadening the availability of discovery."[24] While this broadening arguably served the interests of justice in many cases,[25] it also created a system that could

21. FED. R. CIV. P. 26(b)(1).

22. *Id.*

23. CHIEF JUSTICE JOHN G. ROBERTS, JR., 2015 YEAR-END REPORT ON THE FEDERAL JUDICIARY, U.S. SUP. CT. (Dec. 31, 2015), https://www.supremecourt.gov/publicinfo/year-end/2015year-endreport.pdf.

24. Richard L. Marcus, *Myth and Reality in Protective Order Litigation*, 69 CORNELL L. REV. 1, 6 (1983).

25. *See, e.g.*, Hickman v. Taylor, 329 U.S. 495, 507 (1947) ("No longer can the time-honored cry of 'fishing expedition' serve to preclude a party from inquiring into the facts underlying his opponent's case.").

be burdensome and susceptible to abuse.[26] As Justice Lewis Powell observed when writing on behalf of a unanimous Court in *Seattle Times Co. v. Rhinehart*, abuse of discovery "is not limited to matters of delay and expense; discovery also may seriously implicate privacy interests of litigants and third parties."[27] Yet, prior to the 1983 amendments, Rule 26(b)(1) provided no avenue for relief from the production of private information, even if only of marginal relevance.[28] Thus, when Justice Powell looked to the text of the discovery rules at issue in *Seattle Times*,[29] he found that:

> [t]he Rules do not differentiate between information that is private or intimate and that to which no privacy interests attach. Under the Rules, the only express limitations are that the information sought is not privileged, and is relevant to the subject matter of the pending action. Thus, the Rules often allow extensive intrusion into the affairs of both litigants and third parties.[30]

---

26. *See, e.g.*, Marcus, *supra* note 24, at 6; Herbert v. Lando, 441 U.S. 153, 177 (1979) (Powell, J., concurring) (Experience has shown that the Rules have "not infrequently [been] exploited to the disadvantage of justice.").

27. 467 U.S. 20, 34–35 (1984).

28. FED. R. CIV. P. 26(b) advisory committee note to 1983 amendment (stating that the changes to Rule 26(b)(1) were "designed to . . . limit the use of the various discovery devices").

29. *Seattle Times* involved a First Amendment challenge to a protective order issued by a state court pursuant to Washington Superior Court Civil Rule 26(c). 467 U.S. at 34. As noted in the opinion, however, the Washington rules were modeled after the Federal Rules, *id.* at 29–30, and Washington Superior Court Civil Rule 26(b)(1) in particular was identical to Federal Rule of Civil Procedure 26(b)(1) in effect at the time, *id.* at 30 n.15.

30. *Id.* at 30.

A protective order under Rule 26(c) provided the only tool for courts— upon motion and good cause shown—to "protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense," including by ordering "that certain matters not be inquired into."[31] Showing good cause was (and is) often difficult in contested matters.[32] And even with the rise of stipulated protective orders, invasive discovery remained the norm, and protection of personal privacy the exception.[33] Thus, as prominent trial lawyer (and former federal judge) Simon Rifkind remarked in 1976, "a foreigner watching the discovery proceedings in a civil suit would never suspect that this country has a highly-prized tradition of privacy enshrined in the fourth amendment."[34]

It is therefore somewhat surprising to look back at the pre-2015 history of the amendments to the scope of civil discovery under Rule 26(b) and find little mention of privacy interests in the discussion.[35] Rather, early discussion of the proportionality factors focused primarily on economic factors.[36] A notable (though partial) exception to this lack of discussion arose from cases where a party sought direct access to an opposing party's

---

31. FED. R. CIV. P. 26(c) (1970).

32. *See, e.g.*, Marcus, *supra* note 24, at 23–26.

33. FED. R. CIV. P. 26 advisory committee note to 1983 amendment (noting existing practice of issuing protective orders, but concluding that "[o]n the whole, however, district judges have been reluctant to limit the use of the discovery devices").

34. Hon. Simon H. Rifkind, Are We Asking Too Much of Our Courts?, Address at the National Conference on the Causes of Popular Dissatisfaction with the Administration of Justice (1976) *in* 70 F.R.D. 96, 107.

35. *See* Babette Boliek, *Prioritizing Privacy in the Courts and Beyond*, 103 CORNELL L. REV. 1101, 1128–29 (2018).

