wgs

# The Sedona Conference

## *The Sedona Canada Commentary on Discovery of Social Media*

A Project of The Sedona Conference Working Group 7
(Sedona Canada)

June 2021
Public Comment Version
Submit comments by July 31, 2021,
to comments@sedonaconference.org

# Sedona Canada Commentary on Discovery of Social Media

*A Project of The Sedona Conference Working Group 7 (Sedona Canada)*

**JUNE 2021 PUBLIC COMMENT VERSION**

**Author:** The Sedona Conference

**Drafting Team Leaders and Editors-in-Chief**

Matthew Maslow Christopher Walker

**Drafting Team**

Lisa Alleyne Gretel Best
Pamela Drummond William Ellwood
Melissa Feriozzo Lauren Grimaldi
Kevin Lo David Outerbridge
Molly Reynolds Chuck Rothman
Nic Wall William Walters

**Judicial Participants**

Master Kaufman Justice Calum MacLeod

**Staff Editor:** David Lumia

REPRINT REQUESTS:

Requests for reprints or reprint information should be directed to The Sedona Conference at info@sedonaconference.org.



# Preface

Welcome to the public comment version of The Sedona Conference *Commentary on Discovery of Social Media in Canada ("Commentary),* a project of the Sedona Canada Working Group (WG7) of The Sedona Conference. The Sedona Conference is a research and educational institute that exists to allow leading jurists, lawyers, experts, academics, and others to come together in conferences and mini-think tanks called Working Groups to engage in true dialogue, not debate, in an effort to move the law forward in a reasoned and just way.

I thank all of the drafting team members for their dedication and contribution to this project.

This *Commentary* builds on similar principles and guidelines regarding social media, including *The Sedona Conference Primer on Social Media,* developed by the Sedona Conference in 2017 (and updated in 2019). However, the *Commentary* focuses on the regulatory and practice requirements of the Canadian legal profession.

We hope our efforts will be of immediate and practical assistance to legal service providers, related third-party service providers, and their clients. Please note that this version of the *Commentary* is open for public comment, and suggestions for improvement are welcome. Please submit comments by July 31, 2021 to comments@sedonaconference.org. 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.

Craig Weinlein
Executive Director
The Sedona Conference
June 2021

# Table of Contents

# I. THE PERSISTENCE OF SOCIAL MEDIA

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 legal proceedings 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.

Specifically, a party must consider whether social media content and documents are relevant and should be preserved and listed in an affidavit or list of documents or records.[1] A court may order private portions of a party's social media profiles and pages to be disclosed where the information is relevant and the probative value of the information justifies the invasion of privacy and the burden of production.[2] The mere fact, however, that a party has a social media presence does not presumptively mean that the private aspects of an account are relevant.[3] Rather, relevance must be shown. For example, in *Bishop v. Minichiello*, the defendants sought production of the plaintiff's hard drive to determine the amount of time the plaintiff spent on Facebook.[4] The plaintiff's computer was used by all members of his family. To protect the privacy rights of non-party family members, the Ontario Court ordered the parties to agree on the use of an independent expert to review the hard drive.

In *Fric v. Gershman*,[5] the Supreme Court of British Columbia similarly sought to protect the privacy of third parties when it ordered production of certain photographs posted on the plaintiff's Facebook page. The plaintiff was permitted to edit the photographs prior to disclosure to protect the privacy of other individuals who appeared in them. The Court in *Fric* refused to order production of commentary from the Facebook site, however, holding that if such commentary existed, the probative value of the information was outweighed by the competing interest of protecting the private thoughts of the plaintiff and third parties.[6] Although the presence of relevant information on the

---

1 See *Toth v City of Niagara Falls*, 2017 ONSC 5670 (CanLII), where the Court found that counsel for the plaintiff, should have considered the existence of social media content in a public forum (i.e., Facebook).

2 See *Leduc v. Roman*, 2009 CanLII 6838 (ON SC) [*Leduc*]; *Frangione v. Vandongen*, 2010 ONSC 2823 (CanLII) [*Frangione*]; *Murphy v. Perger*, [2007] OJ No 5511 (WL Can) [*Murphy*], *McDonnell v. Levie*, 2011 ONSC 7151 (CanLII) [*McDonnell*], and *Casco v. Greenhalgh*, 2014 CarswellOnt 2543 (Master) [*Casco*]; *Papamichalopoulos v Greenwood*, 2018 ONSC 2743 and *Wilder v Munro*, 2015 BCSC 183.

3 *Schuster v Royal & Sun Alliance Insurance Company of Canada*, [2009] OJ No 4518 (WL) (ON SC), and see *Stewart v. Kemptster*, 2012 ONSC 7236 (CanLII), *Garacci v. Ross*, 2013 ONSC 5627 (CanLII), and *Conrod v. Caverley*, 2014 NSSC 35 (CanLII).

4 2009 BCSC 358 (CanLII), leave to appeal for further production dismissed, 2009 BCCA 555 (CanLII).

5 *Fric v. Gershman*, 2012 BCSC 614 (CanLII).

6 *Ibid.* at para 75, citing *Dosanjh v. Leblanc and St. Paul's Hospital*, 2011 BCSC 1660.

public portion of a party's social media page may support the inference that relevant information is also contained in the party's private profile, courts have held that in some circumstances, users have a privacy interest in the information that they have chosen not to share publicly.[7]

Even where individuals seek to operate under the privacy that may be afforded by the anonymity of social media profiles, there will be instances where the court determines that the public interest and fairness override an individual's expectation of anonymity and privacy. In *Olsen v. Facebook,*[8] the Court held that anonymous posters should not be permitted to defame without consequences. However, individuals who comment on matters of public interest should not have their anonymity stripped away because they are critical of public figures. Ultimately, the Court found the nature and number of postings by the Facebook accounts overrode a reasonable expectation that account owners were entitled to anonymity, and the Court ordered Facebook to release to the applicants the preserved Facebook information.

Section II of the *Commentary on Discovery of Social Media in Canada* 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, 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 *Commentary on Discovery of Social Media in Canada* concludes in Section VI by analyzing ethical issues that lawyers should consider in connection with social media discovery.

---

7 *Jones v IF Propco*, 2018 ONSC 23.

8 *Olsen v. Facebook*, 2016 NSSC 155.

## 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 platform 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, 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.*"[9] 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 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 *Commentary on Discovery of Social Media in Canada* focuses on the different kinds of social media that exist 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.[10]

### 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 platforms share many similar features. They allow users to post content to bulletin board-type locations. Privacy settings, when

---

[9] *Concise Oxford English Dictionary,* 12th ed., *sub verbo* "social media."

[10] Social media data analytics platforms and content distribution portals for posting on social media sites are outside the scope of the *Commentary on Discovery of Social Media in Canada.*

enabled, permit users some control over the initial distribution of their content.[11] 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.

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; and issues surrounding possession, custody, and control.[12]

### B. Messaging Applications

Reports indicate that users of messaging applications now outnumber users of social media platforms.[13] The advent of more advanced mobile device technology and consumer preference are primarily responsible for this phenomenon.

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

---

[11] See *Frangione v. Vandongen*, 2010 ONSC 2823 (Ont. Sup. Ct. J.) (discussing the impact of privacy settings restricting access to social media on a production order).

[12] See Section III, *infra*.

[13] See *Messaging Apps Are Now Bigger Than Social Networks* (20 September 2016), online: Bus. Insider Intelligence <http://uk.businessinsider.com/the-messaging-app-report-2015-11?r=US&IR=T>.

not pass through the message servers belonging to SMS providers (telecommunications companies such as Bell or Rogers), private enterprises, or governmental entities.

OTT messaging applications generally offer users enhanced functionality at a lower cost than providers of traditional text messaging services.[14] 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.[15]

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, and Facebook Messenger.

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.[16]

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

---

[14] See Janet Balis, *What an OTT Future Means for Brands* (13 May 2015), online: Harv. Bus. Rev., online: <https://hbr.org/2015/05/what-an-ott-future-means-for-brands>.

[15] See James Chavin, Aadil Ginwala & Max Spear, *The future of mobile messaging: Over-the-top competitors threaten SMS* (Sept. 2012), online: McKinsey & Company <https://www.mckinsey.com/~/media/mckinsey/dotcom/%20client_service/Telecoms/PDFs/Future_mobile_messaging_OTT.ashx>.

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

of notoriety due to harassing messages exchanged by application users and other inappropriate conduct.[17]

### 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.[18] 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.[19] Consumer and enterprise-grade versions of these applications, also known as "self-destructing messages" and "disappearing messages," are available from Wickr, Confide, and Snapchat. Other applications such as Facebook Messenger, Signal, and iMessage can be configured to include an ephemeral messaging feature.[20]

### 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 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.[21] These applications typically maintain communicated content in cloud-

---

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

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

19 See generally Agnieszka A. McPeak, "Disappearing Data" (2018) Wis. L. Rev 17 at 32 (discussing various technological features of ephemeral messaging applications).

20 Information from social media which bases communication on timed data (which is deleted after a set period of time) has been mentioned in the Canadian court system. This content itself has been referred to as "disappearing content", or "ephemeral content." Information from these communication mediums can clearly be valuable in court proceedings, and as such, has been requested in the past. In an application for production of documents in the case *Araya v Nevsun Resources Ltd.*, 2019 BCSC 262, personal communications were requested from platforms including Instagram and Snapchat, which use ephemeral content as a central method of communication. However, the production of these documents is another matter in itself. As seen in the court proceedings, information for discovery is limited to that which is within a party's "possession, power and control." The question of whether parties must disclose ephemeral content depends on whether such communication is within a party's possession, power, and control. To answer this question, it is necessary to consult the policies of companies that use ephemeral content, such as Instagram, Snapchat and Facebook follow.

21 See Philip Favro, Donald Billings, David Horrigan & Adam Kuhn, "The New Information Governance Playbook for Addressing Digital Age Threats" (2017) 3 Rich. J.L. & Tech. Ann. Survey ¶10.

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,[22] 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.[23] 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 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.[24] 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."[25]

These considerations also apply to an organization's internal communication tools, such as Zoom, Webex, GoToMeeting, and Microsoft Teams, which can broadcast and record video. Discovery of data from live-streaming video applications involves many of the same issues as those involved in

---

22 See Section II(A), *supra*.

23 See *FAQs*, online: Blind <https://www.teamblind.com/faqs> (last visited 28 Dec. 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.").

24 See *Vector Transportation Services Inc v. Traffic Tech Inc.,* [2008] OJ No 3500 (Ont. Sup. Ct. J.) (ordering that a computer be inspected by a forensic data recovery expert to retrieve deleted emails).

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

discovery of other social media. These issues include preservation and collection; relevance and proportionality; and power, possession, and control.[26]

### D. Location-Based Social Intelligence Platforms

Location-based social intelligence platforms enable searching across social media sites for conversations by keywords and geofencing. Geofencing is a software feature that uses global positioning system or radio frequency identification to define geographical boundaries.[27] To date, law enforcement and news reporters are the most prevalent users. Examples of companies developing and distributing the technology include DigitalStakeout, Echosec, Snaptrends, and Media Sonar.

