

# *The Sedona Conference Primer on Social Media, Second Edition*

*The Sedona Conference*



# 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	Julie Lewis
Michelle Greer Galloway	Lauren Schwartzreich
Alan C. Geolot	Amy E. Sellars
<i>WG1 Steering</i>	<i>Drafting Team Leaders</i>
<i>Committee Liaisons:</i>	<i>and Editors-in-Chief:</i>
Gareth Evans	Alitia Faccone
Annika K. Martin	Philip Favro
Ronni D. Solomon	

*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

---

Copyright 2019, The Sedona Conference.  
All Rights Reserved.

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.....	8
II.	SOCIAL MEDIA AND EMERGING TECHNOLOGIES.....	10
	A. Platforms and Other Traditional Forms of Social Media.....	11
	B. Messaging Applications .....	12
	1. “Over-The-Top” Messaging Applications .....	13
	2. Anonymous Chat and Messaging Applications.....	14
	3. Ephemeral Messaging Applications .....	15
	4. Cloud-Based Messaging and Collaboration Applications for the Workplace.....	15
	5. Discovery Challenges with Messaging Applications.....	16
	C. Live-Streaming Video .....	17
	D. Location-Based Social Intelligence Platforms .....	17
	E. Devices Using Social Media Applications .....	18
III.	THRESHOLD DISCOVERY ISSUES.....	21
	A. Relevance and Proportionality .....	22
	1. Privacy Considerations .....	27
	2. Requesting Social Media Evidence.....	30
	B. Possession, Custody, and Control .....	33
	1. “Control” By Individual Parties .....	34
	2. “Control” by Organizational Parties.....	37
	3. “Control” by Third Parties .....	39
	C. Preservation, Collection, and Search Obligations Generally.....	39
	1. Considerations for Preserving and Collecting Social Media.....	39

2. The Role of Cooperation .....	42
3. The Interplay Between Reasonable Steps and Social Media .....	43
4. Means of Preservation and Collection of Social Media .....	44
a. Static Images .....	45
b. Self-Collection Based on Social Media Processes.....	46
c. Use of an Application Programming Interface Offered by the Social Media Provider .....	48
d. Native or Near-Native File of the Web Content .....	50
e. Other Vendor Services, Including Dynamic Capture .....	51
D. Preservation and Collection Guidance in Light of the Stored Communications Act .....	52
1. Restrictions on Electronic Communication Service Providers.....	53
2. Restrictions on Remote Computing Service Providers .....	53
3. Determining the Type of Service Involved .....	54
4. Protections Limited to Contents of Communications .....	55
5. Public vs. Private Issues .....	56
6. Enforcement of the Prohibition Against Divulging Communications .....	57
7. The Prohibition Against Access by Unauthorized Persons.....	58
8. Seeking to Obtain Information Without Violating the SCA .....	58

E.	Review and Production.....	61
1.	Review .....	61
a.	Small Data Volumes .....	62
b.	Large Data Volumes .....	63
2.	Production.....	65
IV.	CROSS BORDER DISCOVERY ISSUES .....	68
A.	Europe.....	68
B.	Asia.....	75
V.	AUTHENTICATION OF SOCIAL MEDIA EVIDENCE.....	77
A.	General Authentication Requirements.....	77
B.	Self-Authentication .....	79
C.	Judicial Interpretations .....	81
VI.	ETHICAL ISSUES RELATED TO SOCIAL MEDIA AS POTENTIAL EVIDENCE .....	87
A.	Attorney Duty of Competence .....	87
B.	Attorney Advice Related to Client Use of Social Media.....	87
1.	Advising Clients on Social Media Preservation ...	88
2.	Attorney Use of Social Media for Discovery.....	91
VII.	CONCLUSION .....	93



## 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*.<sup>1</sup> 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.*”<sup>2</sup> 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.<sup>3</sup>

#### 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.<sup>4</sup> 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.<sup>5</sup>

---

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.<sup>6</sup>

#### *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.<sup>7</sup> 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.<sup>8</sup> 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.<sup>9</sup>

---

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](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.<sup>10</sup>

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.<sup>11</sup>

### 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.<sup>12</sup> 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.<sup>13</sup> 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.<sup>14</sup> 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,<sup>15</sup> 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.<sup>16</sup> 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.<sup>17</sup> 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.”<sup>18</sup>

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.<sup>19</sup>

### 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.<sup>20</sup> To date, law enforcement and news reporters are the most prevalent users. Examples of companies developing and distributing the technology include DigitalStakeout, Echosec, Snaprends, 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”).<sup>21</sup> 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.<sup>22</sup>

#### *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](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.<sup>23</sup> 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).<sup>24</sup> 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.<sup>25</sup> 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.<sup>26</sup> 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-heat-map.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.<sup>27</sup>

---

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](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.<sup>28</sup> 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.<sup>29</sup>

#### *A. Relevance and Proportionality*

The scope of discovery for social media content is no different from other categories of information.<sup>30</sup> 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](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. Lopiccio*, 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."<sup>31</sup>