36. *See* FED. R. CIV. P. 26(b) advisory committee note to 1983 amendment; *see also* Boliek, *supra* note 35, at 1129 ("[t]he word 'privacy' was curiously absent from this new list of factors").

computer systems under Rule 34(a)(1), which allows parties "to inspect, copy, test or sample . . . any designated tangible things."[37] Computers are tangible things, after all, and many litigants over the years have sought to test, sample, or obtain copies of an opposing party's computer or entire computer system. Such requests are disfavored, however, not only because of the cost and inconvenience, but also because of the threat to privacy.[38] As the advisory committee notes explain, "issues of burden and intrusiveness" raised by Rule 34(a)(1) include "confidentiality [and] privacy."[39] Notably, the advisory committee concluded that such issues "can be addressed under [either the proportionality factors formerly codified in] Rule 26(b)(2) [or] [under the protective order procedures set forth in Rule] 26(c)."[40] An important assumption in this directive was the advisory committee's intent that the burden of privacy should be considered in setting the scope of discovery.

---

37. FED. R. CIV. P. 34(a)(1).

38. *See, e.g.*, S.E.C. v. Strauss, No. 09 Civ. 4150, 2009 WL 3459204, at *12 n.8 (S.D.N.Y. Oct. 28, 2009) ("There is a general reluctance to allow a party to access its adversary's *own* database directly."); NOLA Spice Designs, LLC v. Haydel Enterprises, Inc., No. CIV.A. 12-2515, 2013 WL 3974535, at *2 (E.D. La. Aug. 2, 2013).

39. FED. R. CIV. P. 34(a)(1) advisory committee note to 2006 amendment; see also The Sedona Conference, *The Sedona Principles, Third Edition: Best Practices, Recommendations & Principles for Addressing Electronic Production*, 19 SEDONA CONF. J. 1, 128–29 (2018) [hereinafter The Sedona Principles, Third Edition] ("Direct access to an opposing party's computer systems under a Rule 34 inspection also presents possible concerns such as: . . . revealing . . . highly confidential or private information, such as personnel evaluations and payroll information, properly private to individual employees; . . . revealing confidential attorney-client or work-product communications; . . . [and] placing a responding party's computing systems at risk of a data security breach.").

40. FED. R. CIV. P. 34(a)(1) advisory committee note to 2006 amendment.

However, while many cases discussing direct access requests have cited privacy concerns, few have done so within the framework of a Rule 26(b) proportionality analysis.[41] It is not that these cases have rejected this proportionality framework, but rather that they have simply ignored it. For example, in *John B. v. Goetz*, the Sixth Circuit granted mandamus relief to two state defendants who had been ordered by the district court to provide forensic imaging of their computers, noting that "[t]he district court's compelled forensic imaging orders here fail[ed] to account properly for the significant privacy and confidentiality concerns present in this case."[42] Despite putting great weight on the privacy implications in its decision to grant relief, that opinion did not cite Rule 26(b).

In this context and others, it remained common to think of privacy as a separate consideration—distinct from proportionality—even among thoughtful and forward-looking commentators. For example, when *The Sedona Principles, Second Edition* were published in June 2007, Principle 10 stated that "[a] responding party should follow reasonable procedures to protect privileges and objections in connection with the production of electronically stored information"[43] and Comment 10.e addressed "[p]rivacy, trade secret, and other confidentiality concerns."[44] The Comment recognized that "[e]lectronic

41. The only pre-2015 case we have found that analyzed a direct-access request using the proportionality framework of Rule 26(b) is *NOLA Spice Designs*, 2013 WL 3974535, at *2.

42. 531 F.3d 448, 460 (6th Cir. 2008); *see also* White v. Graceland Coll. Ctr. for Prof'l Dev. & Lifelong Learning, Inc., No. CIV.A. 07-2319-CM, 2009 WL 722056, at *7 (D. Kan. Mar. 18, 2009).

43. The Sedona Conference, *The Sedona Principles, Second Edition: Best Practices, Recommendations, & Principles for Addressing Electronic Production*, p. 51 (June 2007), *available at* https://thesedonaconference.org/publication/The_Sedona_Principles.

44. *Id.* at 56, cmt. 10.e.

information systems contain significant amounts of information that may be subject to trade secret, confidentiality, or privacy considerations," including a wide variety of proprietary business information as well as "customer and employee personal data (e.g., social security and credit card numbers, employee and patient health data, and customer financial records)."[45] Moreover, the Comment appropriately warned that "[p]rivacy rights related to personal data may extend to customers, employees, and non-parties." Yet it did not mention any of the proportionality factors as potentially imposing a limit on the discovery of private information. Rather, it concluded that "the identification and protection of privacy rights are not directly addressed in the [then-recent] 2006 amendments" and reassured parties that "ample protection for such information during discovery is available through a Rule 26(c) protective order or by party agreement."