The technology is still nascent and relies on the social media providers to feed data to these platforms through an application programming interface (API).[28] 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; and power, possession, and control.[29]

### E. Devices Using Social Media Applications

Devices are not social media platforms in and of themselves. Nevertheless, devices in some instances have been designed to work 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.[30] Users frequently use social media to communicate information found on their wearable technologies.

---

[26] The concept of power, possession, and control is referred to by different terminology in the rules of various Canadian provinces and territories and is also referred to as "possession, custody, and control" in this *Commentary* and other Sedona Conference publications. *See* Section III, *infra.*

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

[28] 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* (13 March 2017), online: <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," *The Economist* (22 March 2018).

[29] See Section III, *infra.*

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).[31] 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.[32] 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.[33] Whether in a smartphone or a stand-alone 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 Honor of Kings, Township, and Pokémon Go .

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; and power, possession, and control.[34]

---

[30] See Nicole Chauriye, "Wearable Devices As Admissible Evidence: Technology Is Killing Our Opportunities To Lie" (2014) 24 Cath. U. J. L. & Tech. 495 at 499.

[31] *See ibid.* at 500–02.

[32] See Richard Pérez-Peña & Matthew Rosenberg, "Strava Fitness App Can Reveal Military Sites, Analysts Say," *New York Times* (29 Jan. 2018) online: <https://www.nytimes.com/2018/01/29/world/middleeast/strava-heatmap.html>.

[33] Social media elements may also be found in social robots such as iPal and in devices that use artificial intelligence. Machine learning, based on human behavior, is used to auto-generate code to better customize the social experience. See Robin Raskin, "Robots on the Runway" (15 June 2016), online: Huff Post <https://www.huffpost.com/entry/robots-on-the-runway_b_10460902>.

[34] See Section III, *infra*.

## 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.[35] 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 power, possession, or control over 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
- 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 discovery planning[36] regarding the discoverable information that will be sought or should be provided from social media platforms and applications.[37]

The purpose of discovery planning is to identify and resolve discovery-related issues in a timely fashion and to make access to justice more feasible and affordable. The process is not intended to create

---

[35] *Wilder v. Munro*, 2015 BCSC 1983 (CanLII) at para 16 ("the considerations for the court include the probative value of the information sought, privacy concerns, potential prejudice to the plaintiff and proportionality").

[36] It has been common to refer to the "meet-and-confer" process, or to say that the parties will "meet and confer" or attend a specific "meet-and-confer" session. While this *Commentary* will still use this term, the point is not that there must be one or more meetings; the emphasis should be on conferring with a view to reaching meaningful agreement on a discovery plan.

[37] On January 1, 2010, Ontario amended its Rules of Civil Procedure to include two new rules: Rule 29.1 (Discovery Plan) and Rule 29.2. (Proportionality in Discovery). Rule 29.1 imposes an affirmative obligation on the parties to agree to a discovery plan and requires that "[i]n preparing the discovery plan, the parties shall consult and have regard to the document titled *The Sedona Canada Principles Addressing Electronic Discovery* developed by and available from The Sedona Conference."

side litigation.[38] Cooperation includes collaboration in developing and implementing a discovery plan to address the various steps in the discovery process. These will include some or all of the following steps: the identification, preservation, collection, and processing of documents;[39] the review and production of documents;[40] how privileged documents are to be handled or other grounds to withhold evidence; costs; and protocols.

This section is designed to provide guidance for addressing the most common discovery challenges associated with social media.[41]

### A. Relevance and Proportionality

The scope of discovery for social media content is driven by a balance between relevance, proportionality,[42] and privacy interests. Relevance in discovery is broader than at trial. A consideration of relevance begins with the pleadings:[43]

> A party must produce every document that is relevant to the issues pleaded in the proceeding.
>
> A litigant has the initial obligation of disclosing relevant documents in the first instance. There must be some evidence of non-disclosure or of omission from the

---

38 *Drywall Acoustic, Lathing and Insulation, Local 675 Pension Fund (Trustees) v SNC Lavalin Group Inc.*, 2014 ONSC 660 at paras 81–84.

39 "Processing" means "the automated ingestion of electronically stored information into a program for the purpose of extracting metadata and text; and in some cases, the creation of a static image of the source ESI files according to a predetermined set of specifications, in anticipation of loading to a database. Specifications can include the de-duplication of ESI, or filtering based on metadata contents such as date or email domain and specific metadata fields to be included in the final product." "The Sedona Conference Glossary: eDiscovery & Digital Information Management, Fifth Edition" (2020) 21 Sedona Conf. J. 263 at 355. Processing can also involve steps to deal with documents that require special treatment, such as encrypted or password-protected files. Parties should avoid making processing decisions that have consequences for others without first discussing those decisions. An effective discovery plan will address issues such as the means of creating hash values, whether to separate attachments from emails and which time zone to use when standardizing Date and Time values.

40 Parties may consider adopting a staged or phased approach to eDiscovery where appropriate due to the volume of evidence. Parties should also agree as early as possible on production specifications.

41 For additional guidance on these issues, see The Sedona Conference, "The Sedona Canada Principles Addressing Electronic Discovery, Third Edition, Public Comment Version" (2021) online: <https://thesedonaconference.org/publication/The_Sedona_Canada_Principles> ["The Sedona Canada Principles, Third Edition"], and The Sedona Conference, "Commentary on Legal Holds, Second Edition: The Trigger & The Process" (2019) 20 Sedona Conf. J. 341.

42 "The Sedona Canada Principles, Third Edition," *supra* note 41, Principle 4. Most Canadian jurisdictions have amended their respective rules of court to expressly include proportionality as a general rule for all litigation, and specifically in discovery procedures.

43 *Merpaw v. Hyde*, 2015 ONSC 1053 (CanLII).

> production and disclosure obligations of the litigant before production will be ordered. The court is required to consider proportionality pursuant to Rule 29.2.03, and the evidence must suggest that the benefits of the investigation warrant the costs.
>
> The value of disclosure may be overborne by other values including privacy, access to justice and the fair and efficient use of scarce resources in the administration of justice. The court retains discretion and may refuse disclosure where information is of minimal importance but the search for it might compromise other important interests.[44]

The *Commentary on Discovery of Social Media in Canada* 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.[45]

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 cases, just as all of a party's emails are not likely to be relevant.[46] A court can refuse disclosure when the information is of little importance to the litigation and disclosure may constitute a serious invasion of privacy. The question to be asked is whether the invasion of privacy is necessary to the proper administration of justice, and if so, whether some terms are appropriate to limit that invasion.[47]

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.[48]

---

44 *Ibid*., paras 14–16

45 See Section III(C), *infra*.

46 *M.(A.) v. Ryan*, 1994 CanLII 6417; aff'd, 1997 CanLII 403 (SCC).

47 *Ibid.*

48 *Merpaw v. Hyde*, 2015 ONSC 1053 (CanLII).

Turning to proportionality, courts have repeatedly used the analogy that a computer hard drive is the digital equivalent to a filing cabinet. A request to be able to search a party's filing cabinet in the hopes that there might be found a document in which an admission against interest is made would clearly not be allowed—and its digital equivalent should also not be allowed.[49]

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.

### 1. Privacy Considerations

Privacy considerations impact both the scope and conduct of discovery involving social media evidence. Privacy obligations on parties arise from federal and provincial privacy statutes, as well as common law. These obligations require parties to consider individuals' privacy interests regardless of whether the individual is a party to the litigation. Such privacy interests are often a key consideration when dealing with social media evidence, given both the volume and sensitivity of personal information that exist on social media platforms. Individuals' privacy interests on social media and litigants' discovery rights require balancing. However, both can often be accommodated to a large extent by including practical solutions in the discovery planning process.

Privacy interests are not an automatic bar to discovery of relevant information, regardless of whether it is located in social media or elsewhere. Rather, privacy interests are best viewed as an important aspect of proportionality. Privacy concerns should not be confused with discovery exclusions such as legal privileges or doctrines recognized under well-developed case law. Just like these exclusions, a person's privacy interests in social media communications can influence the scope of discovery. However, unlike discovery exclusions, privacy interests are neither determinative nor binary in their impact. A party may not use privacy expectations as a blanket or categorical protection against discovery, but a party may use privacy interests to protect against overly broad or invasive discovery where privacy interests outweigh the probative value of the information sought. Thus, 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.

Privacy considerations also have implications for the conduct of discovery. Statutory and common law privacy obligations impose requirements on how and when "personal information" should be collected, used, disclosed, and protected.

#### a. What is personal information?

The term "personal information" is broadly defined under Canadian privacy legislation as "information about an identifiable individual." Information will be "about" an individual when it relates to

---

[49] *Ibid.* at para 60.

or concerns the individual.[50] Individuals will be "identifiable" where there is a serious possibility that they could be identified through the use of that information, alone or in combination with other available information.[51]

### b. Statutory Privacy Landscape

Canada and its provinces, to varying extents, have public and private sector privacy legislation[52] governing the collection, use, and disclosure of personal information that may affect the discovery process. The rest of this section focuses on the Canadian private sector privacy regime.

The privacy law regime under the federal Personal Information Protection and Electronic Documents Act (PIPEDA) applies to organizations that collect, use, or disclose personal information in the course of commercial activities.[53]

PIPEDA presumptively applies to all federally or provincially regulated entities, unless the organization is otherwise subject to provincial privacy legislation that has been declared to be "substantially similar" to PIPEDA.[54] The three provinces that have enacted "substantially similar" legislation are Alberta, British Columbia, and Québec. In such cases, the substantially similar provincial law applies instead of PIPEDA, although PIPEDA continues to apply to interprovincial or international transfers of personal information.[55]

---

50 *Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board)*, 2006 FCA 157 (CanLII), [2007] 1 FCR 203, at paras 43, 59, 61.

51 *Gordon v. Canada (Health)*, 2008 FC 258 (CanLII), at para. 33.

52 Legislation regulating the public sector includes: the *Privacy Act*, RSC 1985, c P-21; *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165; *Freedom of Information and Protection of Privacy Act*, RSA 2000, c F-25; *Freedom of Information and Protection of Privacy Act*, SS 1990-91, c F-22.01; *Freedom of Information and Protection of Privacy Act*, CCSM c F-175; *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F-31; *An Act respecting access to documents held by public bodies and the protection of personal information*, LRQ c A-2.1; *Freedom of Information and Protection of Privacy Act*, SNS 1993, c 5; *Personal Health Information Privacy and Access Act*, SNB 2009, c P-7.05; *Freedom of Information and Protection of Privacy Act*, RSPEI 1988, c F-15.01; *Access to Information and Protection of Privacy Act*, 2015, SNL 2015, c A-1.2. *Legislation governing the private sector includes the Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 [*PIPEDA*]; *Personal Information Protection Act*, SBC 2003, c 63; *Personal Information Protection Act*, SA 2003, c P-6.5; *An Act respecting the protection of personal information in the private sector*, LRQ c P-39.1.

53 *PIPEDA*, *supra* note 52, c 5.

54 *Ibid.* at s.26(2).

