Bloomberg BNA

Social Media Law & Policy Report™

Preparing for Social Media Issues in E-Discovery

By William Michael Jr., Catherine Bernard, Laura Hammargren and Megan Anderson

For companies that find themselves involved in litigation regularly, the concept of electronic discovery, or "e-discovery," and its associated considerations, such as best practices for preservation, collection and production of e-mail and computer files, is familiar. But the advent of and continuous developments in social media have increased—sometimes radically—the amount of potentially relevant information that is available electronically, as organizations and individuals create their own constantly expanding and evolving digital trails. And each social media platform creates its own set of complexities with respect to obtaining and preserving information.

Having in place a comprehensive strategy for handling social media in e-discovery—from retention through production—is the most effective means of ensuring that an organization has the ability to comply with applicable discovery rules without exposing the company to overly burdensome (and expensive) discovery expectations. The following checklist is designed to assist organizations and their legal counsel in developing a comprehensive social media strategy for e-discovery.

Given the impact each step has with respect to the other stages of the process, it is important for an organization to consider its discovery strategy comprehensively at the start of any threatened or actual litigation. When it comes to e-discovery, there is no one-size-fits-all approach: different organizations, or even different litigation matters within the same organization, may require very different approaches, depending on the nature of the claims and defenses; the breadth of the litigation; and the extent to which use of social media by the organization and its employees might (or might not) be relevant. And once developed, to ensure a strategy's continued usefulness, the organization must stay updated on changes to technology and social media trends, monitor compliance with social media policies and adjust its discovery strategies as needed.

In developing a strategy to handle social media in e-discovery, an organization should take the following steps:

Step 1: Understand the Scope of Potentially Relevant Social Media

- Define what social media sources may be relevant to the organization and its actual or potential litigation matters:
  - Facebook
  - Google+
  - LinkedIn
  - Twitter
  - Instagram
  - Pinterest
  - Blogs
  - Tumblr
  - Flickr
- Define what aspects of those accounts may be relevant to the organization and its potential/actual litigation matters:
  - Company profile pages
  - Individual profile pages
  - Posts
  - Messages
  - Tags
  - Reviews
  - Other types of messages/statements (e.g., likes, pokes or follows)

Comment: Each link in an organization's digital trail may constitute discoverable information under the broad definitions that typically apply. To anticipate how social media should be handled in discovery, an organization must think through which social media accounts may be at issue in the litigation, and to what extent those accounts may contain relevant information. In addition to the organization's own social media account, the scope of discoverable information may extend to company-authorized individual accounts, and, under some circumstances, private individual accounts.

Step 2: Define Your Access Rights

- Know the legal limitations on your access to social media information.

- State privacy laws
- Electronic Communications Privacy Act and Computer Fraud and Abuse Act considerations
- Ensure compliance with your organization's social media and computer usage policies.
- Account for information stored on personal devices to the extent necessary.

Comment: In order to evaluate what kind of social media information may be at issue, the organization must understand the extent to which it can access that information. Employers generally have broad rights to monitor and access business-related information, especially on business devices; with regard to personal accounts, however, employers' access is much more limited. An increasing number of states are enacting social media privacy laws prohibiting or restricting employers' use of employee user names and passwords. Capture of private electronic communications through the use of keystroke software or other methods may violate the federal Electronic Communications Privacy Act, which prohibits the interception of electronic communications. Similarly, attempts to access an employee's private account surreptitiously—for example, by using a false identity to friend the employee—may violate the Computer Fraud and Abuse Act, which carries criminal penalties.

Organizations should define their access rights clearly by implementing a written social media or computer usage policy that clarifies who owns company-related social media accounts; provides the organization with the right to access work-related social media activity; and permits an employee to agree, to the extent allowed under applicable law, to provide access to personal social media activity. This policy should also account for use of social media on personal devices—e.g., mobile phones and tablets—and outline the same limitations or access issues.

Step 3: Know Your Retention Responsibilities

- Understand whether particularized retention requirements apply to your industry or business.
- Determine what information should be retained, if any.
- Consider any issues with archiving, including the volume of information.
- Establish a system for retaining information to the extent necessary.

Comment: If an organization has decided that company or individual social media accounts will regularly have information relevant to litigation issues, it should institute a written retention policy and implement an automatic archiving system for that information. For example, a sales company with a sales force that contacts customers through text messages or social media may consider that information crucial to litigation claims that it frequently faces. Sometimes, however, the best retention policy is not to retain information at all, or to retain it for only a very short term, for purposes of disaster recovery. Key considerations include whether the law imposes specific retention obligations on the organization's industry, which information is relevant to the organization's core business functions and what it can access legally. Another important factor is the price of retention; depending on the size of the organization, archiving social media and other electronic communications may be substantial, in terms of not only storage costs but also discovery costs, which increase in line with the volume material available for discovery. However, an organization may find it worth the investment to preserve information that might be crucial to a particular type of claim or defense. As explored further below, each social media platform and its different components present different challenges with respect to access, preservation, retention, collection and formatting for production.