Even today, it remains common, among both the bench and the bar, to think of proportionality in discovery as relating primarily to financial burdens.[46] With the re-emphasis on

45. *Id.*

46. Agnieszka A. McPeak, *Social Media, Smartphones, and Proportional Privacy in Civil Discovery*, 64 U. KAN. L. REV. 235, 253 (2015) ("Even with the renewed emphasis on proportionality in the 2015 amendments, the proportionality test itself largely focuses on economic concerns. Indeed, the ''burden or expense'' that the court weighs against the needs of the case are largely financial burdens."); *see also* Samsung Elec. Am. Inc. v. Chung, 325 F.R.D. 578, 592 (N.D. Tex. 2017) (listing the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit as part of the proportionality analysis, many of which relate to the financial burden of discovery). *But see* Henson v. Turn, Inc., No. 15-cv-01497-JSW (LB), 2018 WL 5281629, at *5 (N.D. Cal. Oct. 22,2018) ("While questions of proportionality often arise in the context of

proportionality brought about by the 2015 amendments and the growing public debate over the importance of privacy, however, there has been a clear trend by courts and commentators toward recognition of privacy interests as an integral part of the proportionality analysis required by Rule 26(b)(1).

With the publication of *The Sedona Principles, Third Edition* in 2018, Principle 10 was "modified to refer specifically to privacy obligations because of the increasing importance of privacy in the United States and abroad."[47] Principle 10 now states that "[p]arties should take reasonable steps to safeguard electronically stored information, the disclosure or dissemination of which is subject to privileges, work product protections, privacy obligations, or other legally enforceable restrictions." And new Comment 10.j, which expands on the prior Comment 10.e, instructs that "[p]arties should be aware of and identify personal privacy, trade secret, and confidential ESI [Electronically Stored Information], and properly protect such information from unlawful or inappropriate disclosure."[48] While the Comment still instructs parties that the possibility of a protective order or party agreement provides "[a]mple protections," the Third Edition now also urges parties to discuss appropriate protections for confidential information at the Rule 26(f) conference and even suggests, by way of example, that the "parties may agree to exclude from production categories of private, personal information that are only marginally relevant to the claims and defenses or are cumulative of other produced information."[49] Taken together with Comment 2.c's instruction that "[p]roportionality of discovery of ESI should be addressed by the parties

disputes about the expense of discovery, proportionality is not limited to such financial considerations.").

47. *The Sedona Principles, Third Edition*, *supra* note 39, at 44.

48. *Id.* at 162, cmt. 10.j.

49. *Id.* at 163.

and counsel at the Rule 26(f) meet and confer," Comment 10.j appears to embrace privacy as an aspect of proportionality.[50]

Support has also come from the academic sphere. Shortly after the 2015 amendments, Professor Agnieszka A. McPeak argued in *Social Media, Smartphones, and Proportional Privacy in Civil Discovery* that the proportionality analysis under Rule 26(b)(1) ought to consider not only financial burdens but also the burden of privacy.[51] Looking to the historical development of civil discovery under the Federal Rules and analyzing the intersection between civil discovery and general principles of privacy law, Professor McPeak concluded that courts should consider privacy interests as part of proportionality, particularly as applied to digital data compilations such as social media accounts and mobile devices.[52] More recently, Professor Babette Boliek has advocated for similar limitations in her 2018 article *Prioritizing Privacy in the Courts and Beyond*.[53]

Most importantly, a growing number of courts have followed suit. In October 2018, Magistrate Judge Laurel Beeler expressly held in *Henson v. Turn, Inc.* that privacy interests were an appropriate part of the proportionality analysis required by Rule 26(b)(1).[54] The case involved a data-privacy class action wherein plaintiffs alleged that the defendant had placed so-called "zombie cookies" on users' mobile devices that not only allowed the defendant to track users across the web but also "respawned" whenever users attempted to delete them. During discovery, the defendant issued a number of requests to plaintiffs, including requests for the production of the plaintiffs'

50. *Id.* at 67, 162.

