DISCOVERY OF SOCIAL MEDIA DATA

By Viggo Boserup, Esq.

The digital revolution has caused tremendous growth in the volume of documents stored and collected electronically. It has also caused the creation of new sources of digital data, one of the most significant of which is social media. As a direct outgrowth of mobile and Web-based technologies providing the basis of interactive communication, individuals and whole communities are able to share, discuss and modify user-generated content. The result thus far includes sites such as Facebook, LinkedIn, Twitter, Instagram, Snapchat and many others.

More Devices and More Data

A quick look at the statistics shows a surprisingly rapid rate of adoption of technologies allowing greater access to interactive communication. More than 87 percent of Americans own cell phones, with 46 percent owning smartphones. In July 2011, it was predicted that in five years, smartphones and tablets would reach 1 billion in sales. Instead, just 18 months later, sales reached 2.2 billion. These devices are capable of holding vast amounts of data, including text messages concerning competition, products, colleagues, confidential documents, GPS data and the like. The billions of devices constitute a vast source of discoverable evidence. In response to the proliferation of devices, employers have increasingly permitted employees to bring their own devices ("BYOD") to use at work. The result has been that employees now work at home and other places far removed from the office. Thus, the employer has lost some degree of control over the creation and transmission of company data.

Different but Discoverable

While social media data has vastly increased, the very nature of social media itself often serves as a deterrent to counsel as they consider potential sources of electronically stored information ("ESI") for purposes of discovery. Social media is still frequently viewed as a mysterious area that counsel rarely use, much less understand. The result is often that counsel are reluctant to engage in discovery in social media. The normal obstacles include the technical barrier, concerns over privacy and the rapidly changing nature of social media, with new sites routinely popping up on the social media landscape. The fact is, however, that it can be discoverable under the same rules governing other discovery—if the information being sought is reasonably calculated to lead to the discovery of admissible evidence.

Unique Qualities of Social Media

Initially, counsel need to determine the type of information likely to be at issue because each social media site typically contains identifiable types of information. For example, Facebook, Twitter and Instagram are most likely to contain personal or company photos, have status messages and hold online conversations; LinkedIn is more likely to contain contact and relationship information among business persons; and Box, Dropbox and Yammer are more likely to contain proprietary or confidential company information posted by employees. Counsel also need to be mindful of concerns over privacy. It is important to avoid overly broad requests for information that may invade an individual's right to privacy. Recent court decisions also make it clear that counsel need to determine that the information is not available though public resources in order to effectively counter an argument regarding invasion of right to privacy.

This article was originally published by LAW.COM and is reprinted with their permission.

Finally, social media sites are constantly evolving. The types of information available today will change from year to year. Moreover, sites frequently provide their users with new ways of communicating information with others. Thus, it is important for counsel to stay abreast of new developments in social media.

Conducting Discovery

Having determined that there may be information on social media possibly relevant to a case, counsel need to approach the discovery process differently from other e-discovery. The technical architecture of social media data, which is cloud-based, is different from that of other ESI. Thus, traditional collection tools may not be effective for searching, preserving and collecting social media data. The proper management of discovery in social media requires that metadata is preserved for indexing and searching. Likewise, collection methods must be designed to facilitate significant culling. Secondary and other layers of security must be determined and accommodated. It is essential that the review tool provides a wide variety of formats to allow for a review of data alongside other ESI. Without the proper context consisting of the issues in the case and other ESI, relevant information can be easily overlooked due to the nature of social media data, which is by its nature highly abbreviated with jargon, emoticons and other rapidly evolving shorthand expressions. Thus, it is essential to keep in mind the full and complete context of all social media.

Admissibility of the Evidence

The use of social media data as evidence in a case is subject to traditional rules of evidence. The process of authentication is greatly facilitated by a collection that has been conducted in accordance with best practices technology. That includes chain-of-custody with preservation of all associated metadata. Collection tools should provide for the automatic generation of MD5 hash values at the time of collection. Such tools are far beyond the capacity of the social media sites themselves. For example, Facebook provides a self-collection mechanism, but it offers no hash values and no content from users to friends, such as those friends' "walls," and collects only some metadata. Twitter offers even less, with no self-collection mechanism and no export feature.

To determine admissibility of social media data, counsel need to consider the same elements that apply to other forms of evidence, such as relevance, authenticity, hearsay, original writing rule and the probative value versus unfair prejudice. The problem with social media is how to determine if the offered evidence is legitimate evidence. A Facebook post or email message can in fact be created by someone other than the named sender. Thus, three questions must be answered: 1) What was on the website; 2) does the exhibit or evidence accurately reflect it; and 3) is it attributable to the owner of the site. Those questions are answered by using some of the steps in Federal Rules of Evidence ("FRE") 901: Ask the purported creator if (s)he created the site and the posting; search the creator's computer; obtain information from the website that links the creator and the poster to the site and the posting. [1]

In the leading case of *Lorraine v. Markel American Insurance Co.*, Judge Paul Grimm laid out a concise statement of the many ways in which digital data can be authenticated. He stated that the court must first apply FRE 104 to determine if a jury could reasonably find that the evidence is authentic. If so, it is admitted, and the objecting party has a higher burden of showing that it is in fact a fake.

As the technology has evolved, so has the law. The Federal Rules themselves provide the basis for dealing with digital evidence from the Internet as effectively as they have for other types of traditional evidence. Provided that counsel understand the technical characteristics of digital evidence from the Internet and the options for collecting the date while preserving its integrity, admissibility of the evidence can be approached in a straightforward and comprehensive manner. ■

[1] FRE 901 provides methods of authenticating digital evidence from the Internet as follows: 901 (b)(1) Evidence from someone with personal knowledge—usually the owner of a page; 901(b)(3) Expert or comparison—usually a forensic expert; 901(b)(4) Distinctive characteristics, such as hash values; 901(b)(9) System or process producing reliable results; 901(b)(7) Public records or official publications.

Viggo Boserup, Esq., CEDS, *is a JAMS neutral based in Southern California. In addition to more than 20 years as a fulltime mediator and arbitrator, Viggo serves as special master and referee in a number of cases involving electronic discovery. He is certified as an Electronic Discovery Specialist by the Association of Certified Electronic Discovery Specialists (ACEDS). He can be reached at vboserup@jamsadr.com or for more information, please visit www.jamsadr.com/boserup.*