MANAGING AND COLLECTING SOCIAL MEDIA FOR

Understanding the fundamentals of social networking services, the tools for managing, collecting, and authenticating information they contain, and the way to scope collection efforts can help organizations avoid evidentiary and authentication pitfalls.

Lauren A. Allen, J.D., PMP; and Michael C. Wylie, J.D.

Social networking services (SNS) are now an entrenched form of business and personal communication that requires the attention of records and information management (RIM) professionals and attorneys.

As described by U.S. Magistrate Judge Kristin Mix (District of Colorado) in "Discovery of Social Media" in *The Federal Courts Law Review,* Vol. 5, Issue 2, *social media* includes [internal citations omitted] "'web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system.'"

This description includes the current array of *SNS types*: blogs, micro-blogs, wikis, web, video sites, and other new and evolving methods, as well as the most commonly used SNS: Twitter, Facebook, Google+, LinkedIn, Pinterest, YouTube, and Foursquare.

Ubiquity of Social Media

Organizations, both public and private, are embracing SNS.

In the private sector, a benchmark report from social media management company Spredfast, *Q2 2012 Social Engagement Index,* indicates that companies average 29 internal users of 51 accounts across an average of three SNS.

In an example from the public sector, as listed on the U.S. Navy's *Social Media Directory*, some 672 organizations within the Navy alone have one or more SNS presence.

Numbers for SNS use by individuals are no less staggering. For example, in the October 4, 2012, online *Newsroom,* Facebook founder and CEO Mark Zuckerberg headlined a posting with "One Billion People on Facebook."

Similarly, according to Nielsen's *State of the Media: The Social Media Report 2012*, the total number of minutes spent on SNS by users on mobile and PC devices increased 21% between July 2011 and July 2012.

Legal Implications of Social Media

With the rise in personal and professional use of SNS, RIM professionals and attorneys are increasingly required to address social media in both compliance and litigation. But, because social media evolved quickly – and to a large extent is still evolving – and because it is hosted in the amorphous cloud, these professionals are often unaware which properties of social media information are valuable as evidence.

As a result, organizations, attorneys, courts, and regulators are all grappling with the legal and practical implications of retaining, collecting, managing, and presenting social media information in a litigation context.

U.S. Courts, Agency Provide Guidance

According to a blog and lists published on the website of X1 Discovery, an e-discovery and enterprise search solutions provider, more than 900 court cases in the past two years addressed evidence from SNS. Cumulatively, these cases leave little doubt that the standard discovery framework – and resulting records management requirements – apply to social media in the same way they apply to myriad other electronic evidence.

Similarly, *The Sedona Conference® Primer on Social Media,* published in December 2012, notes that the U.S. Financial Industry Regulatory Authority, Securities and Exchange Commission, Federal Trade Commission, and Food and Drug Administration have all issued guidance on social media use in their respective regulated industries.

Keys for Managing Social Media

Social media, like cloud-based e-mail and network infrastructure solutions, presents unique challenges in terms of monitoring, collecting, and managing the information as it resides on third-party network infrastructure and outside an end user's or organization's control.

To effectively manage social media information and ensure that organizations remain in compliance with their obligations during dis-

E-DISCOVERY

covery, attorneys and RIM professionals need to:

1. Understand the types of information available from social media sources and determine what information is possibly relevant for monitoring and collecting
2. Identify where to get the relevant information when it is necessary
3. Determine how secure the relevant social media is
4. Select an appropriate collection or monitoring tool based on the return on investment – i.e., balance the value of retrieving or maintaining the information with the cost of collecting or maintaining it in a particular manner

1. Understand Types of SNS Information

The most basic requirements of RIM professionals and attorneys are to understand the information available via social media and how such information can be relevant.

The potentially discoverable data types on SNS are the same as on other web pages. Social media's evidentiary value stems from the facts that the data originates with users, and it is arranged based on interactions between users.

User activity on general purpose SNS, such as Facebook and Google+, falls within four categories: profile pages, posts, tags, and private messages. While many of the services use varying nomenclature for features, they have substantially similar functionality.

In her article "Understanding and Authenticating Evidence from Social Networking Sites" in the Winter 2012 issue of *Washington Journal of Law, Technology & Arts*, Heather Griffith provides a short but straightforward description of social media interaction on Facebook and MySpace. More detailed descriptions can be found in Mix's article and in detailed help information written by individual SNS providers.

2. Identify Where to Collect Social Media

In a civil context, the level of information any monitoring or collection tool can reach is constrained by the type or level of access an attorney or records manager has to a target account. Therefore, the second requirement in collecting social media is determining the pathway that allows the collection of the greatest amount of information.

Because social media is hosted on geographically diverse servers and often uses cloud technology, there are effectively four potential sources for social media: the social media provider, the account holder, third-party access, and indirect access.