51. McPeak, *supra* note 46, at 236.

52. *Id.*

53. Boliek, *supra* note 35, at 1129–31.

54. 2018 WL 5281629, at *5 (N.D. Cal. Oct. 22, 2018).

mobile devices for inspection (or complete forensic images of such devices), production of plaintiffs' full web browsing history from their mobile devices, and production of all cookies stored on or deleted from plaintiffs' mobile devices.[55] Plaintiffs objected that Turn's requests were "overbroad, irrelevant, and invasive of their privacy interests" and "fl[ew] in the face of Rule 26(b)'s relevancy and proportionality requirements."[56] In ruling on the requests, Judge Beeler unambiguously held that privacy was a valid proportionality consideration:

> While questions of proportionality often arise in the context of disputes about the expense of discovery, proportionality is not limited to such financial considerations. Courts and commentators have recognized that privacy interests can be a consideration in evaluating proportionality, particularly in the context of a request to inspect personal electronic devices.[57]

Judge Beeler collected numerous cases to support this proposition, mostly regarding requests either for inspection or for forensic images of computers or mobile devices, wherein the courts had found that such requests were disproportionate to the needs of the case.[58]

One such case involved an order from Magistrate Judge Nathanael M. Cousins of the Northern District of California in *In re: Anthem, Inc. Data Breach Litigation*, another data-privacy class

---

55. *Id.*

56. *Id.* at *4.

57. *Id.* at *5 (citing Tingle v. Hebert, No. 15-626-JWD-EWD, 2018 WL 1726667, at *7–8 (M.D. La. Apr. 10, 2018); Areizaga v. ADW Corp., No. 3:14-cv-2899-B, 2016 WL 9526396, at *3 (N.D. Tex. Aug. 1, 2016); Johnson v. Nyack Hosp., 169 F.R.D. 550, 562 (S.D.N.Y. 1996)).

58. *Henson*, 2018 WL 5281629, at *5.

action wherein the defendant had requested either access to or forensic images of plaintiff's devices—namely "computer systems that connect to the internet."[59] The defendant argued that its request was necessary in order to analyze whether the devices contained malware or other electronic markers establishing that the plaintiffs' personal information had been compromised prior to the cyberattack in question.[60] Plaintiffs, on the other hand, objected that the discovery was "highly invasive, intrusive, and burdensome." In denying defendant's request, Magistrate Judge Cousins applied the last Rule 26(b)(1) proportionality factor, finding that "the burden of providing access to each plaintiff's computer system greatly outweighs its likely benefit" and noting the "Orwellian irony" that would have resulted from a contrary ruling requiring "that in order to get relief for a theft of one's personal information, a person has to disclose even more personal information."[61] As Judge Cousins reminded the parties, "under the revised discovery rules, not all relevant information must be discovered."[62]

---

59. Order Denying Anthem's Request to Compel Discover of Plaintiff's Computer Systems, *In re* Anthem, Inc. Data Breach Litig., No. 15-md-02617 LHK (NC), 2016 WL 11505231, at *1 (N.D. Cal. Apr. 8, 2016).

60. *Henson*, 2018 WL 5281629, at *5.

61. *In re Anthem*, 2016 WL 1150523, at *1; *cf.* Miller, *supra* note 9, at 465 ("A legal system that does not recognize the right to keep private matters private raises images of an Orwellian society in which Big Brother knows all.").

62. *In re Anthem*, 2016 WL 1150523; *see also* Prado v. Equifax Info. Servs. LLC, No. 18-cv-02405-PJH (LB), 2019 WL 1305790, at *3 (N.D. Cal. Mar. 22, 2019); T.C *ex. rel.* of S.C. v. Metro. Gov't of Nashville & Davidson Cty., Tenn., No. 3:17-CV-01098, 2018 WL 3348728, at *14 (M.D. Tenn. July 9, 2018) ("[T]he party seeking to discover those thoughts and feelings via social media must still make a showing of relevance and proportionality to the claims of the litigation."); Hespe v. City of Chicago, No. 13 C 7998, 2016 WL 7240754, at *3 (N.D. Ill. Dec. 15, 2016) ("[I]nspection of plaintiff's electronic devices is not proportional to the needs of this case because any benefit the inspection might provide is outweighed by plaintiff's privacy and confidentiality

In addition to these decisions, several other recent cases have denied motions to compel because of privacy concerns but without explicitly framing the question within the proportionality framework provided by Rule 26(b). For example, in *Locke v. Swift Transportation Co. of Arizona, LLC*, a district court denied a motion to compel production of the entirety of the plaintiffs' social media accounts: "that some of a party's social media information is discoverable does not make the entirety of a party's social media information available for inspection [as this would] ''sanction an[] inquiry into scores of quasi-personal information that would be irrelevant and non-discoverable."[63]

