July 2014

MAYER • BROWN

ELECTRONIC DISCOVERY & INFORMATION GOVERNANCE

Tip of the Month

Managing the Risks and Costs Associated with Enterprise Social Networks

Scenario

An international company has decided to launch an enterprise social network to facilitate a more collaborative work environment. The Chief Data Officer is tasked with forming and leading a committee to assess any risks associated with the implementation of the new technology, to encourage employee participation and to develop policies and procedures for the governance of the enterprise social network.

Uses of Enterprise Social Networks

The way that people communicate is constantly evolving. The current trend favors collaborative communication via social media or social networks. Recognizing this trend, businesses see potential value in employing social networking technology within their organizations. These internal social networks are often referred to as “enterprise social networks” (ESNs). ESNs refer to internally deployed software designed to promote collaboration, communication and knowledge-sharing among employees in a group setting. Examples of such software include Jive, Yammer and Chatter.

According to Deloitte, the adoption of these enterprise social networks has been on the rise; in early 2013, Deloitte predicted that more than 90 percent of Fortune 500 companies would partially or fully implement an ESN by the end of 2013. But how companies use their ESNs can vary widely. Some organizations are limiting the use of ESNs to community building or promoting a common corporate culture by, for example, coordinating charitable activities or encouraging communication among affinity groups. Some organizations are using ESNs to centralize communications about corporate activities such as human resources, benefits, policies or strategic initiatives. And some organizations are using ESNs to improve workplace productivity through collaboration around projects, clients or products.

Dumping Grounds of Information and Hotbeds of Legal Risk

A company’s intended use of its ESN will dictate not only implementation and deployment of the software, but also the policies and procedures governing the network. The biggest risks associated with ESNs lie in ESNs that are *not* governed—that is, networks that are allowed to develop organically or as directed by individual employees as opposed to corporate management. Such ESNs inevitably become dumping grounds for corporate information and hotbeds of legal risk.

The idea that improperly managed data can lead to legal risk is hardly revolutionary. But the dynamic and interactive nature of ESNs, their expansive reach and their non-traditional format combine to complicate the company's ability to ensure that data stored in such networks can be retained, organized, retrieved and disposed of by the company as needed to meet the company's business, legal and regulatory needs.

- Retention. ESNs, with their non-traditional format and diversity, create a conundrum for records management. Ungoverned use of ESNs may make identifying categories or types of information stored within the social network difficult to locate or isolate. And questions frequently arise as to whether the company can assign a standard retention period for the entire ESN, or whether the company must find ways to assign retention periods on a subject or content basis.
- Litigations/Investigations. ESNs do not fit neatly into the traditional e-discovery concepts or technologies used for preservation and collection of electronic communications. On the one hand, ESNs contain the type of employee communications traditionally associated with "custodial" data, which are typically preserved, at least in part, by issuing legal hold notices. On the other hand, ESNs are not like traditional custodial data, are not controlled by the custodian and are more akin to dynamic structured databases. The changing nature of the ESN content, the potential difficulties in identifying relevant data within the ESN and the ESN's unique technology all combine to increase the risk that relevant data may not be properly preserved or collected.
- Employment. ESNs also raise unique employment concerns. Inappropriate posts that may violate the company's acceptable use polices are magnified given the extensive reach and interactive nature of such networks. At the same time, companies need to be careful that any monitoring of the ESN does not infringe on their employees' privacy rights (whether based on state, federal or foreign laws) or result in employment action based on posts that may amount to protected activity.
- Intellectual Property/Confidential Information. The expansive reach of ESNs can also raise unexpected intellectual property issues. Employees may unwittingly post subscription articles to an ESN without realizing that such actions may violate the company's licensing arrangements for those publications. Or employees may post confidential or privileged information to an ESN that does not have restricted access, inadvertently exposing that information to employees who are not authorized to view that information.

Tips for Managing Enterprise Social Networks

To avoid the corporate dumping ground and to effectively manage the risks of an ESN, it is critical that the company clearly define (i) the purpose for the ESN; (ii) the audience for the ESN; (iii) the rules and guidelines governing the ESN; and (iv) the roles and responsibilities for managing the ESN. These issues should be thoroughly assessed and considered by the company *before* the enterprise social network goes live.

- Define the Purpose. As noted above, there are various uses for an ESN. Those uses impact the risks associated with the network and inform the types of policies and controls that are appropriate to manage the risks. Take the time to consider the intended purpose of the ESN—and any particular sections or sites within the ESN—so that all relevant stakeholders understand, and agree on, the appropriate use of the ESN.
- Consider the Audience. Careful consideration should be given to the intended audience for any ESN. Evaluate whether the ESN is intended for use by all company employees, or whether access to certain sites within the ESN must be restricted for confidentiality, business or legal reasons. For regulated employees or employees subject to special retention requirements, consider what the company's retention obligations are, and whether

those obligations include sites that the regulated employee viewed or posts that the employee made. Additionally, use of, or access to, the ESN by non-U.S. employees may raise data protection concerns in certain jurisdictions, so such access should be carefully vetted before launching the ESN.

- Tailor Policies and Training Programs. A company's general electronic communications or acceptable use policies may be insufficient to address the nuances of ESNs. While those policies can and should incorporate ESN use, additional policies and training tailored to the ESN and its authorized uses should be developed and clearly communicated to employees. For example, if establishing social or community-building ESNs, there should be clear directives not to engage in business activities on the site, and clear notice provided concerning any monitoring activities as well as the consequences for violating the company's policies. For clear business activities, policies should be developed on whether and how a document would become a record, subject to normal record retention and storage requirements, whether the network will be moderated or collaborative and whether it is designed to replace other authorized forms of communications. Finally, policies and procedures regarding legal hold obligations, regulatory retention requirements and acceptable use that are specific to ESNs are critical to manage the legal and regulatory risks, regardless of the defined purpose.
- Delineate Roles and Responsibilities. It is important to clearly establish roles and responsibilities for the ESN. While many groups within the company will have some role in the operation of the ESN, from IT to business lines, someone within the company must be accountable for ensuring that the content of the ESN is properly managed by the company. This includes responsibility for ensuring, *inter alia*, that (i) new sites are approved by the company; (ii) appropriate measures are in place with respect to security and access to the ESN; (iii) policies and procedures are in place and updated on a regular basis; (iv) regular training is conducted for employees on the appropriate use of the ESN; and (v) inactive sites are shut down on a timely basis.

For inquiries related to this Tip of the Month, please contact Anthony J. Diana at adiana@mayerbrown.com or Therese Craparo at tcraparo@mayerbrown.com.

Learn more about Mayer Brown's Electronic Discovery & Information Governance practice or contact Anthony J. Diana at adiana@mayerbrown.com, Eric B. Evans at eevans@mayerbrown, Michael E. Lackey at mlackey@mayerbrown.com or Edmund Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com.