55 Alberta, Saskatchewan, Manitoba, Ontario, New Brunswick, Nova Scotia, and Newfoundland and Labrador have enacted privacy legislation as well, but only with respect to personal health information collected, used, or disclosed by health information custodians. These statutes should be consulted when a party to litigation (or third-party source of evidence) is a health information custodian or agent, and counsel anticipate that personal health information will be relevant to the issues in the case.

Although the provincial statutes and PIPEDA share common objectives and are based upon similar key principles, there are some obligations imposed by the provincial statutes that exceed those imposed by PIPEDA.

The main area for uneven privacy law coverage between the federal and provincial statutes is in relation to employee personal information. PIPEDA only applies to information about employees of organizations that are federal works, undertakings, or businesses (as defined in PIPEDA).[56] In contrast, the privacy legislation in Québec, British Columbia, and Alberta applies to employee information held by organizations subject to these laws. As a result, organizations may face different privacy law considerations when handling social media evidence that contains, or constitutes, personal information of employees, depending on whether they are governed by federal or provincial law and whether they are deemed to be federal businesses under PIPEDA.

The prevailing view is that Canadian private sector privacy legislation does not apply to personal information collected for purposes of litigation. Further, while this legislation typically requires consent of and notice to an individual before their personal information is disclosed, disclosure required by the rules of court or a court or tribunal order is typically exempt.

Outside of the litigation context, an individual's consent is, with some exceptions, required for the collection, use, or disclosure of their personal information. Such consent may be implied in certain circumstances, but express consent is required for the collection, use, or disclosure of sensitive information and is encouraged by privacy regulators as a best practice in almost all cases. The central exemptions relevant to the litigation context are discussed below.

### c. Privacy Law Exemptions Relevant to Civil Litigation

Provincial private-sector privacy laws each include a provision providing that nothing in those Acts shall be construed to interfere with information that is otherwise available by law to a party to a proceeding.[57] This prevents litigants from objecting to production of personal information contained in social media evidence relevant to the case.[58]

In contrast, PIPEDA does not contain a general exemption for information used in litigation, but the prevailing view is that PIPEDA does not apply to personal information handled in the course of litigation because litigation does not constitute a commercial activity. For example, if a defendant hires a private investigator to perform social media searches about the plaintiff, the defendant is not

---

[56] *PIPEDA*, *supra* note 52, s.2(1).

[57] *Personal Information Protection Act*, SBC 2003, c 63, s.18(i); *Personal Information Protection Act*, SA 2003, c P-6.5, s.20(e); e *Protection of Personal Information in the Private Sector* [*Québec's Private Sector Act*] s.18.

[58] Hatfield v. Intact Insurance Company, 2014 NSSC 232 (CanLII), at paras 25–30. See also *Pettigrew v. Halifax Regional Water Commission*, 2018 NSSC 197 (CanLII), at paras 26–27 for a similar conclusion respecting the application of the Nova Scotia Freedom of Information and Protection of Privacy Act in relation to the disclosure of third-party information.

engaged in a commercial activity that engages PIPEDA, nor is any person employed by them doing so.[59] In contrast, if a federal business engages a background check service to perform social media searches before hiring a job candidate, the information will be subject to PIPEDA when used for hiring purposes. Importantly, however, if those social media search results become relevant to subsequent litigation, they may be produced without consent if necessary, to comply with discovery obligations under the exemption described below.[60]

PIPEDA does contain certain exceptions to the requirement for consent that permit the collection, use, or disclosure of personal information that may apply in the litigation context. Of particular relevance, PIPEDA allows disclosure of personal information (1) to the organization's lawyer or notary;[61] (2) where required to comply with a court (or tribunal) order;[62] or (3) where required to comply with rules of court relating to document production.[63]

Given the exemption of litigation, statutory privacy law obligations are typically engaged for purposes and activities that extend beyond what is strictly required for the litigation. Examples of activities that may engage statutory obligations include collecting irrelevant personal information from social media pages, sharing information with U.S. counsel in parallel proceedings, and responding to access requests from likely litigants in advance of litigation.

Parties and their counsel should generally avoid the collection, use, or disclosure of personal information where it is unnecessary or unrelated to the litigation.

Parties and their counsel should also ensure that proper safeguards are incorporated into the collection, review, and disclosure of personal information from social media. Failure to apply proper safeguards could give rise to privacy complaints if personal information is collected, reviewed, used, or disclosed where not strictly required by court rules or orders.

In addition, parties should be mindful of activities that may engage privacy laws in other jurisdictions. International privacy laws may apply to personal information on social media and may not have the same exemptions for litigation purposes.

---

59 *State Farm Mutual Automobile Insurance Company v. Privacy Commissioner of Canada*, 2010 FC 736 (CanLII), at para 106.

60 *Wyndowe v. Rousseau*, 2008 FCA 39 (CanLII), at paras 35–49. Kelly Friedman, "Canada's Privacy Regime as It Relates to Litigation and Trans-Border Data Flows" (2012) 13 Sedona Conf. J. 253 at 255–56 [*Friedman*] online: <https://thesedonaconference.org/sites/default/files/publications/253-266%20Friedman.pdf>.

61 *PIPEDA*, *supra* note 532, s.7(3)(a).

62 *Ibid.* s.7(3)(c).

63 *Ibid.*

### d. Privacy Obligations and the Implied Undertaking Rule

The "implied undertaking rule" is a common law rule that prohibits parties from disclosing evidence and information obtained during the discovery process outside the confines of the litigation.[64] This rule has since been codified in various civil procedure rules and is referred to as the "deemed undertaking rule." Although this rule may lend comfort to litigants who are required to disclose personal details in the course of litigation but are concerned about broader dissemination of that information, the deemed undertaking rule does not provide full privacy protection. For example, in Ontario, the deemed undertaking rule only applies to evidence obtained in the discovery process and does not apply to evidence filed with the court or referred to during a hearing.[65] A court order can also be obtained to relieve compliance with the deemed undertaking rule.[66]

### e. Common Law Privacy Issues Relevant to Social Media Evidence

Because social media is so easily used to communicate and create personal information, a party (or a party's employee) may have significant privacy concerns about the production of such evidence even if it is required by court rules and permitted by privacy statutes. In many cases it is necessary to balance privacy interests with discovery obligations even where consent to produce personal information is not required by statute. Similarly, privacy must be considered where no statute applies, such as for many organizations' employee information or data gathered outside the context of commercial or public-sector activity.

A privacy interest arises in information "that could qualify as revealing very personal information over which most right thinking Canadians would expect a reasonable expectation of privacy" or information that reveals "intimate details of the lifestyle and personal choices of the individual."[67] Although individuals' privacy interests may be diminished when they are parties to litigation, there are scenarios where privacy concerns will outweigh the need for full disclosure of relevant information in the judicial process.[68]

---

64 *Goodman v. Rossi* (1995), 24 OR (3d) 359 (Ont. C.A.). See *Friedman*, *supra* note 60, at 259–60 for a more extended discussion.

65 *Rules of Civil Procedure*, RRO 1990, Reg 194, r. 30.1.01.

66 *Rules of Civil Procedure*, RRO 1990, Reg 194, r 30.1.01. "The Sedona Canada Principles, Third Edition," *supra* note 41, Comment 9.c.

67 *Carter v. Connors*, 2009 NBQB 317 (CanLII), at para 38.

68 Although obiter to the decision of the court, Justice McLachlin's (as she was then) comments in *M. (A.) v. Ryan*, 1997 CanLII 403 (SCC), [1997] 1 SCR 157, at paras 36–38 have been repeatedly cited by the courts in production cases, including those for social media content, for guidance in determining the appropriate balance to be struck when assessing a litigant's privacy interest in an application for production of documents.

Common privacy concerns with social media include the form of access to the account information and the sensitivity of the communications. Because relevant information from social media accounts are documents for the purpose of discovery, social media evidence should be produced by the party with control over it. It will generally never be necessary or appropriate to allow the opposing party to access a social media account directly or to require a litigant to provide their account password to another party. In rare cases where information about social media usage is relevant and cannot be obtained through production of documents or metadata from the accounts or associated devices, an expert should be engaged to perform a targeted review. Having a third party access the account or device, rather than providing a password and direct access to an opposing party or counsel, and permitting that expert to separate relevant information from data outside the scope of litigation or information belonging to non-parties minimizes the privacy intrusion.[69]

### f. Litigants' Privacy Interests

In other cases, the content of documents subject to discovery will require significant balancing of parties' privacy interests with their rights to discovery. For example, the plaintiff in a case alleging nonconsensual distribution of intimate images may seek to avoid producing copies of the images themselves and propose to instead provide metadata about when the images were sent to the defendant or posted by the defendant to public websites. A court will first have to assess whether the content of the documents—the images themselves, in the above example—is relevant to the issues in the litigation. If relevance has been established, the court must then weigh the benefits of requiring the disclosure of the information against the invasion of privacy and the burden of production.[70] In assessing the weight to be given to the privacy interest in a particular case, courts have generally sought to assess "whether the invasion of privacy is necessary to the proper administration of justice and, if so, whether some terms are appropriate to limit that invasion."[71] For example, where there is risk that an opposing party will misuse the personal information contained in certain productions, an order restricting access to counsel only may be appropriate.

Some courts have found litigants' privacy interests in social media posts to be limited, even where the documents are on a restricted access page, because the act of sharing materials on social media undercut the assertion of a privacy interest.[72] A number of decisions, however, have expressed a contrasting view: by restricting access or setting a social media page to private, a party has indicated

---

[69] *Bishop v. Minichiello*, 2009 BCSC 358 (CanLII), at paras 46–58, leave to appeal for further production dismissed, 2009 BCCA 555.

[70] *Leduc, supra* note 2, at paras 14, 32–36; *Frangione, supra* note 2, at paras 26–73; *Murphy, supra* note 2, at para 10; *McDonnell, supra* note 2*,* at paras 15–16; and *Casco*, *supra* note 2, at para 2.

[71] *A.M. v. Ryan*, 1994 CanLII 6417 (BC CA), at para 45; see also *Merpaw v. Hyde*, 2015 ONSC 1053 (CanLII), at para 20.

[72] The most extreme statement of this view was made by the court in *Murphy, supra* note 2, when it concluded at para. 20 that "[t]he plaintiff could not have a serious expectation of privacy given that 366 people have been granted access to the private site." See also, for example, *Leduc*, *supra* note 2, at para 35, and *Frangione, supra* note 2, at para 38.

a choice to exclude all other users. From this choice, the courts inferred that a litigant retains a "real" privacy interest in the content of the restricted access site.[73] This is consistent with the conception of privacy rights based on the individual's discretion to control, not simply to hide, their personal information.[74] It is also consistent with the common law development of privacy torts in Canada, several of which focus on the individual's right to control the forum and scope of access to and disclosure of their personal information.