Finally—and quite recently—the recently published *Sedona Conference Primer on Social Media, Second Edition* likewise takes the view that "[t]he proportionality limitation on the scope of

interests.") (internal quotation marks omitted); *Areizaga*, 2016 WL 9526396, at *3 (N.D. Tex. Aug. 1, 2016) ("[T]he Court finds that, on this record, ADW's request to obtain a forensic image of Plaintiff's personal electronic devices is too attenuated and is not proportional to the needs of the case at this time, when weighing ADW's explanation and showing as to the information that it believes might be obtainable and might be relevant against the significant privacy and confidentiality concerns implicated by ADW's request—even with ADW's offer to pay all expenses and to use a third-party vendor who will restrict ADW's access to the substantive information of any user-created files and particularly data that appears to be of a personal nature that may be included in the proposed forensic image."); Rodriguez Ayala v. Cty. of Riverside, No. EDCV 16-686-DOC (KKx), 2017 WL 2974919, at *4 (C.D. Cal. July 12, 2017) ("Here, in light of the limited relevance of the information balanced against the burden of production on the privacy rights of non-parties, the Court finds the discovery sought does not meet the proportionality requirement of Rule 26."); Crabtree v. Angie's List, Inc., No. 1:16-cv-00877-SEB-MJD, 2017 WL 413242, at*3 (S.D. Ind. Jan. 31, 2017) ("[T]he Court finds that the forensic examination of Plaintiffs' electronic devices is not proportional to the needs of the case because any benefit the data might provide is outweighed by Plaintiffs' significant privacy and confidentiality interests.").

63. No. 5:18-CV-00119-TBR-LLK, 2019 WL 430930, at *3 (W.D. Ky. Feb. 4, 2019).

discovery includes two factors that implicate privacy concerns, i.e., ''the importance of the discovery in resolving the issues, and whether the burden . . . of the proposed discovery outweighs its likely benefit."[64] Although the Primer cautions that privacy is not a per se bar to discovery as in the case of legal privileges, it nevertheless states that parties "consider managing the discovery to minimize potential embarrassment to third parties and protect against unnecessary disclosure of their sensitive personal information."[65]

THE IMPLICATIONS OF PRIVACY BEING AN ASPECT OF PROPORTIONALITY

Including privacy as part of the proportionality analysis has important implications for courts and litigants alike. As the Rules make clear, achieving proportionality is the responsibility of all parties: "the parties and the court have a collective responsibility to consider the proportionality of all discovery and consider it in resolving discovery disputes."[66] Nor is the proportionality inquiry relevant *only* at the time when documents are finally handed over to the opposing party. As the advisory committee note to the 2015 amendment of Rule 37(e) explains, proportionality considerations are relevant as early as the preservation stage and will be considered a "factor in evaluating the reasonableness of preservation efforts."[67] Indeed, Comment 2.b of *The Sedona Principles, Third Edition* states that "[p]roportionality should be considered and applied by the court and parties to all aspects of the discovery and production of ESI including: preservation; searches for likely relevant ESI; reviews for

64. The Sedona Conference, *Primer on Social Media, Second Edition*, 20 SEDONA CONF. J. 1, 27–28 (2019).

65. *Id.*

66. FED. R. CIV. P. 26 advisory committee's note to 2015 amendment.

67. FED. R. CIV. P. 37(e) advisory committee's note to 2015 amendment.

relevancy, privilege, and confidentiality; preparation of privilege logs; the staging, form(s), and scheduling of production; and data delivery specifications."[68] Privacy considerations, therefore, are relevant from the outset—even when initially identify-ing the custodians, data sources, and time period likely to contain relevant information.[69]

A. Preservation

Our experience has shown that in a document review of any scale—especially if emails or other communications are involved—private personal information inevitably will be preserved and later swept up during the collection process. This includes not only personally identifiable information such as social security numbers and credit card information, but also more intimate and potentially embarrassing details, including everything from vacation photos to medical records. The more custodians, the broader the time period, and the more personal the data sources—especially chat systems, social media, and mobile devices—the more personal information will be potentially implicated downstream as a consequence. Moreover, such communications will very often involve numerous third parties, potentially implicating their privacy interests as well under both the Federal Rules and newer regulatory regimes such as GDPR and the CCPA.