Step 4: Issue Appropriate Preservation Notices

- Determine who and what comes within the scope of retention.
- Issue preservation notices that specifically list any social media to be preserved by employees.
- Think through preservation issues with respect to the specific type of social media accounts.
- Set up specific retention system for those social media accounts.

Comment: Once a lawsuit has been served, or even beforehand, if the organization anticipates litigation, the law imposes an obligation to retain all potentially relevant information. The first priority is to issue a preservation notice (also referred to as a hold notice) to all employees who are likely to have such information. Just as with all other types of potentially discoverable materials, whether social media information should be preserved depends on the relationship of the employee and the evidence to the claim or defense at issue. Because of the potential costs of collecting and producing social media, these questions should be given careful thought and consideration. Once it is determined what social media information might be relevant to the claims at issue, the preservation notice should clearly state what employees need to preserve and to what extent, as well as the method of preservation. If the information is voluminous, the organization may want to bring in a third party to ensure accurate preservation. Because social media accounts rarely are stagnant, if social media must to be preserved as of a certain time, that preservation should be done as soon as possible.

Step 5: Collect the Appropriate Social Media

- Work with opposing counsel and the court to set parameters around social media discovery.
  - Clarify the extent to which items housed on third-party servers or personal devices are considered to be in the organization's control.
- Design a collection process that incorporates the relevant social media.
  - Aggregate content into a usable, understandable format.
  - Establish a plan for imaging personal devices to extent allowed/necessary.
- Consider a collection tool that can be integrated with current e-discovery software.
- Use forensics where necessary.
- Fully document the process.

Comment: Many of the considerations relevant to collection will already have been thought through during Steps 1-4 above. First and foremost, the company must balance the importance and value of the information against potential costs and burden.

Once it has done those evaluations, the organization should work with opposing counsel and the court to try and set appropriate limitations on social media discovery.

Part of this discussion should be the question of access. The court and opposing counsel may view private messages as akin to e-mail, but it must be clarified that they are not. Not only are such items housed on the server of third-party social media providers, but, as discussed above, there are legal restrictions that may preclude the organization from accessing employee data. Further, opposing counsel and the court may need to be educated on certain functionalities of social media, such as tools where the messages are not stored (e.g., Snapchat). The goal is to craft a discovery plan that accounts for the level of access the organization has to specific social media accounts and the degree of information it realistically can obtain at a reasonable cost.

Social media e-discovery presents unique collection issues. Litigants commonly agree to use search terms to create the subset of documents for review and production, and predictive coding technologies are an increasingly popular tool in cases involving voluminous e-discovery. The informality of social media, however, lends itself to the widespread use of abbreviations, lingo and misspellings, which may make use of search keywords and/or predictive coding difficult. Additionally, unlike e-mail, a social media collection will encompass photos, hyperlinks and other uncommon forms of data. Finally, the organization may need to take particular steps to ensure that it collects and produces social media information in a usable format. For example, although a Facebook profile appears to the user to be a single, consolidated page, archived user content actually may be stored in different formats across multiple databases. Further, the organization may be required to produce the metadata for that content. In such circumstances, it may be advisable to use a forensic professional to capture those data; the short-term cost will be significantly outweighed by the long-term consequences of an inadequate collection process. Whatever collection system the organization implements, it must be well-documented, as the defensibility of the process used and the information captured may be questioned throughout the discovery process and potentially up through trial.

Step 6: Investigate and Request Social Media From Other Party Appropriately

- Investigate publicly available information on social media that the other party might have.
- Negotiate with the other side to the extent possible to come to a clear understanding about social media collection and production.
- Seek discovery of social networking information from the opposing party before subpoenaing the social networking sites.
- Make sure to include social media in written discovery and in preparation for witness interviews and depositions.

Comment: Before discovery starts, the organization should look into existing publicly available social media information about the opposing party. Knowledge of what an opponent has made available in the past is an important weapon to have in the arsenal during negotiations with an opponent over the proper collection and production of its own social media evidence. To ensure that the organization does not commit any legal or ethical violations, this initial investigation should be limited to publicly available data.

As courts typically find that a social media account hosted by a third-party provider is within the custody and control of the account holder, subpoenas for social media data are not appropriate until all reasonable efforts have been made to obtain that information from an opponent through the ordinary discovery process. Although applicable court rules generally define the scope of documents available through discovery in a manner that includes social media information, it is prudent to state explicitly whether social media is included in a discovery request, and if so, what types.

William Michael Jr. is a partner and co-leader of Mayer Brown's White Collar Defense & Compliance group. He is based in Chicago and can be reached at wmichael@mayerbrown.com.

Catherine Bernard is counsel in Mayer Brown's Litigation & Dispute Resolution practice and a member of the firm's Electronic Discovery and Information Practice group. She is based in Washington DC and can be reached at cbernard@mayerbrown.com.

Laura Hammargren is an associate in the White Collar Defense & Compliance group of Mayer Brown in Chicago. She can be reached at lhammargren@mayerbrown.com.

Megan Anderson is an associate in Mayer Brown's Litigation & Dispute Resolution practice in Chicago. She can be reached at manderson@mayerbrown.com.