### g. Third-Party Privacy Interests

Courts have not hesitated to order production of content from social media platforms even in the absence of the consent of the third party. However, where the social media content contains personal information that is not relevant or where their privacy interest outweighs factors favouring disclosure, courts have ordered that the information be redacted or otherwise concealed to protect the third party's privacy interest.[75] This balancing exercise may also result in the severance of different parts of social media evidence. For example, a court may order production of a posted photograph that depicts third parties but permit the comments on such a photo to be withheld on the basis of privacy concerns and relevance.[76]

Third-party interests also arise where social media evidence is no longer in the control or possession of any party and must be obtained from the social media platform or provider. In such cases, a party may seek a Norwich order for pre-discovery production from third parties. This may be necessary to give the third party comfort that it is legally permitted to disclose personal information in its possession without consent of the subjects. In assessing such applications, courts weigh a variety of factors, including the privacy interests of the person whose information is to be disclosed.[77]

---

[73] See S*tewart v. Kempster*, 2012 ONSC 7236 (CanLII), at para 24. See also *Jones v. I.F. Propco*, 2018 ONSC 23 (CanLII), at para 41.

[74] This issue has been addressed in detail in the criminal law and Charter privacy rights context. For example, the Supreme Court in *R. v. Marakah*, 2017 SCC 59 (CanLII), and *R. v. Jones*, 2017 SCC 60 (CanLII), made it clear that a party can have a reasonable expectation of privacy in their digital communications even if the information has been sent to another, such as by text message. Therefore, charter privacy rights of individuals vis-à-vis the state do not depend on the complete nondisclosure of personal information; an individual may selectively disclose private details via social media to some while maintaining privacy rights over that information against others.

[75] *Fric v. Gershman*, 2012 BCSC 614 (CanLII), at para72.

[76] *Ibid.* at para 75, citing *Dosanjh v. Leblanc and St. Paul's Hospital*, 2011 BCSC 1660.

[77] The court in *York University v. Bell Canada Enterprises*, 2009 CanLII 46447 (ON SC), weighed five factors in assessing York University's application for a Norwich Order to have Bell and Rogers disclose information necessary to identify the anonymous author(s) of allegedly defamatory emails and a web posting, including at paragraphs 29-36 whether the interests of justice when set against competing interests such as a customer's expectation of privacy favour obtaining the disclosure. See also *Carleton Condominium Corporation No. 282 v. Yahoo! Inc.*, 2017 Carswell Ont 10986 at paras15–19.

### h. Best Practices

Parties and their counsel should anticipate litigant and third-party privacy concerns at the outset of the discovery planning process and raise them with opposing counsel well in advance of production. Agreements on privacy-accommodating steps should be memorialized in the discovery plan, or otherwise in writing. In many cases the parties will be aligned on the appropriate steps to avoid unnecessary invasions of privacy, or the issues can be streamlined to reduce costs associated with seeking court direction.

Practical solutions can often accommodate both discovery rights and privacy interests of litigants and third parties. Reviewing metadata only or disclosing information on a "counsel's eyes only" basis are two examples discussed above. Other examples include permitting parties to redact or sever sensitive and irrelevant information from documents being produced; restrictions on filing information in court without notice; and data security practices including requirements to destroy information after the matter has ended.

Counsel should also consider whether case-specific privacy issues meet the *Sierra Club* test for a confidentiality order and the high value courts assign the open court principle.[78] Parties should not assume that simply because they agree to designate documents containing personal information as confidential the court will seal them from public access. Alternative measures—including modifying documents to render them less sensitive, producing or filing different evidence, or agreeing to uncontested facts that render the personal information unnecessary—should be considered and discussed with all parties early in the discovery and trial preparation phases of litigation.

The same considerations regarding litigants' privacy interests apply to discovery of third-party information. While parties may pursue discovery of relevant social media content regarding third parties,[79] they should consider managing the discovery to minimize potential embarrassment to third parties and protect against unnecessary disclosure of their sensitive personal information.[80] 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. 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.

---

78 *Sierra Club of Canada v. Canada (Minister of Finance)*, 2002 SCC 41 (CanLII), [2002] 2 SCR 522.

79 See *Frangione, supra* note 2, (holding that an inference could be made from the plaintiff's Facebook profile that private messages with Facebook friends were likely relevant).

80 See *Carter v. Connors*, 2009 NBBR 317 (QB) (holding that document production should not trench upon third-party privacy rights).

### 2. Requesting Social Media Evidence

The appropriate procedure for requesting and obtaining relevant social media information, as with all types of electronically stored information (ESI), is 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 nonprivileged information.[81]

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.[82] 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 responding party's duty to conduct a reasonable inquiry is triggered.[83]

Upon determining that the preservation of social media evidence is necessary,[84] the parties should discuss the requirement during the discovery planning stage. Specifically, the parties should communicate to the affected persons the need to preserve relevant social media information. This notice is referred to as a "legal hold" or preservation notice.[85] The style, content, and distribution of the le-

---

81 *Merpaw v. Hyde*, 2015 ONSC 1053 (Ont. Sup. Ct. J.) (stating that the defendant must establish evidence of omission of relevant documents).

82 *Rules of Civil Procedure*, RRO 1990, r. 30.02(1); *Court of Queen's Bench Rules*, Man Reg 553/88, r. 30.02(1); *Rules of Court of New Brunswick*, NB Reg 82-73, r. 31.02(1); *Rules of the Supreme Court of the Northwest Territories*, NWT Reg R-010-96, r. 219; *Rules of Civil Procedure*, PEI Rules, r. 30.02(1); *Supreme Court Civil Rules*, BC Reg 168/2009, r. 7-1(1); *Alberta Rules of Court*, Alta Reg 390/68, r. 187.1(2); R*ules of the Supreme Court*, 1986, SN 1986, r. 32.01(4); *Nova Scotia Civil Procedure Rules*, NS Civ Pro Rules 2009, r. 14.08(2); *The Queen's Bench Rules*, Sask QB Rules 2013, r. 5-6(2); *Rules of Court*, Yuk Reg OIC 2009/65, r. 25(3).

83 *Rules of Civil Procedure*, RRO 1990, r. 30.02(2); *Court of Queen's Bench Rules*, Man Reg 553/88, r. 30.02(2); *Rules of Court of New Brunswick*, NB Reg 82-73, r. 31.02(2); *Rules of Civil Procedure*, PEI Rules, r. 30.02(2); *Alberta Rules of Court*, Alta Reg 390/68, r. 205; *Rules of the Supreme Court*, 1986, SN 1986, r. 32.02; *Nova Scotia Civil Procedure Rules*, NS Civ Pro Rules 2009, r. 14.10; *The Queen's Bench Rules*, Sask QB Rules 2013, r. 5-6(2); *The Queen's Bench Rules*, Sask QB Rules 2013, r. 5-11; *Rules of Court*, Yuk Reg OIC 2009/65, rr. 25(3)-(4); *Supreme Court Civil Rules*, BC Reg 168/2009, r. 7-1(13); Rules of the Supreme Court of the Northwest Territories, NWT Reg R-010-96, r. 225.; *Leduc v. Roman*, [2009] OJ No 681 (Ont. Sup. Ct. J.) ("A party who maintains a private, or limited access, Facebook profile stands in no different position than one who sets up a publicly-available profile. Both are obliged to identify and produce any postings that relate to any matter in issue in an action.").

84 The Crown and police in criminal proceedings also have a duty to preserve evidence. *See R v. Sharma*, 2014 ABPC 131 (CanLII) at para 92.

85 "Legal hold" refers to the process by which an organization seeks to satisfy an obligation to preserve, initially by issuing a communication designed to suspend the normal disposition of information pursuant to a policy of through automated functions of certain systems. The term "legal hold notice" is used when referring to the actual communication. The term "legal hold" is used rather than "litigation hold" (or other similar terms) to recognize that a legal hold may apply in nonlitigation circumstances (e.g. pre-litigation, government investigation, or tax audit). See The Sedona Conference, "Commentary on Legal Holds, Second Edition: The Trigger & The Process" (2019) 20 Sedona Conf. J. 341.

gal hold will vary widely depending upon the circumstances, from a formal legal hold notice to an email communication. Regardless of form, the language used should be plain and provide clear instructions to recipients. The legal hold should set out in detail the kinds of information that must be preserved so the affected custodians can preserve it. The legal hold should mention the volatility of social media content and make it clear that particular care must be taken not to alter, delete, or destroy it.[86]

In the civil law jurisdiction of Québec, the parties' obligations in the context of litigation differ from that in common law jurisdictions. For instance, the obligation to disclose documents to the opposing party ("communication of documents") is, at the first stage of litigation, limited to those documents that the disclosing party intends to refer to as exhibits at the hearing. The receiving party can also request specific documents in the context of discovery.

Although there is no specific obligation to preserve electronic documents in advance of litigation,[87] the Superior Court has recognized the existence of an implicit obligation to preserve evidence based on the general obligation of parties to refrain from acting with the intent of causing prejudice to another person or behaving in an excessive or unreasonable manner, which would be contrary to the requirements of good faith as prescribed by the *Code of Civil Procedure*.[88]

Before litigation has started, a party who has reason to fear that relevant evidence will become lost or more difficult to use can apply to the court for an order to allow a person of the party's choice to examine the evidence in question if its condition may affect the outcome of the expected legal proceeding.[89]

In Québec, in view of the absence of an express preservation obligation, a party seeking a preservation order would need to present a motion for injunction or safeguard order in accordance with the criteria governing such proceedings.[90] In all circumstances, parties should send a legal hold letter to the other parties to ensure that the other parties are aware of the ESI[91] that will be requested.

Social media evidence is often sought in cases where a party's physical or mental state during a 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

---

86 Ontario Bar Association, *Model Precedents*, online: <https://www.oba.org/EIC/Model-Precedents>.

87 *Jacques c Ultramar ltée*, 2011 QCCS 6020 (CanLII).

88 *Québec Code of Civil Procedure*, CQLR c C-25, s 4.1.

89 *Ibid*, s 438.

90 *Ultramar, supra* note 87, at para 26.

91 Electronically stored information, regardless of the media or whether it is in the original format in which it was created, as opposed to stored in hard copy (i.e., on paper).

may be relevant and discoverable.[92] Such information has been found to be relevant in criminal proceedings, employment discrimination, personal injury, and workers compensation cases. In all cases courts must assess whether evidence from social media may reveal some insight into the crime or credibility of the witness, weighing whether the evidence is more probative than prejudicial.[93]

### B. Possession, Custody, and Control

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.[94] A party who uses social media may not have "possession" of the data, except to the extent that some of the data may be on the party's devices.[95] That social media technologies are constantly changing their functionality and storage features adds to the complexity of this issue.

#### 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.[96] 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

---

92 *See Jones v. I.F. Propco*, 2018 ONSC 23 (Ont. Sup. Ct. J.); *Stewart v. Kempster*, 2012 ONSC 7236 (Ont. Sup. Ct. J.); *Papamichalopoulos v. Greenwood*, 2018 ONSC 2743 (Ont. Sup. Ct. J.) (photos at odds with the plaintiff's allegedly severe and permanent injuries are relevant and producible).

93 *R. v. Seaboyer*, [1991] 2 SCR 577 (preventing inflammatory statements or embarrassing photographs from distracting the court), *R. v. Jilg*, 2010 BCSC 1476.