Thus, while many preservation steps can seem like passive exercises, the impact on privacy can nevertheless be significant. Suspending the periodic deletion of emails under a corporate party's records retention policy, instructing employees in a legal hold not to delete text messages, and retaining the laptop of a

68. *The Sedona Principles, Third Edition*, *supra* note 39, at 67.

69. *See* Boliek, *supra* note 35, at 1134 ("A means to assure protection [of privacy] is to consider and weigh the affected parties' privacy interest at every step of the discovery process.").

departing employee (rather than repurposing it) all typically result in an increase in the volume of private personal information and, therefore, the potential exposure of private information in the event of an inadvertent release or data breach. Reducing such exposure is one of the primary reasons that companies implement such programs as part of their information governance programs. To achieve proportionality, therefore, a producing party may appropriately consider not only what is likely to be relevant but also what is likely to implicate privacy interests. Privacy interests therefore may serve as appropriate factors to reasonably limit the scope of preservation in many cases. For example, a party employee's personal email account—even if used on rare occasion for business purposes—might therefore lie outside of the appropriate scope of discovery.

B. Collection

At the collection and processing phases, privacy concerns are truly amplified. Data is copied from its source location and transferred to other systems for processing. Processed copies of the data are then loaded into still other systems, such as Early Case Assessment tools, for further analysis prior to review. Along the way, it is common for the data to pass through many hands. A typical collection workflow may involve the party's own Information Technology (IT) personnel, a dedicated eDiscovery collection vendor, and a separate eDiscovery review vendor, all overseen by inside and outside counsel. At the end of collections, there may be multiple copies of the data in both "raw" and processed forms stored in multiple locations, including intermediate locations such as removable media, file shares, and "staging" locations. As the Sixth Circuit has noted, "[d]uplication, by its very nature, increases the risk of improper

exposure, whether purposeful or inadvertent."[70] And "ESI productions in civil litigations can be ripe targets for corporate espionage and data breach as they may contain trade secrets and other proprietary business information; highly sensitive and private medical, health, financial, religious, sexual preference, and other personal information; or information about third parties subject to contractual confidentiality agreements."[71]

Those charged with identifying and collecting relevant data may therefore appropriately determine what data sources are likely to contain sensitive information *prior* to collection. Among other things, well-designed custodian interviews and close cooperation with internal IT personnel can help determine the likely relevance of a data source as well as the kind of sensitive information that might be contained in it. This information will allow counsel to make an informed choice about whether privacy interests should limit the scope of what is collected and, if so, in what matter.

Minimizing the privacy burdens when collecting from mobile devices is especially challenging.[72] For example, if a corporate party allows its employees to use their personal phones for business purposes, as is now common with bring-your-own-device (BYOD) programs, it can be difficult to disentangle business from personal data given the current state of mobile device collection technology, which often requires "imaging" the entire contents of the device. This is especially true where an employee has used text messaging or other personal communications apps for substantive business purposes. In such situations, if an employee's use for business purposes has been limited—as is

70. John B. v. Goetz, 531 F.3d 448, 457 (6th Cir. 2008).

71. *The Sedona Principles, Third Edition*, *supra* note 39, at 179 n.147.

72. *See generally* Robert D. Keeling, *The Challenge of Collecting Data from Mobile Devices in eDiscovery*, 18 SEDONA CONF. J. 177 (2017).

often the case—it may be more proportional to not collect the device at all. Or, at most, to assist the employee with running a limited number of searches and "screenshotting" any relevant messages, rather than capturing a forensic image of the entire device. Although this approach would not capture potentially relevant metadata, the relative importance of that metadata must be weighed against the potential privacy harm resulting from a forensic collection.

Personal messaging apps also present particular challenges when used for business purposes. Increasingly often, these tools include a number of privacy-oriented features such as encrypted and self-destructing messages. While these important features help to protect user privacy, they can result in communications being beyond an organization's reach if its employees use these apps for their work. Organizations may therefore wish to consider adopting a policy requiring employees to use a dedicated enterprise application with a limited retention period for business messaging. Although these "ephemeral" messaging applications have been scrutinized by some in the wake of the *Waymo, LLC v. Uber Technologies, Inc*. matter, not every use of such technology should arouse suspicion.[73] As stated in the recent public comment version of *The Sedona Conference Commentary on Legal Holds, Second Edition: The Trigger & The Process*: "Transient or ephemeral data not kept in the ordinary course of business (and that the organization may have no means of preserving) may not need to be preserved."[74] Moreover, certain enterprise editions of these tools allow parties to set a definite retention period (e.g., none, 3 days, 6 days, 15 days, 20 days), facilitate search and collection, and encourage separation of

73. No. C 17-00939, 2018 WL 646701 (N.D. Cal. Jan. 30, 2018).

74. The Sedona Conference, *Commentary on Legal Holds, Second Edition: The Trigger & The Process*, 20 SEDONA CONF. J. 341, 395 (2019).

business and personal communications. Their use should not be discouraged.