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.<sup>32</sup> 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.<sup>33</sup>

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.<sup>34</sup> As with discovery of other ESI, a party is generally not entitled to inspect or obtain all data from a particular source.<sup>35</sup> 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.<sup>36</sup> 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.<sup>37</sup>

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.<sup>38</sup> 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.”<sup>39</sup>

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.<sup>40</sup> 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.<sup>41</sup> 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.<sup>42</sup> It also teaches that counsel must be competent (or partner with a competent lawyer) to facilitate appropriate discovery of this information.<sup>43</sup>

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.<sup>44</sup>

### 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.’”<sup>45</sup> 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.”<sup>46</sup>

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.<sup>47</sup> 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.<sup>48</sup>

---

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,<sup>49</sup> they should consider managing the discovery to minimize potential embarrassment to third parties and protect against unnecessary disclosure of their sensitive personal information.<sup>50</sup> 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.<sup>51</sup>

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.<sup>52</sup> 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.<sup>53</sup>

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.<sup>54</sup> Such information has been found to be relevant in employment discrimination, personal injury, and workers compensation cases.<sup>55</sup>

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.<sup>56</sup> 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.<sup>57</sup> 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.<sup>58</sup> 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.<sup>59</sup>

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."<sup>60</sup>

---

57. *Id.* at \*2.

58. *Id.*

59. *Id.* at \*1.

60. *Id.* at \*2.

*B. Possession, Custody, and Control*<sup>61</sup>

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.<sup>62</sup> 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.<sup>63</sup> 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.<sup>64</sup>

---

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, Eighth, 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.<sup>65</sup> 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.<sup>66</sup> 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,<sup>67</sup> or as a “customer” or “subscriber” of the account pursuant to the SCA.<sup>68</sup>

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.<sup>69</sup>

## 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.<sup>70</sup>

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.<sup>71</sup>

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.”<sup>72</sup> It does not appear that courts have held that employers have the “practical ability” to obtain their employees’ social media information.<sup>73</sup> 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.<sup>74</sup>

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. *Supra* 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.<sup>75</sup> 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.<sup>76</sup> 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.<sup>77</sup>

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.<sup>78</sup> 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.<sup>79</sup>

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.<sup>80</sup> 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.<sup>81</sup>

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.<sup>82</sup>

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.<sup>83</sup>

## 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.<sup>84</sup> 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.<sup>85</sup> 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 Edition*, *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).<sup>86</sup>

### 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.<sup>87</sup>

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.<sup>88</sup>

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.<sup>89</sup>

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.<sup>90</sup> 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.<sup>91</sup> Social media may also contain data and content, such as video, that cannot be properly collected in the form of static images.<sup>92</sup> 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.<sup>93</sup> 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.<sup>94</sup>

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.<sup>95</sup>

#### 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).<sup>96</sup> 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.<sup>97</sup> 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.<sup>98</sup>

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](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.<sup>99</sup>

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.<sup>100</sup>

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.<sup>101</sup> Among messaging applications, Slack also has an API that may allow access to vendors.<sup>102</sup>

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.<sup>103</sup>

---

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/](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.<sup>104</sup>

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.<sup>105</sup> 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.<sup>106</sup>

---

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.<sup>107</sup>

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*<sup>TM</sup>, 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.<sup>108</sup> 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.<sup>109</sup> 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.”<sup>110</sup> 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.”<sup>111</sup>

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.”<sup>112</sup>

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.<sup>113</sup> Moreover, an entity may qualify as providing both types of service, even for a single type of communication.<sup>114</sup>

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.<sup>115</sup>

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.<sup>116</sup> 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.<sup>117</sup> 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.<sup>118</sup>

#### 4. Protections Limited to Contents of Communications

The SCA prohibits disclosure of the "contents of communications," such as the substance of the message conveyed.<sup>119</sup> 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.<sup>120</sup> 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.<sup>121</sup>

### 5. Public vs. Private Issues

The prohibitions in the SCA apply only to those that provide services to the public.<sup>122</sup> Additionally, SCA protections apply only to private communications and not those readily accessible to the public.<sup>123</sup> 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.<sup>124</sup> 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.<sup>125</sup>

#### 6. Enforcement of the Prohibition Against Divulging Communications

There are some exceptions that allow service providers to disclose communications,<sup>126</sup> but no exception exists under the SCA for civil subpoenas.<sup>127</sup> The SCA provides a civil cause of action against service providers that violate the Act.<sup>128</sup> The aggrieved party may sue for both equitable relief and damages.<sup>129</sup> 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.<sup>130</sup>

#### 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.<sup>131</sup> This prohibition applies to attorneys who, through improper means, gain access to protected content.<sup>132</sup>

#### 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.<sup>133</sup> 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.<sup>134</sup>

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.<sup>135</sup>
- 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.<sup>136</sup>

---

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.<sup>137</sup> 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.<sup>138</sup>

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.<sup>139</sup> 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.<sup>140</sup> 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.’”<sup>141</sup> 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.<sup>142</sup>