94 The concept of possession, control, or power, as addressed herein, derives from *Alberta Rules of Court*, Alta Reg 390/68, r 193(1); *Alberta Rules of Court*, Alta Reg 124/2010, r 5.14(1); *Supreme Court Civil Rules*, BC Reg 168/2009, rr 7-1(10), 7-1(15); *Court of Queen's Bench Rules*, Man Reg 553/88, rr 30.04(1), 30.04(3); *Rules of Court of New Brunswick*, NB Reg 82 82-73, r 31.04; *Rules of the Supreme Court of the Northwest Territories*, NWT Reg R-010-96, r 225(1); *Rules of the Supreme Court*, SN 1986, r 32.05; *Nova Scotia Civil Procedure Rules* (1972), NS Civ Pro Rules 2009, rr 14.10, 16.02, 20.04; *Rules of Civil Procedure*, RRO 1990, r 30.04; *Rules of Civil Procedure*, PEI Rules, r 30.04; *The Queen's Bench Rules*, Sask QB Rules 2013, rr 5-11(1), 5-11(3); *Rules of Court*, Yuk Reg OIC 2009/65, r 25(18). *Rules of Civil Procedure*, RRO 1990, r 30.04 states "[a] party who serves on another party a request to inspect documents (Form 30C) is entitled to inspect any document that is not privileged and that is referred to in the other party's affidavit of documents as being in that party's possession, control or power." The occasional use of "*and* power" in the *Commentary* is intended to address all three factors. It does not replace or diminish the "possession, control, or power" standard, which is discussed in this Section.

95 See The Sedona Conference, "Commentary on Rule 34 and Rule 45 'Possession, Custody, or Control'" (2016) 17 Sedona Conf. J. 467 at 524.

96 *Leduc v. Roman*, [2009] OJ No 681 (Ont. Sup. Ct. J.) at para 32 ("A party who maintains a private, or limited access, Facebook profile stands in no different position than one who sets up a publicly-available profile. . . . Mr. Leduc exercised control over a social networking and information site to which he allowed designated "friends" access.").

preserve and collect information from the account. Further, the user can do so without violating the service provider's terms of service or provincial or federal law (such as PIPEDA).

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 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.[97] Nevertheless, the user may still exercise "control" over such information and may be able to gain, grant, or deny access pursuant to end-user agreements, social media provider policy,[98] or as a "cus-

---

[97] Account activity log data may include the date and time the account was accessed, internet protocol (IP) addresses from where the account was accessed, and reports detailing other aspects of the user's social media account. *Carter v. Connors*, 2009 NBBR 317 (QB) ("It is not clear at this point whether Bell-Aliant has the capacity to generate discrete Facebook use data and the requested order is conditional on those records being in existence or able to be specifically identified and generated."); *Conrod v. Caverley*, 2014 NSSC 35 (SC) (stating that usage records were relevant and the contents did not reveal any potentially sensitive personal information).

[98] See, *e.g.*, *Facebook Terms of Service* § 3, online: Facebook <https://www.facebook.com/legal/terms/update> (last revised 22 Oct. 2020) ("You own the intellectual property rights (things like copyright or trademarks) in any such content that you create and share on Facebook and the other Facebook Company Products you use. 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, online: Twitter <https://twitter.com/en/tos> (effective 18 June 2020) ("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 considered part of the Content."); *Instagram Privacy and Safety Center, Terms of Use* § 4, online: Instagram Help Ctr. <https://help.instagram.com/478745558852511> (last revised 20 Dec. 2020) ("We do not claim ownership of your content that you post on or through the Service and you are free to share your content with anyone else, wherever you want."); *LinkedIn User Agreement* § 2.2, online: LinkedIn <https://www.linkedin.com/legal/user-agreement> (effective 11 August 2020) ("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, online: Snap <https://www.snap.com/en-US/terms/> (effective 30 Oct. 2019) ("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, online: Reddit <https://www.redditinc.com/policies/user-agreement> (last revised 15 Sept. 2020) ("You retain any ownership rights you have in Your Content, but you grant Reddit the follow-

tomer" of or "subscriber" to the account.[99] As noted in more detail below, most social media platforms have established means by which a user can download content (data) from the platform.

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 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 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 of or subscriber to the social media service.

Thus far, courts have not expressly applied the practical ability test to an individual's ability to obtain the social media information of another entity or party. Nevertheless, a few courts in the United States have found control—without specifically invoking the practical ability test—despite the individual not having a legal right to the requested information.[100]

### 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.[101]

Employers generally do not have control over their employees' personal social media accounts. Personal property of an employee is not generally under the "control" of the employer unless the employer has a legal right to obtain the property from its employee.[102]

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 laws. Moreover, provin-

---

ing license to use that Content . . . ."); *Tumblr Terms of Service* § 6, online: Tumblr <https://www.tumblr.com/policy/en/terms-of-service> (last modified 25 Sept. 2019) ("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.").

99 See Section III(D), *infra*.

100 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).

101 *Red Label Vacations Inc. v. 411 Travel Buys Ltd.*, 2015 FC 18.

102 See *Canadian Broadcasting Corporation v Canadian Media Guild,* 2021 CanLII 761 (CA LA); *R v. Cole*, 2012 SCC 53 (holding that employees have a reasonable expectation of privacy in their work computers where personal use is permitted or reasonably expected).

cial and federal statutes 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.[103] And employers do not have "control" over something that they are prohibited from accessing by 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 reasonably anticipated litigation.[104] 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.[105]

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.[106] For example, a party might need to collect its relevant ESI from a third-party social

---

[103] *Canadian Broadcasting Corporation v. Canadian Media Guild*, 2021 CanLII 761 (CA LA) (holding that an employee's manager was not permitted to search private social media accounts inadvertently left logged into on a shared work laptop).

[104] See *Blatherwick v. Blatherwick*, 2015 ONSC 2606 at paras 295–97, 560–62 (defendant found in breach of Mareva Order that required he preserve relevant electronic documents after emails had been automatically deleted).

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

[106] See Section III(B), *supra*.

media provider to avoid its potential loss, particularly if the provider could take action to terminate the account and delete content.

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.

A party should also consider the types of social media data that may be obtained, which may go beyond ESI that would 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.[107] Features such as encryption and ephemeral messaging can also raise preservation issues that need to be considered in any review of social media data.[108]

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 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.[109]

A party should additionally consider whether the dynamic nature of a social media platform requires that it perform more than one collection from that platform. 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.

---

[107] See Section III(A), *supra*.

[108] See Section II(B)(3), *supra*.

[109] See "Commentary on Proportionality in Electronic Discovery," *supra* note 105, 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.[110]

### 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.[111] Such discussions will ideally take place as early as possible and should be raised prior to or during discovery planning. Relevance and proportionality principles 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.[112] There will undoubtedly be instances where such cooperation may not be possible (as when opposing counsel has not been identified after the duty to preserve is triggered) or practicable (when an adversary is unreasonable).[113]

### 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. Each party has an obligation to take reasonable steps to preserve, disclose, and produce any document the party's possession, power, or control that the party knows exists and knows is relevant to the action.[114]

---

[110] See Section V, *infra.*

[111] See "The Sedona Conference Cooperation Proclamation" (2009 Supp.) 10 Sedona Conf. J. 331; As noted above, as an example, under the Ontario Rules of Civil Procedure (Rule 29.1), all parties to an action must agree to a discovery plan if they intend to obtain evidence through documents, oral examination or examination for discovery by written questions. A discovery plan outlines the scope of the discovery for all parties and is meant to be a collaborative process which assists in moving the legal proceeding forward.

[112] See "Commentary on Proportionality in Electronic Discovery," *supra* note **Error! Bookmark not defined.**5, at 155–59 (explaining in Principle 2 the roles of cooperation and phased discovery in advancing the aims of proportional discovery).

[113] See The Sedona Conference, "Commentary on Preservation, Management and Identification of Sources of Information that are Not Reasonably Accessible" (2009) 10 Sedona Conf. J. 281.

[114] *Rules of Civil Procedure*, RRO 1990, O Reg 194, r 30; *Alberta Rules of Court*, Alta Reg 124/2010, Part 5; *Supreme Court Civil Rules*, BC Reg 168/2009, r 7-1; *Court of Queen's Bench Rules*, Man Reg 553/88, r 30; *Rules of Court*, NB Reg 82-73, r 31; *Rules of the Supreme Court*, SNL 1986 c 42, Sch. D, r 32; *Rules of the Supreme Court of the Northwest Territories*, NWT Reg 010-96, Part 15; *Rules of the Supreme Court of the Northwest Territories*, NWT Reg 010-96 (Nu), Part 15; *Nova Scotia*

Canadian courts have repeatedly held that ESI is producible and compellable in discovery.[115] Rules of court make relevancy a prerequisite to production, regardless of the form of record. For example, Part Five, Rule 5.2(1) of the *Alberta Rules of Court*[116] provides that producible records be both relevant and material. The Ontario *Rules of Civil Procedure*[117] provide that every document relevant to any matter in question in the action shall be produced. The British Columbia rules were amended in 2009 to introduce concepts of proportionality and narrow the scope of documentary discovery.[118]

The "reasonable steps" standard calls for a good-faith assessment of what data may be relevant to the claims or defenses in the litigation. Generally, once evidence is in a party's possession and control, they have an obligation to preserve it until trial.[119] 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 re-

---

*Civil Procedure Rules,* Royal Gazette Nov 19, 2008 at r 16; *Supreme Court Rules of Civil Procedure*, Prince Edward Island*,* r 30; *The Queen's Bench Rules*, Sask. Gaz. December 27, 2013, 2684, Part 5; *Rules of Court*, YOIC 2009/65, r 25; *Tax Court of Canada Rules (General Procedure)*, SOR/90-688a, rr 78-91; and *Federal Courts Rules,* SOR/98-106, rr 222- 233.

115 See *Cholakis v. Cholakis*, [2000] MJ No 6 at para 30, 44 CPC (4th) 162 (CanLII) (Man QB): "The plaintiff has satisfied me that the electronic information requested falls within the definition of a document under the Rules and contains relevant information that should be produced. If the defendants . . . wish to provide the information in a format that does not reveal irrelevant information, then it is incumbent upon them to develop a mechanism by which that can be done. The interests of broad disclosure in a modern context require, in my view, the production of the information in the electronic format when it is available."

The general rules requiring documentary production are found at the following sections in the relevant province's rules: *Ontario Rules of Civil Procedure*, RRO 1990, O Reg 194, r 30.02 [*Ontario Rules*]; *Alberta Rules of Court*, Alta Reg 124/2010, Part 5 [*Alberta Rules*]; *British Columbia Supreme Court Civil Rules*, BC Reg 168/2009, r 7-1 [*BC Rules*]; *Manitoba Court of Queen's Bench Rules*, Man Reg 553/88, r 30.02 [*Manitoba Rules*]; *New Brunswick Rules of Court*, NB Reg 82-73, r 31.02 [*NB Rules*]; *Newfoundland and Labrador Rules of the Supreme Court*, SNL 1986 c 42, Sch. D, r 32.01 and 32.04; *Northwest Territories Rules of the Supreme Court*, NWT Reg 010-96, r 219, 225 and 229 [*NWT Rules*]; *Nunavut Rules of the Supreme Court*, NWT Reg 010-96 (Nu) r 219, 225 and 229 [*Nu Rules*]; *Nova Scotia Civil Procedure Rules*, Royal Gazette Nov 19, 2008 at r 16. [*Nova Scotia Rules*]; *Prince Edward Island, Supreme Court Rules of Civil Procedure* [*PEI Rules*] , r 30.02; *Saskatchewan The Queen's Bench Rules*, Sask. Gaz. December 27, 2013, 2684, Part 5 [*Saskatchewan Rules*]; *Québec Code of Civil Procedure*, CQLR c C-25, s 401-403 [*Québec Code*]; *Yukon Rules of Court*, YOIC 2009/65, r 25 [*Yukon Rules*]; *Tax Court of Canada Rules (General Procedure)*, SOR/90-688a, r 78 and 80 [*Tax Court Rules*]; and *Federal Courts Rules* (SOR/98-106), r 222 and 223.