C. Review

At the review stage, the privacy implications are second perhaps only to those of production. In large reviews, dozens or even hundreds of lawyers, including contract lawyers retained solely for the purpose of review, will read and classify the collected materials. This disclosure is itself burdensome. Sharing sensitive information—especially regarding intimate personal, medical, religious, or financial matters—to a large group of people is a substantial burden, even if that information goes not further.

The use of Technology Assisted Review (TAR) can greatly mitigate the potential privacy burdens at the review stage, however. In the majority of matters, the most personal and embarrassing documents are often among the least likely to be relevant. Culling the document population based on likely relevance (as determined by a well-trained TAR model) will significantly reduce the need for any human to lay eyes on irrelevant documents containing private information. In addition, a number of search, analytics, and machine-learning approaches can help identify documents that are likely to implicate privacy concerns.

D. Production

In any large review, however, some not insignificant number of private information will nevertheless be subject to eyes-on review. For those documents that are irrelevant, the reviewers' task is typically to make sure that they are not inadvertently

produced.[75] A determination that a document is relevant, however, is not the end of the inquiry, as the Rules provide parties and courts with great flexibility to ensure that privacy concerns are respected.

One way this can be accomplished is through the use of Rule 26(c) protective orders. Often, parties agree to enter blanket protective orders that govern how confidential documents may be used by the receiving party.[76] However, even a carefully drafted protective order is sometimes insufficient. For one thing, there is no guarantee that it will be granted. Legal process in the U.S. tilts strongly toward public disclosure, and courts have on occasion rejected agreed-upon disclosure limitations because they gave "each party carte blanche to decide what portions of the record shall be kept secret."[77]

This aside, once a document is provided to another party, the producing party's control over that information is dramatically limited and the risk of disclosure heightened.[78] "[P]rotective

75. This can be easier said than done, especially in large reviews, which further bolsters the case for culling at the preservation, collection, and processing stages.

76. In recent years, privacy-conscious parties have negotiated consensual protective orders that not only limit how confidential information may be used, but also how produced information may be stored and transmitted. *See, e.g.*, *In re* Takata Airbag Prods. Liab. Litig., 1:15-cv-02599 (S.D. Fla. Aug. 28, 2015); *In re* Wells Fargo Collateral Protection Ins. Litig., 8:17-ml-02797 (C.D. Cal. Jan. 9, 2018). Often parties also negotiate procedures for the eventual deletion of many produced documents once the matter has been resolved.

77. Citizens First Nat. Bank of Princeton v. Cincinnati Ins. Co., 178 F.3d 943, 945 (7th Cir. 1999) (Posner, J.); *cf.* Miller, *supra* note 9, at 431–32 (opposing this trend).

78. *Cf.* John B. v. Goetz, 531 F.3d 448, 458 (6th Cir. 2008) ("[T]he imaging of these computers and devices will result in the duplication of confidential and private information unrelated to the [underlying] litigation. This

orders are effective only when the signatories comply with their parameters, and even then information can be misplaced or disclosed inadvertently."[79] This danger is particularly acute when the information produced has value outside of the litigation. Data breaches and leaks can irrevocably expose sensitive information to the public. This danger was realized in dramatic fashion in the *Zyprexa* litigation, in which a plaintiffs' expert, a lawyer not directly involved in the litigation, and a New York Times reporter subpoenaed millions of documents that were sealed under a protective order under false pretenses and then disclosed many of those documents to the public.[80] Further, even if information is not disclosed improperly, disclosing private information to a litigation opponent can itself pose a substantial burden on privacy interests.

Such concerns in our view should encourage parties to properly consider privacy concerns in evaluating individual documents. Consider, for example, a large spreadsheet file containing several dozen worksheets, each with thousands of lines, many of which contain extensive personal customer information that is of no relevance to the case. If one of the entries is technically relevant to a party's request, but it is not of significant "importance . . . in resolving the issues" in the case, must the entire file therefore be produced? We believe that a party acting in good faith can reasonably conclude that it need not, as it is not "proportional to the needs of the case" and is therefore not

duplication implicates significant privacy and confidentiality interests—regardless of whether the imaged media are initially held under seal—and these interests cannot be fully protected *ex post*.").

