Social Media Law Update BLOG
Highlighting Legal Issues Regarding Social Media
SHEPPARD MULLIN
SHEPPARD MULLIN RICHTER & HAMPTON LLP
ATTORNEYS AT LAW

5 | 17 | 2011 by Sheppard Mullin

By Michelle Sherman

Is Your Company's Social Media Launch Ahead Of Its Compliance Program

Many businesses are still coasting along enjoying the marketing advantages of social media without making sure they have a good compliance program in place. For every company with a Facebook fan page or Twitter account roughly 65 percent would admit they do not have a social media policy. For companies with a social media policy, many of those policies have been lifted from online samples that may be over broad, and include provisions that have been challenged with some success in court.

"Penny wise and pound foolish," companies are not having their social media business practices reviewed by knowledgeable legal counsel. Companies invest time and money putting together a Facebook fan page that is promoted throughout the company without training their employees on the Do's and Don'ts of posting comments on the fan page, or using social media in general.

Another risk of social media was highlighted by settlements that the FTC reached with Twitter and Google concerning shortcomings in their privacy guidelines. The consent decrees reached by each of the companies highlight how seriously the FTC takes the safeguarding of consumer information. In the case of Twitter, the FTC put the responsibility for hackers gaining administrative access to Twitter personal accounts on Twitter. One hacker gained access to non-public information such as users email addresses and mobile phone numbers. The same hacker changed the passwords for approximately 45 high profile Twitter users including President Obama and sent phony tweets from those accounts.

The hacker found his way into the system because Twitter did not have a feature that is commonly used with online stock brokerage accounts where the system will lock you out after a few unsuccessful attempts to enter the correct password. The hacker used an automated password guessing tool which submitted thousands of guesses until finding the correct password. The FTC identified other shortcomings in Twitter's security system including: (1) Not requiring that passwords be unique and different from what a Twitter employee, who also had administrative control of the Twitter system, used to access third-party programs and networks; (2) not requiring periodic changes of administrative passwords; and (3) not requiring that Twitter passwords in personal email

accounts be stored encrypted instead of the plain text that some Twitter employees used. The FTC framed the complaint as Twitter not living up to its representations to consumers on its security practices. Twitter's privacy policy stated, "Twitter is very concerned about safeguarding the confidentiality of your personally identifiable information. We employ administrative, physical, and electronic measures designed to protect your information from unauthorized access." Twitter settled with the FTC and agreed, among other things, to establish and maintain a comprehensive information security program so that nonpublic consumer information cannot be hacked into. This security information program will be assessed by an independent third-party auditor every other year for the next ten years. Twitter must also maintain records regarding its privacy practices and policies. Each violation of the settlement order may result in a civil penalty up to $16,000. The recent Google Buzz settlement is a perfect example of a company forgetting to read and take into account its own privacy policy. Google's Gmail privacy policy assured users of its email service that the information was being stored for the user's purposes, and that Google would seek permission in advance of using the user's personal information for a different purpose.

In launching Google Buzz, a social networking platform that Google hoped would compete with Facebook, the FTC alleged that Google tried to create instant networks of friends for its users by pulling from their email contact lists without considering this information may be very sensitive to the individual users (imagine, clients of therapists and attorneys, abusive ex-husbands, children and job recruiters). As a result, Google has had to enter into a comprehensive settlement that goes beyond the current regulatory requirements, and will likely hamstring Google's efforts to compete with Facebook and other social networking sites that are not subject to similar restrictions. Among other things, Google must get *affirmative* consent to any new or additional uses of previously collected data. Google must also implement a comprehensive privacy program that is reduced to writing, and includes an employee designated to manage the privacy program; and implement privacy controls and procedures with regular audits to make sure it is effective. Every two years, Google must have an independent auditor review the privacy program and prepare a written report. Google must comply with this comprehensive privacy program for 20 years, and that time period can be extended if Google violates the settlement consent order. These FTC consent orders underscore the importance of making sure companies have their social media practices reviewed by knowledgeable legal counsel, risks identified and addressed, employees trained on correct usage, and new social media marketing strategies coordinated with legal counsel.

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