Social Media Law Update

Posted at 1:59 PM on January 18, 2011 by Sheppard Mullin

E-Discovery Rules Applied to Social Media: What This Means in Practical Terms for Businesses

By Michelle Sherman

Companies are on social media. They are interacting and connecting with customers through Facebook, Twitter and blogs. In a study last year, so the numbers are already on the conservative side, 65% of Fortune Global 100 companies have active Twitter accounts, and 54% have Facebook fan pages. One third of these companies have a blog. This is how companies are doing business today. And, with this presence online comes legal obligations to capture and save these communications.

1. E-Discovery Rules Apply To Social Media Activity.

These communications and online activity should be thought of as an extension of "electronically stored information" ("ESI") and the discovery rules that apply when a company is in a legal dispute that would trigger a duty to preserve company emails and electronic documents. When the Federal Rules of Civil Procedure were amended in 2006 to include ESI, the term was "intended to be read expansively to include all current and future electronic storage mediums" Notes of the Advisory Committee to the 2006 Amendments to Rule 34. It does not matter how brief the storage period, courts will treat the information as discoverable. Accordingly, even storage in the "cloud" or on a social networking site will be treated as discoverable ESI.

To summarize the e-discovery rules, there is a duty to preserve relevant or potentially relevant information once litigation is pending or reasonably anticipated as long as it is in your custody or control. For the party filing the legal action, the litigation hold and "do not destroy" notice should be triggered before the complaint is filed. "A duty to preserve evidence arises when there is knowledge of a potential claim." *Micron Tech. v. Rambus*. In *Micron Tech*, the district court for Delaware held that the implementation of a document retention policy around the time that Rambus was already preparing its litigation strategy to enforce its patent portfolio, and Rambus started and was continuing to destroy documents until just prior to filing its suit, was evidence of spoliation. The court imposed the most severe discovery sanction, and declared that the patents in suit were unenforceable against Micron Tech.

A recent study found that courts are increasingly imposing strong sanctions against attorneys and their clients for failing to comply with the e-discovery rules. In a study of 401

cases before 2010 in which sanctions were sought, sanctions were awarded in over half of them. Some of the sanctions were especially severe, and included case dismissals, adverse jury instructions and large monetary sanctions. $5 million sanctions were ordered in five cases, and $1 million or more in four others. Defendants were sanctioned for e-discovery violations nearly three times more often than plaintiffs, and the number one reason for imposing sanctions was failure to preserve electronic evidence.

What this means in practical terms for companies is several things.

2. Update Document Retention Policies to Include Social Media Activity.

Companies should update their document retention policy to include social media activity. The procedures that the company is following for e-mails in terms of storage and retention periods may be a good starting point. By having established processes and following them, adversaries in litigation will have a hard time arguing that the company has destroyed relevant, and possibly damaging information. The standard for preservation is "reasonableness and proportionality" so modeling it after the procedure for retention of company emails makes sense and is internally consistent.

The revisions to the document retention policy should also take into consideration any industry regulations, such as state laws governing real estate brokers, and SEC and FINRA record keeping rules for the financial services industry. For example, FINRA issued guidance in January 2010 for blogs and social networking sites, and set forth the record keeping responsibilities in the financial broker-dealer business.

> "Every firm that intends to communicate, or permit its associated persons to communicate, through social media sites must first ensure that it can retain records of those communications as required by Rules 17a-3 ad 17a-4 under the Securities Exchange Act of 1934 and NASD Rule 3110."

The company's current document retention policy is a good starting point, and the assistance of legal counsel is advisable in making any revisions to include social media.

3. Identify A Vendor That Can Capture And Store Social Media Activity.

For both regulatory and sound business reasons, Citigroup Inc. is reportedly capturing its social media activity through CoTweet. Citigroup is planning to handle more of its customer relationships through Twitter. The goal is to "build rapport with customers, and they come back to you just as they would in a branch," according to Frank Eliason, Citigroup's senior vice president of social media. Citigroup is training 100 customer service representatives to handle customer complaints and questions on Twitter. The representatives are also being encouraged to build customer followings through Twitter.

In storing its Twitter activity, Citigroup has practical concerns for not having its data stored in the "cloud," including the statutory requirements that banks safeguard the privacy of customer data, and also have an audit trail for most of their interactions with customers.

CoTweet is not the only option. Companies should work with legal counsel and their IT/litigation support departments to identify the best vendors for their purposes. Some terms worth negotiating with the vendor include: (1) the company owning the data; (2) strict limitations on who can have access to the data; (3) the holding period for the data; and

(4) storing personal data in encrypted form. Some other vendors that offer storage capabilities include: (1) SocialSafe which allows businesses to download the information so it is not stored in the "cloud"; and (2) Backupify which represents that it stores the data to a cloud but has a "great security and data duplication policy."

4. Conclusion.

Businesses cannot afford to postpone updating their document retention policies, and finding a good solution for storing their social media activity. Courts are ordering sanctions for e-discovery violations, and businesses subject to state and federal regulations are being required to store much of this information as well. If a business anticipates being involved in litigation, make sure your legal counsel is asking about your social media activity, and how the potentially relevant or discoverable data is being maintained.

For further information, please contact Michelle Sherman at (213) 617-5405. (Follow me on Twitter!)