### *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.<sup>143</sup>

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.<sup>144</sup> 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.<sup>145</sup>

Parties might alternatively consider obtaining archival downloads of user information from social media sites,<sup>146</sup> 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.<sup>147</sup> Information may also be difficult to review.<sup>148</sup> 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.<sup>149</sup>

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.<sup>150</sup> 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.<sup>151</sup> 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.<sup>152</sup>

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.<sup>153</sup> 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.<sup>154</sup>

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.<sup>155</sup> The vendor then ran search terms agreed to by the parties and provided only responsive material to the plaintiff.<sup>156</sup>

---

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.<sup>157</sup> In contrast, personal data may be protected more broadly by treaty<sup>158</sup> 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.”<sup>159</sup> 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\(01\)](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.<sup>160</sup> 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,<sup>161</sup> social security numbers,<sup>162</sup> and medical records.<sup>163</sup>

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.”<sup>164</sup> 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,”<sup>165</sup> 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.<sup>166</sup>

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.<sup>167</sup> 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<sup>168</sup> 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.<sup>169</sup>

Following *Aérospatiale*, however, courts have largely disfavored conducting discovery under the Hague Convention.<sup>170</sup> 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.<sup>171</sup> 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.<sup>172</sup>

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](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.<sup>173</sup> As a result, cross-border discovery requests for social media content may be rejected even if those requests are reasonable and proportional.<sup>174</sup>

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,<sup>175</sup> under one of several special circumstances, including if “the transfer is necessary for the establishment, exercise or defence of legal claims.”<sup>176</sup> 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 dubbio, pertanto . . . che la richiesta assolva una finalità puramente esplorativa, incompatibile con la lettera o 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](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.”<sup>177</sup> 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.<sup>178</sup> It was replaced by the “EU-U.S. Privacy Shield Framework” in 2016.<sup>179</sup> The Privacy Shield provides participating companies with a legal mechanism for the transfer of personal data from the EU to the United States.<sup>180</sup> 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, Maximilian 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](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.<sup>181</sup> 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.<sup>182</sup> 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](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.<sup>183</sup>

### 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.<sup>184</sup> 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.<sup>185</sup> It is similar to the EU-U.S. Privacy Shield.<sup>186</sup> 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*<sup>187</sup> 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)*<sup>188</sup> 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?<sup>189</sup> 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.”<sup>190</sup> 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.”<sup>191</sup> 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.<sup>192</sup>

---

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.”<sup>193</sup> Evidence “describing a process or system and showing that it produces an accurate result” can also be used to authenticate documents or ESI.<sup>194</sup> 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.<sup>195</sup> 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.<sup>196</sup>

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.”<sup>197</sup> The trial judge is ordinarily responsible for making preliminary determinations with respect to the admissibility of evidence, including whether the evidence is authentic.<sup>198</sup> 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.<sup>199</sup>

### *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.<sup>200</sup> Reasonable advance written notice and access to the certification and record must be given to the adverse party, who can then challenge its authenticity.<sup>201</sup>

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.<sup>202</sup> 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.<sup>203</sup> 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.”<sup>204</sup>

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.”<sup>205</sup> 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.”<sup>206</sup> 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.”<sup>207</sup>

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.<sup>208</sup>

### 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.<sup>209</sup> 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).<sup>210</sup> 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.<sup>211</sup>

These divergent approaches were at one time described as the “Maryland approach” and the “Texas approach,”<sup>212</sup> 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.<sup>213</sup> 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.<sup>214</sup>

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.”<sup>215</sup> This could include “direct testimony from a witness with personal knowledge, . . . comparison with other authenticated evidence, or . . . circumstantial evidence.”<sup>216</sup> 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.”<sup>217</sup>

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.”<sup>218</sup> 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.”<sup>219</sup> The court also stated that “the bar for authentication of evidence is not particularly high.”<sup>220</sup>

---

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. Clevestine*, 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.”<sup>221</sup> 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.”<sup>222</sup> 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.”<sup>223</sup>

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.<sup>224</sup>

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."<sup>225</sup> 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]."<sup>226</sup>

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.<sup>227</sup> 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,<sup>228</sup> requires that counsel must render competent representation by providing “the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.”<sup>229</sup> Legal knowledge and skill include keeping current with “the benefits and risks associated with relevant technology.”<sup>230</sup>

### 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.<sup>231</sup> 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.<sup>232</sup>

### 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.<sup>233</sup> 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."<sup>234</sup>

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.<sup>235</sup>

---

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 does not violate substantive law or the duty to preserve.<sup>236</sup>

Both the substantive legal consequences for a party and ethical consequences for the attorney are illustrated in *Lester v. Allied Concrete Company*.<sup>237</sup> *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.<sup>238</sup>

*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.<sup>239</sup> 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.<sup>240</sup>

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.<sup>241</sup> 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.<sup>242</sup> Rule 4.3 governs a lawyer's behavior in making contact with unrepresented persons.<sup>243</sup>

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).<sup>244</sup>

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)<sup>245</sup> and could also be grounds for discovery sanctions.<sup>246</sup>

---

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.