Most SNS providers claim they are prohibited under U.S. federal law, specifically the Stored Communications Act, from disclosing user content in response to a civil subpoena. (See sidebar "The U.S. Legal Framework for Social Media in Court.") While providers are not prohibited from providing basic user information in civil litigation, the SNS providers' claim means that options for lawyers and RIM professionals to access social media content are limited to access as an account holder, third-party access, or indirect access.

Account Holder Access: *Access as an account holder* requires that a user, adverse party, or agent accesses a social media site via the user's profile username and password or other means of identity verification. With respect to discovery of a non-business account, there are only two ways to get direct access through the account holder in a civil

The U.S. Legal Framework for Social Media in Court

Social media information is useful evidence in many types of legal claims, including employment law claims, Federal Trade Commission violations, intellectual property infringement matters, breach of contract cases, and insurance fraud. Use of social media did not change the applicable U.S. Federal Rules of Evidence (FRE) or the U.S. Federal Rules of Civil Procedure (FRCP).

Discovery

According to FRCP 26(b)(1), parties may obtain discovery over any "non-privileged," "relevant" information, and discovery requests must only be "reasonably calculated to lead to the discovery of admissible evidence." Relevance and privilege are defined by the FRE.

Admissibility

In federal court, admissibility of social media evidence usually hinges on the outcome of FRE Rule 403, balancing the probative value of evidence against the danger of unfair prejudice, usually the right to privacy. Note that many state courts, including those in Pennsylvania and New York, have expressly stated that there is no expectation of privacy on SNS.

Authentication

The most litigated aspect of social media is authentication. FRE Rule 901(a) governs authentication of social media evidence. The ease with which social media information can be manipulated, the manner in which social media information is created, and the way in which it is stored raise novel issues concerning its veracity.

Stored Communication Act

As interpreted by several SNS, the Stored Communications Act has been deemed to prohibit SNS providers from releasing anything more than basic user information pursuant to civil subpoena. However, the act does not prohibit users from providing the information themselves, and users can still be subpoenaed and compelled to release social media information in a civil suit.

case – through an agreement with an opposing party or by court order.

Barring evidence of spoliation, a court is unlikely to order a user to hand over access information to an entire profile or account. However, by limiting the scope of the information requested and by using appropriate software or methods, attorneys may be able to convince the court or opposing counsel that the request is relevant and reasonable.

An employment relationship may create additional methods of account holder access to an account. For instance, an account may be a business account to which the employer has access through a second employee or to which an employer has direct access under terms of an employment contract.

In some states, an employer may also require social media access information as a prerequisite to employment. However, according to the National Conference of State Legislatures online posting "Employer Access to Social Media Usernames and Passwords," six states (California, Delaware, Illinois, Maryland, Michigan, and New Jersey) have banned this practice. Note also that, as illustrated in the case of *PhoneDog v. Kravitz*, 2011 U.S. Dist. LEXIS 129229 (N.D. Cal. Nov. 8, 2011), the line between employer-owned and employee-owned accounts can be extremely fine.

Third-Party, Indirect Access: Third-party access and indirect access are less preferred methods of access because, regardless of the collection or monitoring tool used, a target user may restrict information from view through the use of security or privacy settings. *Third-party access* is using a third-party account to view and collect data from a target user's profile. Note that this method raises a number of ethical concerns not addressed here.

Indirect access consists of access via a web search.

3. Determine Security of Social Media

Security issues related to SNS encompass a number of factors that courts have discussed in deciding the authentication issue. Foremost among these are the availability of user-level security or privacy settings and user's application of such settings.

Other issues discussed by courts include account password protection, multiple users' access of a single account, past hacking events, and the security of the computer and network used to access the information.

Obviously, these factors vary by SNS and in many cases will also vary by user, but generally, the more secure the information, the easier to authenticate.

4. Select Collection or Monitoring Tool

Once the extent of availability of social media data is understood, RIM professionals and attorneys must assess the benefits and limitations of approaches to collecting it. Perhaps the most pressing issue in making such a decision is weighing the return on investment in terms of evidence quality and ease of authentication of using more expensive means.

When it comes to monitoring and collecting social media, organizations have multiple tools at their disposal. These solutions range from simple to complex, and costs tend to rise proportionally with the level of information the tool can deliver. Options for monitoring and collecting fall into the categories of screen capture, archiving solutions, and forensic software.

Screen Capture. The lowest-tech solution for addressing social media is simple screen capture. As it sounds, this method captures text and images on a SNS and saves them in a static hard copy or electronic image format. This is an extremely low-cost method of saving information, which maintains the visual relationships between data but not hyperlinks or relational references between pages.