116 *Alberta Rules*, *supra* note 11515.

117 *Ontario Rules*, *supra* note 11515, r 30.02 (1): Every document relevant to any matter in issue in an action that is or has been in the possession, control or power of a party to the action shall be disclosed as provided in rules 30.03 to 30.10, whether or not privilege is claimed in respect of the document.

118 See *BC Rules*, *supra* note 11515.

119 *R. v. Prosa*, 2015 ONSC 3122 (Can LII). Rules in the various Canadian provinces and territories refer to the concept of possession, custody, and control differently. As an example, in Alberta, the term "possession, power, and control" is used. *See* footnote **Error! Bookmark not defined.**.

view of the reasonableness of a party's preservation actions should use as its frame of reference the party's knowledge at the time preservation decisions were made.[120]

Collection of data from social media platforms should be conducted with a view to what is proportionate in the circumstances. Proportionality is the barometer applied to the question of how much time, effort, and expense a party should reasonably have to expend with respect to ESI in light of all relevant factors. Every jurisdiction that has adopted ESI-related rules of procedure that impose affirmative obligations has adopted a proportionality principle. All ESI is potentially discoverable, and parties have a duty to preserve, search, and then produce what meets the relevant test for disclosure. But no party is required to preserve, search, and produce all (or particularly problematic sets of) ESI where to do so would impose costs and burdens disproportionate to the value of the case or the probative value of the evidence in question, taking into account the availability of the same information from other sources and other factors.

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.[121]

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

---

[120] See "Commentary on Proportionality in Electronic Discovery," *supra* note 105, at 151; "The Sedona Canada Principles, Third Edition," *supra* note 41, Comment 3.a; *Culligan Canada Ltd. v. Fettes*, 2009 SKQB 343 at para 87 (reversed on other grounds): "As soon as litigation was threatened in this dispute, all parties became obligated to take reasonable and good faith steps to preserve and disclose relevant electronically stored documents."

[121] See "The Sedona Canada Principles, Third Edition," *supra* note 41, Principle 2 (stating that "in any proceeding, steps taken in the discovery process should be proportionate, taking into account: . . . (v) the costs, burden and delay that the discovery of the ESI may impose on the parties.)

### 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.[122] 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.[123] Social media may also contain data and content, such as video, that cannot be properly collected in the form of static images.[124] In addition, social media outlets use different interfaces to display content, further complicating efforts to create standardized snapshots.[125] 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.[126]

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.[127]

### 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.

---

[122] See Section V, *infra*; *R. v. Mills*, 2019 SCC 22 at paras 53–57 (screenshots of Facebook and email messages admissible and not a breach of privacy); *R. v. Martin*, 2021 NLCA 1 at paras 29, 70–71 (screenshots of Facebook posts were admissible as there was no allegation the screenshot software altered their contents)

[123] See *R. v. Hirsch,* 2017 SKCA 14 at para. 18; Hon. Paul Grimm, Gregory Joseph & Daniel Capra, "Best Practices for Authenticating Digital Evidence" (2016) West Acad. Pub. (discussing circumstances in which static evidence of social media can be authenticated). See also *R. v. Bernard*, 2016 NSSC 358 at para 58 (evidence inadmissible based on the absence of evidence as to the origin of the screenshots); *R. v. Ball*, 2019 BCCA 32 (fact that photographed Facebook messages were admitted without testing their admissibility part of finding of miscarriage of justice).

[124] Depending on the specific type of information that needs to be preserved or collected, videoing/interactive demonstration software that creates a record of the experience of navigating a site may more accurately represent the dynamic nature of the information, including capturing dynamic and nontext postings such as audio and video materials.

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

[126] Circumstantial evidence may enhance authentication, including the presence of photographs, email addresses, and posting dates. See, *e.g., R v. Durocher*, 2019 SKCA 97 at paras 47–50. 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.

[127] For example, Snapchat conversations disappear as soon as they are read unless a screenshot is taken as recognized in *R v White-Halliwell*, 2019 ONSC 597 at paras 70–72.

Facebook, for example, requires a username and password to process a download request, and as a result, this process must generally be carried out by the account user (or someone to whom the user has provided login credentials).[128] 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.[129] This download gives the user copies of all the user's tweets since the account's creation.

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 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.[130]

WhatsApp facilitates conversation history exports from within the application itself. These exports generate a plain-text version of the text communication; however, exports are limited to a maximum number of messages and media (i.e., images and video files) before and after those currently displayed on the phone's screen.[131] These exports, while easy to perform, may not capture the entirety of the conversation, and the generated plain-text file is easy to modify after export.

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.

---

[128] See *Accessing & Downloading Your Information,* online: Facebook Help Ctr. <https://www.facebook.com/help/1701730696756992/?helpref=hc_fnav> (last visited 8 March 2021).

[129] *How to Download Your Twitter Archive,* online: Twitter Help Ctr., <https://help.twitter.com/en/managing-your-account/how-to-download-your-twitter-archive> (last visited 8 March 2021).

[130] *Accessing Your Account Data,* online: LinkedIn Help <https://www.linkedin.com/help/linkedin/answer/50191/accessing-your-account-data?lang=en> (last visited 8 March 2021).

[131] As of August 2020, the export feature is limited to 40,000 messages when exported without media, or 10,000 messages and a selection of most recent images. *How to save your chat history*, online: WhatsApp <https://faq.whatsapp.com/android/chats/how-to-save-your-chat-history/> (last visited 28 August 2020).

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

Several 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 Application Programming Interface (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 content and may generate a message-digest hash for verification of the extracted data.[132]

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.[133] Among messaging applications, Slack also has an API that may allow access to vendors.[134]

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.[135] Twitter provides information through its API on individual users and their tweets.[136]

---

[132] 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* (11 Oct. 2011), online: eDiscovery L. & Tech Blog <http://blog.x1discovery.com/2011/10/11/key-facebook-metadata-fields-lawyers-and-ediscovery-professionals-need-to-be-aware-of>.

[133] 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*, online: X1 <https://www.x1.com/products/x1-social-discovery/> (last visited 7 June 2021).

[134] See*, e.g., Guide to Slack import and export tools,* online: Slack Help Ctr. <https://get.slack.help/hc/en-us/articles/204897248-Guide-to-Slack-import-and-export-tools> (last visited 7 June 2021).

[135] See *Terms of Service,* online: Facebook <https://www.facebook.com/terms.php?ref=p> (last visited 8 March 2021); see also *What Type of Web Data Can You Collect From Facebook?* (17 June 2016), online: Bright Planet <https://brightplanet.com/2016/06/type-web-data-can-collect-facebook/>.

[136] See *Twitter Terms of Service,* online: Twitter <https://twitter.com/en/tos> (last visited 8 March 82021); see also *What Type of Data Can You Get from Twitter* (15 March 2016), online: Bright Planet <https://brightplanet.com/2016/03/what-type-of-data-you-can-get-from-twitter/>.

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. Original Digital Format or Near-Original Digital Format of the Web Content

With the International Organization for Standardization (ISO) 28500 Web ARChive (WARC) standard, it is possible to get an original digital format or near-original digital format file of the collected content of a social media platform. This standard, established by the International Internet Preservation Consortium, uses a WARC file as a container or image for accessed web resources and metadata.[137] 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 platform.

With the original digital format or near-original digital format file capture, the data can be viewed as the content orginally appeared on the social media platform, 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.

To carry out this imaging of the web content, it would be necessary to have the consent of the user.

#### 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 platform. Dynamic capture allows a vendor to identify rele-

---

[137] *ISO 28500:2017 Information and documentation—WARC file format*, online: ISO <https://www.iso.org/standard/68004.html> (last visited 8 March 2021).

vant data in the collaboration site or capture interactive data on the social media platform. 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. 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 circumstances. Selecting the proper approach for review may involve several factors, including whether there is a need to review the data interactively as it appeared on the social media platform 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.[138]

#### a. Small Data Volumes

It may be preferable to review social media content using the original digital format or near-original digital format 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 platform, or over a certain period of time. Available social media and API prod-

---

[138] *Rules of Civil Procedure*, RRO 1990, O Reg 194, r 30.04; *Alberta Rules of Court*, Alta Reg 124/2010, s.5.14; *Supreme Court Civil Rules*, BC Reg 168/2009, r 7-1(15); *Court of Queen's Bench Rules*, Man Reg 553/88, r 30.04; *Rules of Court*, NB Reg 82-73, r 31.04; *Rules of the Supreme Court*, SNL 1986 c 42, Sch. D, r 32.05; *Rules of the Supreme Court of the Northwest Territories*, NWT Reg 010-96, s.225; *Rules of the Supreme Court of the Northwest Territories*, NWT Reg 010-96 (Nu), s.225; *Nova Scotia Civil Procedure Rules,* Royal Gazette Nov 19, 2008 at rr 16.05-16.06; *Supreme Court Rules of Civil Procedure*, Prince Edward Island, r 30.04; *The Queen's Bench Rules*, Sask. Gaz. December 27, 2013, 2684, Part 5-11; *Rules of Court*, YOIC 2009/65, r 25(4); *Tax Court of Canada Rules (General Procedure)*, SOR/90-688a, r 85; and *Federal Courts Rules,* SOR/98-106, r 228. See *Marineland of Canada Inc. v. Demers*, 2017 ONSC 2230 (defendant not required to produce a hard copy of records if publicly available after listing relevant websites in Schedule A of his affidavit of documents); *Schuster v. Royal & Sun Alliance Insurance Company of Canada*, 2009 CanLII 58971 (ON SC) at paras 17–18 (it is beyond the scope of discovery obligations to produce user name and passwords for social medial accounts). 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).

ucts can be used to collect an entire archive or certain categories of information associated with the social media account, such as chat messages, account activity, and multimedia files, making the review experience similar to the experience the user had when uploading or posting content. This functionality could be important in a trademark case, for example, where the way the allegedly infringing mark is displayed throughout a platform and over time is critical.

Parties might alternatively consider obtaining archival downloads of user information from social media accounts, 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.[139] Information may also be difficult to review.[140] 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 case team is most concerned with the text from social media platforms 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 prevents social media data from being reviewed in isolation. This functionality is optimized when social media metadata is available.

---

[139] 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. In one case, a court ordered production of a family computer hard drive to help determine an individual's Facebook usage activity: *Bishop (Litigation Guardian of) v. Minichiello*, 2009 BCSC 358 (B.C. S.C.), leave to appeal B.C.C.A. ref'd 2009 BCCA 555.

