ARTICLES

# Social Media Content: What Is It and How Do I Use It at Trial?

By Marie V. Lim – September 7, 2018

Most lawyers are familiar with the concept of e-discovery: the preservation, collection, and production of electronically stored information (ESI). More often than not, when the term "ESI" arises, emails are the first items that come to mind. Other electronic documents, such as Word and Excel files, are often considered next. These types of documents do not constitute the entire ESI universe, however. As technology changes, so does the ESI universe. The use of social media for both personal and business reasons has grown in recent years. For that reason, requests for social media content, in addition to emails and other electronic documents, should be standard in any litigation. What follows is a brief overview of how to deal with social media content from preservation through trial.

**What Are Social Media?**

Social media platforms are electronic forms of communication in which users share information via websites and applications (e.g., Facebook, LinkedIn, Twitter, Instagram). Depending on the user's privacy settings, this content can be made available to the general public or only to those individuals with whom the user wishes to share the information. Social media content may be used in litigation in a variety of ways—among them, supporting or disproving defamation claims; establishing physical, emotional, or mental state; or determining where a person may have been at a certain time.

**Is Social Media Content Discoverable?**

Federal Rule of Civil Procedure 34 governs the production of ESI, which includes "writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations." Social media content can take on any of the forms listed. *See* *D.O.H. ex rel. Haddad v. Lake Cent. Sch. Corp.*, No. 2:11-CV-430 (N.D. Ind. Jan. 15, 2014); *Forman v. Henkin*, 30 N.Y.3d 656 (2018). Therefore, it is discoverable but only if relevant as specified under Federal Rule of Civil Procedure 26(b)(1).

Also, Federal Rule 34 requires the production of ESI within a party's "possession, custody, or control." It is important to determine where social media content resides and whether it is actually the user who has possession, custody, or control of this content. When it comes to paper documents, it is fairly easy to determine who "owns" the documents. With social media, that determination isn't so simple. Arguably, the content resides on the network server of the social media site. After all, the site itself is the one that is hosting the data. However, issuing subpoenas to social media sites is fruitless because they will not produce data without the user's consent. *See* *Crispin v. Christian Audigier Inc.*, 717 F. Supp. 2d 965 (C.D. Cal. 2010); *Romano v. Steelcase Inc.*, 907 N.Y.S.2d 650 (N.Y. Sup. Ct. Suffolk Cty. 2010).

An alternative approach is to seek production of the social media content directly from the user, given that he or she controls it. In *Gatto v. United Air Lines, Inc.*, No. 10-CV-1090-ES-SCM

(D.N.J. Mar. 25, 2013), the court held that "Plaintiff's Facebook account was clearly within his control, as Plaintiff had authority to add, delete, or modify his account's content."

Furthermore, one must not circumvent procedural rules in order to obtain social media content. For example, an attorney (or legal support staff) may not try to gain access to a social media platform, such as Facebook, by setting up a fake account and attempting to "friend" the target. Several bar associations, such as New York (Social Media Ethics Guidelines (May 11, 2017)) and New Hampshire (Ethics Comm. Advisory Op. 2012-13/05), have issued guidelines and opinions stating that such actions are deceptive and unethical.

**How Do I Preserve and Collect Social Media Content?**
Preservation can be accomplished in a number of ways. First, avoid spoliation claims by ensuring that litigation hold notices specifically address the preservation of social media content. Parties should be instructed not to delete content from their social networking accounts. Doing so may result in sanctions. See *Allied Concrete Co. v. Lester*, 736 S.E.2d 699 (Va. 2013).
Some websites, such as Facebook and LinkedIn, allow users to download an archive of their account for free. If this feature is not available, you should consider using tools specifically designed for archiving and collecting social media, such as X1 Social Discovery or Nextpoint. Archiving tools are the best way to preserve social media because they preserve not only visible content but also the underlying associated metadata. Reaching for the print screen button may seem tempting, but think twice before doing so. Screenshots capture only images of the content, not metadata that may be important depending on your case and part of your production obligations.

**In What Format Do I Produce Social Media Content?**
Address production format with opposing counsel early on in your case. If the parties agree that metadata are not important, they may agree to produce screenshots only. If metadata will be an issue, the parties may agree to produce files in native format or as static images along with corresponding metadata contained in a separate file. It is important to know the export features of your archiving tool before agreeing to produce in a certain format.

**How Do I Authenticate Social Media Content for Use at Trial?**
Federal Rule of Evidence 901 requires a proponent to "produce evidence sufficient to support a finding that the item is what the proponent claims it is." Generally, this requirement is satisfied with the testimony of a witness or forensic expert. However, such extrinsic evidence is unnecessary for the self-authenticating items specified in Federal Rule of Evidence 902, such as business records and public records, and now ESI, pursuant to amendments that took effect December 1, 2017. Rule 902 was amended to address the ever-changing ESI landscape and to streamline the authentication process. Under the new amendments, self-authenticating evidence now includes the following:

(13) Certified Records Generated by an Electronic Process or System. A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11).

(14) Certified Data Copied from an Electronic Device, Storage Medium, or File. Data copied from an electronic device, storage medium, or file, if authenticated by a process of digital identification, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent also must meet the notice requirements of Rule 902(11).

Note that self-authentication for both of these items substitutes written certification for the live testimony that may have been required by Rule 901. Certification under Rule 902(13) should address the accuracy of the electronic process by which a record was generated (e.g., operating system registries and logs). Certification under Rule 902(14) relates to a file's hash value, which is essentially a digital fingerprint (e.g., a unique sequence of numbers and letters generated by a computer algorithm) that will change if the original copy has been altered. In addition to these certifications, notice requirements under Rule 902(11) must be met in order to give the adverse party an opportunity to inspect and possibly challenge the records or data.

Of course, the parties may choose to bypass all of these steps by entering into stipulations regarding authenticity.

**What about Hearsay Issues?**
Authentication of social media content does not necessarily mean that it is admissible. When a statement is made via social media, hearsay issues will arise when the one who made the statement is unavailable as a witness at trial. The court in *Lorraine v. Markel American Insurance Co.*, 241 F.R.D. 534 (D. Md. May 4, 2007), recognized admissibility issues relating to ESI and that

> to properly analyze hearsay issues there are five separate questions that must be answered: (1) does the evidence constitute a statement, as defined by Rule 801(a); (2) was the statement made by a "declarant," as defined by Rule 801(b); (3) is the statement being offered to prove the truth of its contents, as provided by Rule 801(c); (4) is the statement excluded from the definition of hearsay by rule 801(d); and (5) if the statement is hearsay, is it covered by one of the exceptions identified at Rules 803, 804 or 807.

Id. at 562–63.

ESI, including social media content, is not treated differently under the Federal Rules of Evidence. *See United States v. Browne*, 834 F.3d 403 (3d. Cir. 2016).

**Conclusion**

Social media usage is ever-expanding. If such content has not already made an appearance in one of your cases, it is more likely than not that it will in the near future. Be prepared to deal with social media content by knowing how to preserve it, collect it, and use it at trial.

*Marie V. Lim is an e-discovery attorney at Novack and Macey LLP in Chicago, Illinois.*