As indicated by *The Sedona Conference® Social Media Primer*, simply printing out social media site data could result in an incomplete and inaccurate data capture that is hard to authenticate, except on the basis of the personal knowledge of a witness.

Archiving Solutions. Archiving solutions are software designed to target primarily text and image data from an SNS profile. Several social media network providers offer archive functionality, which preserves some user data.

Due to terms of use restrictions, these often provide minimal data, such as a user's posts to his or her own profile, shared photos, private messages, and other information. It does not include metadata or any comments users make on other users' posts or profiles.

To paraphrase Wikipedia, *metadata* can be briefly defined as data about data, data about containers of data, and data about data content. In the social media context, metadata often includes author, recipient, date, time, and location information.

Forensic Software. Currently available forensic software can be used either as a tracking tool to actively monitor a user's activities on the site or as a forensic tool to gather a snapshot of current and past usage. In either case, forensic software is currently the only way to collect metadata on a social media site.

Forensic software can include both static collection tools – useful for collecting a snapshot of all of the material related to a social network profile at a given point of time – and dynamic tracking tools – used to actively monitor a target user account.

Excluding law enforcement situations, these solutions are usually dependent on having an agreement with or court order involving the target account user. Note that compliance archiving tools are a sub-

Read More About It

Facebook, 2013. Facebook for Business. Available at *www.facebook.com/business*.

Payne, Andrew C. Twitigation: Old Rules in a New World, 49 WASHBURN L.J. 841, 845-46 (Spring 2010). Available at *www.washburnlaw.edu/wlj/49-3/articles/payne-andrew.pdf*.

Twitter, 2013. Types of Tweets and Where they Appear, Copyright Twitter 2013. Available at *http://support.twitter.com/groups/31-twitter-basics/topics/109-tweets-messages/articles/119138-types-of-tweets-and-where-they-appear.*

set of forensic software and are used extensively inside and outside regulated industries. Compliance archiving tends to be more costly than other methods typically used in litigation.

Avoiding Evidentiary, Authentication Issues

With smart approaches, attorneys and RIM professionals can tackle the challenges that monitoring and collecting social media present. "The best strategy for handling difficult preservation and collection issues is to confer with opposing counsel and agree on reasonable steps," according to *The Sedona Conference® Primer on Social Media*.

Narrow the Scope

During litigation, the elements of a claim, public web searches, available sources of information, and the types of information available on SNS should all be used to narrow the scope of information requested in discovering social media to avoid requests being found irrelevant or overbroad.

Authenticate Information

While social media information is not self-authenticating, under Federal Rule of Evidence (FRE) 901, the SNS matrix, comprising all the information making up a profile (e.g., HTML text, images, metadata, hash tags, posted information, online relationships), provide fodder for authenticating evidence in conjunction with deposition testimony, forensic investigation of software or hardware, or subpoena to a SNS provider to confirm user identity.

In other instances, enough matrix information can also allow for authentication by distinctive characteristics. In fact, the court in *Lorraine v. Markel American Ins. Co.*, 241 F.R.D. 534 (D. Md. 2007) applied FRE Rule 901(b)(4) by ruling that metadata-level hash values were sufficient circumstantial evidence to authenticate.

For this reason, once the scope of a collection has been set, attorneys and RIM professionals should collect broadly. Acting within the confines of any litigation agreements, the more data collected, the easier it will be to find circumstantial evidence allowing authentication of social media evidence.

Similarly, preserving metadata and maintaining a clear chain of custody can be critical to authenticating social media and other electronic evidence. If metadata – especially dates, times, GPS stamps, and computers from which posts were made – are potentially relevant, use of a forensic software tool is necessary, as forensic software is currently the only method of preserving metadata from social media sites.

Monitor Compliance

In compliance monitoring, use careful scoping and technology to effectively manage social media information on an enterprise level and avoid creating over-monitoring.

Selling management on more software tools and increased staffing is never easy. However, RIM professionals can point to numerous court cases where social media has come into play as one reason to proactively tackle the issue of monitoring and collecting it.

Prepare, Don't Pry

With changes in the way that organizations are using social media, RIM professionals should expect SNS content to be relevant in litigation or a regulatory event. Failure to consider the legal and technical considerations of social media may leave organizations scrambling to comply with e-discovery demands or facing court sanctions.

On the other hand, RIM professionals need to be careful that monitoring social media is undertaken only with respect to organizational accounts. Employer monitoring of employee social media is restricted in several states, may run afoul of anti-discrimination laws and the National Labor Relations Act, and, as noted in *The Sedona Conference® Primer on Social Media*, it may open employers up to liability for actions of their employees. **END**

Lauren A. Allen, J.D., can be contacted at laurenallen@deloitte.com. *Michael C. Wylie, J.D., can be contacted at* miwylie@deloitte.com. *Their bios can be found on page 47.*