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

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 platform. The difficulty in collecting metadata associated with the social media content, combined with other issues such as the tendency of social media postings to incorporate content from external sites, can make using a conventional platform to review social media content difficult or inefficient. As with the ongoing work surrounding the collection of social media content, review platforms are also rapidly evolving to display social media in more intuitive and appropriate formats.

### 2. Production

The same analysis that guides the selection of an appropriate review platform also applies to the production of social media data.[141] 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.[142] Doing so, however, may run afoul of the requesting party's production requests or a desire to produce in a reasonably usable format.[143] The complexities 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 platform. Production in this manner would be consistent

---

[141] Definitions of "document" are found at the following sections in the respective province's rules: *Ontario Rules*, *supra* note 11515, r 30.01; *BC Rules*, *supra* note 115, r 1; *Manitoba Rules*, *supra* note 115, r. 30.01; *NB Rules*, *supra* note 11515, r 31.01; *NWT Rules*, *supra* note 11515, r 218; *Nu Rules*, *supra* note 11515, r 218; *Yukon Rules*, *supra* note 11515, r 1 (8); *PEI Rules*, *supra* note 11515, r 30.01; *Saskatchewan Rules*, Part 17; *Québec, An Act to establish a legal framework for information technology*, RSQ c C-1.1 [*Québec Information Technology Act*], s 3; *Tax Court Rules*, *supra* note 11515, r 78; *Federal Courts Rules*, *supra* note 11515, r 222(1).

[142] See, *e.g.*, *J.C. v. M.C.,* 2014 NBQB 161 at para. 9 (party produced hard copy of a text message conversation at the request of the court).

[143] See *Cholakis v. Cholakis* (2000), 44 C.P.C. (4th) 162 (M.B.Q.B.) (Court ordered production of accounting data in electronic format even though it had already been produced on paper); *Walter Construction (Canada) Ltd. v. Greater Vancouver Sewerage and Drainage District*, 2003 BCSC 1582 (electronic documents ordered to be produced despite documents already being provided in hard copy).

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.

There are different potential responses to this request. One strategy is to give the requesting party access to a copy of the original digital format or near-original digital format file or to certain portions of the API used for collection. Another strategy is for the responding party to produce static images of the pertinent platforms so the requesting party may observe how they appeared. While unlikely to be required to do so by a court, the responding party may choose to grant the requesting party access to the social media account in order to review the content interactively.[144] 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.[145] A responding party exercising this option should consider potential safeguards to be implemented, such as a written agreement with the reviewing party restricting what information can be accessed and reviewed, only permitting access under supervision and only for a limited period of time, and either not sharing login details or immediately changing them after access.

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 U.S. 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. The vendor then ran search terms agreed to by the parties and provided only responsive material to the plaintiff.[146]

---

144 Courts have held it is beyond the scope of discovery obligations to force a party to produce social medial passwords: *Schuster v. Royal & Sun Alliance Insurance Company of Canada*, 2009 CanLII 58971 (ON SC) at paras 17–18.

145 See Section III(D)(8), *supra*.

146 *Pre-Paid Legal Servs., Inc. v. Cahill*, No. 6:2012-cv-0346, 2016 WL 8673142, at *1 (Sept. 30, 2016). For a more common alternative, see *Loblaws Inc. v. Columbia Insurance Co.*, 2019 FC 961 at para 152 (expert using keyword searches of social media accounts to find relevant posts).

## IV. CROSS-BORDER DISCOVERY ISSUES

Parties who seek discovery of information from persons outside of Canada or social media information located in a foreign country should determine whether there are laws that preclude the processing, transfer, or production of social media information. Parties seeking social media information within Canada may consult federal laws focused on the protection of personal data in commercial activities.[147] Personal data may also be protected more broadly by treaty[148] or applicable foreign law outside of Canadian borders.

### A. United States

The U.S. lacks comprehensive, centralized data protection laws. Recently, states such as California, Nevada, and Maine have enacted privacy legislation.[149] More broadly, the U.S. is party to the Hague Convention of the Taking of Evidence Abroad in Civil or Commercial Matters (Hague Evidence Convention). The Hague Evidence Convention allows authorities in one signatory country to obtain evidence located in another signatory country within judicial proceedings by means of a Letter of Request. While Canada is not a signatory to the Hague Evidence Convention, the U.S. has codified the Hague Convention within 28 U.S. Code § 1782. Canadian parties seeking evidence from the U.S. can still achieve this process by securing letters of request or letters rogatory from a Canadian court and applying to a U.S. court for enforcement through Section 1782.

---

147 Federally, the Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5) (PIPEDA) applies to data collection, use and disclosure of personal information by private sector conducting commercial activities across Canada, and employment information of federally regulated organizations. All businesses that operate within Canada and handle personal information that crosses provincial or national borders are subject to PIPEDA. For more information, see Section III.A.1, "Privacy Obligations," *supra*.

148 *Charter of Fundamental Rights of the European Union* (EU), 2000 O.J. (C 364) 1, online: <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 June 2020, out of 55 countries, only five (Ghana, Guinea, Mauritius, Namibia, Senegal) have ratified the treaty. See *African Union Convention on Cyber Security and Personal Data Protection*, June 27, 2014, EX.CL/846(XXV), online: <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>.

149 *California Consumer Privacy Act*, Cal. Civ. Code §1798.100 (West 2018), online: <https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5>, *An Act to Protect the Privacy of Online Consumer Information*, Me. Rev. Stat. Ann.. § 9301 (2019) online: <https://www.mainelegislature.org/legis/bills/bills_129th/billtexts/SP027501.asp>; Nev. Rev. Stat. § 603A (2019) online: <https://www.leg.state.nv.us/NRS/NRS-603A.html>.

### B. Europe

While Canada is not a signatory to the Hague Evidence Convention, it has entered into bilateral treaties with a number of EU member states for judicial cooperation when requesting evidence abroad.[150]

The European Union (EU) provides broad protections of personally identifiable information. Defined broadly, "personal data" includes any information relating to an identifiable individual.[151] Like Canada, the EU views the privacy of "personal data" as a "fundamental human right."[152] An even stricter standard of protection applies to sensitive personal information such as racial or ethnic origin, religious beliefs, and political opinions.[153]

The General Data Protection Regulation (GDPR) is the basis of EU data protection law. The GDPR allows for data transfers to countries like Canada, whose legal regime was found by the Commission to provide an "adequate" level of personal data protection.[154]

The GDPR broadly defines the "processing" of data and proscribes the processing of personal data unless an exception applies. Processing includes "collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."[155] 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,"[156] such processing could violate the GDPR.

---

150 *Response Canada to 2008 Evidence Questionnaire*, online: <https://assets.hcch.net/upload/wop/2008canada20e.pdf>.

151 *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*, 2016 O.J. (L119) 1, at art. 4(1) [*GDPR*], online: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN> (prohibiting the processing of such personal information barring narrow, delineated exceptions).

152 *Charter of European Union*, *supra* note 148, at art. 8; Section 8 of the *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11, s 91(24).

153 *GDPR*, *supra* note 151, at art. 9.

154 *Ibid.*, at art. 45; *Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act* (notified under document number C(2001) 4539) (2002/2/EC) at art 1, online: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02002D0002-20161217&from=EN>.

155 *Ibid.* at art. 2.

156 *Ibid.* at art. 6.

While the GDPR applies to all member states, there are several provisions that allow member states to independently interpret domestic data protection legislation.[157] Canadian parties looking to control and process personal information from the EU should consult specific member state legislation in addition to the GDPR to determine whether additional steps are required to maintain compliance.

### C. Asia

Canada is a founding member of the Asia-Pacific Economic Cooperation (APEC) and a member of APEC's Cross-Border Privacy Rules System (CBPR). The APEC Privacy Framework sets out nine guiding principles related to privacy.[158] Similar to both Canada and the EU, the APEC Privacy Framework takes a broad view of privacy and employs stringent protections. CBPR establishes a privacy framework for the transfer of personal data by participating countries.[159] Parties seeking cross-border discovery of social media must satisfy the CBPR 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 *Commentary on Discovery of Social Media in Canada*. The Sedona Conference's *Practical In-House Approaches for Cross-Border Discovery & Data Protection*[160] and *International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition)*[161] 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.

---

[157] For example, i*bid.* at art. 6(2).

[158] See *APEC Privacy Framework* (2015), online: Asia-Pacific Economic Cooperation <https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)>.

[159] *Cross Border Privacy Rules System*, online: <http://www.cbprs.org/> (last visited June 21, 2020).

[160] 17 Sedona Conf. J. 397 (2016).

[161] See The Sedona Conference, "International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition)" (January 2017), online: <https://thesedonaconference.org/publication/International_Litigation_Principles>.

## V. AUTHENTICATION OF SOCIAL MEDIA EVIDENCE

The Canada Evidence Act[162] (CEA) and most provincial evidence statues contain provisions that relate to the admissibility of "electronic evidence." As will be seen below, these provisions only concern authentication and the application of the best evidence rule as they relate to electronic evidence. They do not affect any rule of law relating to the admissibility of evidence.[163] While the evidence statutes' requirements are mandatory,[164] the ultimate admissibility of the evidence depends on the purpose for which it is tendered and any related general law of evidence. Failure to attend to the evidence statutes' requirements has resulted in evidence ruled inadmissible even though the requirements would have been easily met.[165]

Subsections 31.1 to 31.8 of the CEA apply to "electronic documents," which are defined as: "data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device. It includes a display, printout or other output of that data."[166] This broad definition would include copies of any documents stored in a computer or smartphone, including social media evidence such as Facebook posts, emails and other forms of electronic communications.[167]

The provisions of the Canada Evidence Act that concern electronic documents modify the common law rules of authenticity and "best evidence" to address the unique nature of electronic evidence.[168]

### A. Authentication

The most fundamental rule governing the admissibility of any form of documentary evidence is that the document must be authenticated.[169] This requires the person proffering an item into evidence to give evidence that the item is what it purports to be. At common law, this requirement was met by providing "some evidence" to establish that fact. It is a low standard that can be met by either direct or circumstantial evidence.[170]

---

[162] *Canada Evidence Act*, R.S.C. 1985, c. C-5.

[163] *Ibid.*, s. 31.7.

[164] *Richardson v. R.,* 2020 NBCA 35 at para 32.

[165] *R. v. Donaldson*, 2016 CarswellOnt 21760, [2016] O.J. No. 7153, 140 W.C.B. (2d) 513, at paras 3–4 and 22. See also *R. v. Ball* 2019 BCCA 32 at para 86 and *R. v. Bernard* 2016 NSSC 358 at para 40.

[166] *Canada Evidence Act*, *supra* note 162, s. 31.8.

[167] *R. v. Ball,* 2019 BCCA 32 at para 67; *Richardson v. R.*, 2020 NBCA 35 at para 22.

[168] *R. v. Avanes et al.,* 2015 ONCJ 606 at para 55.

[169] *McWilliams' Canadian Criminal Evidence*, 5th ed, 24:40:10.

[170] *R. v. C.B.*, 2019 ONCA 380, at para 66.