79. Boliek, *supra* note 35, at 1132.

80. *See id.*; William G. Childs, *When the Bell Can't Be Unrung: Document Leaks and Protective Orders in Mass Tort Litigation*, 27 REV. LITIG. 565, 578–97 (2008) (recounting the saga of the Zyprexa leak).

within the scope of discovery.[81] That it has already been collected and reviewed—and that the majority of the monetary costs of discovery associated with this document have therefore already been incurred—does not change this. The burden of privacy is distinct and independent from the expense of litigation,[82] and the risks to privacy are felt primarily after, rather than before, production.

If so, the question then arises: must the party seek judicial relief before doing so or disclose the judgment to the opposing party? We are inclined to think not. While the temptation to use privacy as a stalking horse to gain an unfair litigation advantage is real, it is not unique. For better or worse, the same danger is present whenever a party makes relevance determinations, which are not logged or otherwise disclosed. And unlike documents withheld on the basis of the attorney-client privilege—which are often highly relevant—the good-faith determination discussed here is that the burden of privacy outweighs the value in the production of a marginally relevant document.[83] This kind of calculus is codified in Rule 26(b) and reflects the kind of common sense decision-making that parties have routinely made, both before and after the 2015 amendments.[84] When a

81. FED. R. CIV. P. 26(b)(1).

82. *See* McPeak, *supra* note 46, at 291 ("Nonpecuniary burdens are a necessary consideration as a limit to civil discovery and an important aspect of the proportionality analysis.").

83. So-called "privacy logs," are unnecessary and would amount to a *de facto* amendment to Rule 26(b)(1). They may, however, be useful in instances where there are other legal protections of privacy in play. *See In re* Xarelto (Rivaroxaban) Prods. Liab. Litig., MDL NO. 2592, 2016 WL 2855221, at *5 (E.D. La. May 16, 2016); Kristen A. Knapp, *Enforcement of U.S. Electronic Discovery Law Against Foreign Companies: Should U.S. Courts Give Effect to the EU Data Protection Directive?*, 10 RICH. J. GLOBAL L. & BUS. 111, 127 (2010).

84. *Cf. In re* Convergent Techs. Sec. Litig., 108 F.R.D. 328, 331 (N.D. Cal. 1985) (Under the 1983 amendments, "counsel . . . *must* make a common sense

document (or set of documents) is both of significant relevance and poses a significant burden on privacy, however, a party should identify the right balance to strike—whether through redactions, a protective order, or some other mechanism. As with most other discovery matters, a little common sense and reflection usually allow a party acting in good faith to reach a reasonable and defensible conclusion.

Finally, the burden of protecting appropriate privacy interests during litigation counsels in favor of cost shifting in many cases. If a requesting party has served document requests that will require significant work to protect legitimate privacy interests in the course of responding to those requests, the producing party often will be justified in seeking the producing party to share some or all of that burden. The burdensome and expensive costs of privacy redactions, for example, often constitutes a prime opportunity for cost shifting. This will further have the effect of encouraging cooperation between the parties on limiting the scope of production of minimally relevant documents that entail expensive privacy review in order to produce.

CONCLUSION

There is an emerging consensus that privacy burdens may properly be considered as part of the proportionality analysis required by revised Rule 26(b)(1) to determine the scope of discovery. Those burdens grow heavier as discovery progresses

---

determination, taking into account all the circumstances, that the information sought is of sufficient potential significance to justify the burden the discovery probe would impose, that the discovery tool selected is the most efficacious of the means that might be used to acquire the desired information (taking into account cost effectiveness and the nature of the information being sought), and that the timing of the probe is sensible, i.e., that there is no other juncture in the pretrial period when there would be a clearly happier balance between the benefit derived from and the burdens imposed by the particular discovery effort.").

from identification through review and onto production, yet early decisions at the identification and preservation stage regarding the scope of discovery may have significant and widespread downstream privacy consequences. From the earliest stages of discovery, therefore, a producing party and its counsel may appropriately consider not only what is likely to be relevant but also what is likely to be private and unlikely to be relevant—i.e., to give careful attention to potential situations where "the burden or expense of the proposed discovery outweighs its likely benefit" and may therefore be beyond the scope of discovery. To the extent private information nevertheless is included in the collection, producing parties and their counsel may take reasonable steps at each phase of discovery, including making use of available technology, to reduce potential privacy burdens.

Moving the Law Forward in a Reasoned & Just Way