Section 31.1 of the CEA codifies the authenticity requirement. It provides that the person "seeking to admit an electronic document has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic document is what it is purported to be." The Court of Appeal for Ontario has interpreted the words "evidence capable of supporting" as evidencing a low threshold.[171] It is important to keep in mind that under this low threshold, a document may be authenticated even though there are competing claims as to the document's "genuineness." In other words, if the party offering the document into evidence provides evidence capable of supporting that it is genuine, the test will be met regardless of the strength of the contrary view. This is because disputes about authenticity are better resolved at the end of the case with an appreciation of all the evidence.[172] The integrity or reliability of the electronic document is not open to attack at the authentication stage of the enquiry.[173]

Section 31.1 does not limit how and by what means authenticity may be established.[174] The test would be met if witness presented with an electronic document was able to articulate some basis for authenticating it as what it purports to be. In *R. v. K.M.,*[175] for example, the Court held that the authentication requirement had been met when a witness testified that a printout of Facebook messages exchanged with the accused "reflected what he could see on the computer screen [. . .] after logging on to his Facebook account."[176]

The authenticity requirement may also be met by providing circumstantial evidence that the document is what it purports to be. For example, in a case where the police seized password-protected Blackberries, which required specialized expertise to extract their contents, the Ontario Court of Justice held that the authenticity requirement had been met when the PIN numbers on the extracted messages matched the PIN numbers on the Blackberries themselves.[177]

Another useful manner of meeting the authenticity requirement through circumstantial evidence is through the common law "reply letter" doctrine. It holds that correspondence can be authenticated as having been sent by an individual by showing that it is a reply to a letter sent to that individual.[178] As a matter of logic, the same should hold true for text messages and emails. If a person sent a text

---

171 *R. v. S.H.* 2019 ONCA 669 at para 25.

172 David M. Paciocco, "Proof and Progress: Coping with the Law of Evidence in a Technological Age" (2013) 11 C.J.L.T. 181 at 197.

173 *R. v. Hirsch,* 2017 SKCA 14 at para 18.

174 *R. v. C.B.,* 2019 ONCA 380, at para 68; *R. v. Hirsch*, 2017 SKCA 14 at para 18.

175 2016 NWTSC 36.

176 *Ibid,* at paras 16 and 36.

177 *R. v. Arvanes et al,* 2015 ONCJ 606 at paras 66–68.

178 Paciocco, *supra* note 172, at 197.

or email to the email address or phone number believed to be linked with the intended recipient, evidence of a response purportedly from that person affords some evidence of authenticity.[179]

### B. "Best Evidence" Requirement

At common law, the best evidence rule required a party to produce the best evidence available. The rule sought to avoid fraud or forgery[180] and is premised on the notion that forgery would be easier to detect on an original document than on a copy.[181] This rule has declined in importance, and its remnants in Canada states that "if an original document is available in one's hands, one must produce it."[182] The concept of an original is not readily applied to electronic documents.[183] However, the Canada Evidence Act's broad definition of "electronic document" embraces any data that is translated from computer code and can be read or perceived, including a display or printout.

Most provinces have passed legislation that provides guidance for the use of electronic means for creating and managing records.[184] Currently, legislation across Canada provides a means to facilitate the admissibility of ESI in the courts, including the establishment of evidentiary presumptions related to integrity of electronic information and procedures for introducing such evidence and challenging its admissibility, accuracy, and integrity. The legislation generally does not modify any common law or statutory rule related to the admissibility of records, except the rules relating to authentication and best evidence.[185] Section 31.2 of the Canada Evidence Act provides four different ways of satisfying the best evidence rule. As will be seen below, these "best evidence" provisions provide assurance that "the document provided to the Court is the same as the one that was input into the computer" and are therefore an "adjunct to authenticity."[186] Each of the statutory conditions described below may be proven by calling a witness or by filing an affidavit under subsection 31.6.

---

179 *R. v. C.B.*, 2019 ONCA 380, at para 68.

180 *R. v. After Dark Enterprises Ltd.*, (1994) ABCA 360 at para 9.

181 *R. v. Sampson,* 2020 BCPC 27 at para 23.

182 Paciocco, *supra* note 172, at 199.

183 *R. v. Hirsch,* 2017 SKCA 14 at para 22.

184 The Yukon, Prince Edward Island, Ontario, Newfoundland, Nova Scotia, and Nunavut have respectively passed: *Electronic Commerce Act*, RSY 2002, c 66; RSPEI 1988, c E-4.1; SO 2000, c 17; SNL 2001, c.E-5.2; SNS 2000, c 26; and SNu 2004, c 7. Alberta, New Brunswick, British Columbia, and the North West Territories have similar legislation under the title of the *Electronic Transactions Act*, found respectively at: SA 2001, c E-5.5; RSNB 2011, c 145, SBC 2001, c 10, and SNWT 2011, c 13. Manitoba's legislation is titled: *Electronic Commerce and Information Act*, CCSM 2000 c E55. Saskatchewan's legislation is entitled: *Electronic Information and Documents Act*, SS 2000, c E-7.22. Québec's legislation is: *Québec Information Technology Act*, *supra* note 14141.

185 *See, e.g.*, *Evidence Act*, RSO 1990 c E.23, s 34.1 [*Ontario Evidence Act*]; *Québec Information Technology Act*, *supra* note 14141, s 5, 6 and 7.

186 Paciocco, *supra* note 172, at 200; see also *Richardson v. R.*, 2020 NBCA 35 at para 28.

### 1. Proving the integrity of the system that recorded or stored the document

Subsection 31.2(1)(a) provides that the best evidence rule is satisfied on proof of the integrity of the electronic document system by or in which the electronic document was recorded or stored. The standard of proof is on the balance of probabilities and requires the party seeking admission to establish that it is more probable than not that the system had integrity.[187]

Proving that the system had integrity requires one to establish that the electronic document system had the capacity to accurately record, maintain, and display the data.[188] This can be established through direct evidence about the operation of the system. For example, the Court was satisfied that a computer system had integrity and admitted Facebook messages when one of the parties testified about the steps she took to engage in a chat and testifying that the system worked in the usual way.[189] If the opposing party admits to have authored postings on social media platforms that are at issue, integrity of the computer system will have been proved.[190]

### 2. Proving the integrity of the system though one of the presumptions of integrity

A party may rely on one of the presumptions contained in subsection 31.3 to prove the integrity of the computer system. Different standards of proof apply to the various presumptions described below:

#### a. By providing evidence capable of proving that the system was operating properly, or if it was not, that it did not affect the integrity of the documents

Subsection 31.3(a) sets a low threshold of proof by merely requiring "evidence capable of supporting a finding" that the computer system was operating properly.[191] The evidence can be direct or circumstantial. Evidence that an email was received on a device such as a computer or a phone and that it was readable and coherent would meet this requirement.[192] The Court of Appeal for Ontario held that the text messages extracted from a person's smartphone that were in "chronological order and customary format, demonstrating coherent conversations between a sender and a recipient"

---

187 Paciocco, *supra* note 172, at 202; *see also Richardson v. R.*, 2020 NBCA 35 at para 32.

188 Paciocco, *supra* note 172, at 202.

189 *R. v. Soh*, 2014 NBBR20 at paras 28–30.

190 *Holden v. Hanlon*, 2019 BCSC 622 at para 50.

191 *Canada Evidence Act*, *supra* note 162, ss. 31.3(a); *R. v. S.H.* 2019 ONCA 669 at para 25.

192 Paciocco, *supra* note 172, at 202.

could support a finding that the smartphone was working properly.[193] The fact that the content of the text messages is congruent with other evidence at trial can also support a finding that the device is working properly.[194]

#### b. By establishing that the electronic document was recorded or stored by an adverse party.

Subsection 31.3(b) provides that the integrity of the system that stored or recorded an electronic document may be proved by establishing that the documents was recorded or stored by an adverse party. The fact underlying this presumption (the document was stored or recorded by an adverse party) must be proved on the balance of probabilities. This presumption is based on the notion that the opposing party who stored or recorded the document is in the best position to explain if the computer system was unreliable.

#### c. Presumption of integrity if the electronic document is a business record

Subsection 31.3(c) provides that the system that stored or recorded the electronic document has integrity if it is established that the document was recorded or stored in the usual and ordinary course of business by a person who is not a party and who did not record or store it under the control of the party seeking to introduce the document.[195] This presumption could be used where an internet service provider produces text messages as a result of a production order. Duplicate receipts stored in a pharmacists' computer were found to meet this presumption.[196]

### 3. Presumption of integrity based on electronic signature

Section 31.4 provides that regulations may be made establishing evidentiary presumption in relation to secure electronic signatures. The Secure Electronic Signature Regulations[197] establish such a presumption. A document signed with a "secure electronic signature" (meeting certain defined technical requirements) will be presumed to have been signed by the person identified in the digital signature certificate.[198]

---

193 *R. v. S.H.* 2019 ONCA 669 at paras 24–27.

194 *R. v. S.H.* 2019 ONCA 669 at para 27.

195 *Canada Evidence Act*, *supra* note 162, ss. 31.3(c).

196 *R. v. Piercey*, 2012 ONCJ 500 at paras 26–27.

197 SOR/ 2005-30.

198 *Ibid* at s. 5.

### 4. Printouts that have been manifestly and consistently relied upon

The final method of meeting the best evidence requirement is the presumption, contained in section 31.2(2), that applies to printouts that have been "manifestly and consistently acted on, relied on or used as a record or the information recorded or stored in the printout."

# 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 counsel's use of social media.

## A. Counsel Duty of Technology Competence

The Federation of Law Societies of Canada's Model Code of Professional Conduct ("The Code") require lawyers to understand the impact and consequences of technology use by clients and counsel. The Model's duty of technology competence requires that lawyers develop an understanding of, and ability to use, technology relevant to the nature and area of the lawyer's practice and responsibilities.[199] The Code sets out statements of principle followed by exemplary rules and commentaries. The Code is a model that the individual provinces and territories may or may not incorporate into their own codes.

## B. Counsel's 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 platforms, 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. These ethical violations could come in the form of impersonation or pretext when attempting to gain access to information that is not publicly available (for example, by "friending" a party's social media account). 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. 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

---

[199] The Federation of Law Societies of Canada, *Model Code of Professional Conduct*, as amended 19 October 2019, online: <https://flsc.ca/wp-content/uploads/2019/11/Model-Code-October-2019.pdf>.

be considered harassing, burdensome, or otherwise improper. Such "frivolous" requests may thus violate the principle of proportionality and could also be grounds for discovery sanctions.[200]

[200] Law Society of Ontario, *Rules of professional conduct*, rule 5.1-3.1(c); Law society of Prince Edward Island, C*ode of professional conduct*, rule 5.1-3.1(c) ("a lawyer, when acting as an advocate . . . (c) shall not make frivolous requests for the production of documents or make frivolous demands for information at the examination for discovery."). Other rules of professional contain broader statements suggesting counsel avoid and discourage resort to frivolous or vexatious behaviour.

## VII. CONCLUSION

While the *Commentary on Discovery of Social Media in Canada* offers insightful guidance on social media discovery issues as they stand in 2021, 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.