AN OFFICIAL PUBLICATION OF THE
OHIO CHAMBER OF COMMERCE:
SEPTEMBER/OCTOBER 2009

Ohio MATTERS

CAPTURING THE SPIRIT

Highlights from the 2009 Policy Conference at Salt Fork State Park

Available online at www.ohiochamber.com

Social Media & Pitfalls for Businesses

By Heather Enlow
Vorys, Sater, Seymour and Pease LLP

The use of social media by businesses has exploded. Sites such as Twitter and Facebook appeal to businesses because they provide a free medium through which to connect with their customers and foster their brands. Just because these sites are free, however, does not mean that they do not come with potential costs. When using social media, there are several considerations that businesses should take into account.

Read and Obey the Terms of Use

The first thing that all businesses should do is read the sites' terms of use. When establishing a social media account, a business most likely will be required to click to agree to the particular site's terms of use. Based on this agreement, these terms govern the business' relationship with the site and in many cases place limitations on the use of the site. These terms also constitute a contract between the business and the site, and violations of the terms could create breach of contract liability for the business.

Terms of use are frequently updated, and the click through agreement may allow the site to unilaterally revise the terms, so businesses should check them periodically to ensure compliance with the updated terms. Although these terms tend not to be particularly onerous, businesses must comply. Facebook's terms, for example, prohibit sending unauthorized commercial communications on its systems, collecting users' information by automated means and offering sweepstakes or other promotions without Facebook's consent. Facebook's terms also restrict what personal information can be collected from users who interact with businesses and/or require businesses to disclose how they will collect and use personal information.

Facebook, MySpace and other social media sites have brought lawsuits in order to enforce their terms of use. Courts in California have held that commercial e-mails sent over Facebook's and MySpace's internal e-mail systems must comply with CANSPAM, and recently the Northern District of California allowed a suit to proceed that was brought by Facebook for violations of its terms of use. The court upheld Facebook's allegations that violations of its prohibition on collecting user information by automated means constituted copyright infringement.

In addition, criminal penalties could be imposed for violations of terms of use. Although Lori Drew's criminal conviction based on her violation of MySpace's terms for cyberbullying was recently overturned, the fact that the jury convicted her initially could encourage prosecutors to try similar claims. Thus, violations of the terms can result in significant liability for businesses, and as a result, policies must be put in place to review and comply with the applicable terms of use.

Recognize the Loss of Control

When signing up for and engaging in social media, businesses often do not realize that social media sites are largely unrestricted in their use of the information businesses upload to their account. In February, Facebook changed its terms of use such that it seemed that Facebook, not users, owned all information that was uploaded to Facebook. After a significant backlash by users, Facebook revised its terms to make clear that users own all information and content uploaded to Facebook.

Although Facebook and other social

media sites do not claim to own the information businesses upload, they do grant themselves broad rights to use such information. For example, Facebook's terms grant it a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any content that is posted on Facebook. Facebook's license only expires when an account or content is deleted, but even then the license does not expire if the content has been shared with others and those with whom the content was shared have not deleted it. It is important to realize that once content has been uploaded, users with whom the business interacts may believe that they are free to use the content as they please. This means that it is incumbent upon the business to attempt to patrol and monitor the use of the content, including the business' marks, once the material has been uploaded. Moreover, as Facebook and other social sites continue to develop and engage in advertising on their networks, there may be limited ways to control how advertising is placed near the material. For example, there is nothing, at this time, to prevent Facebook from displaying advertisements of competitors on a business' "page."

Although these services are a great way to connect and market to consumers, it is important to remember that once information is made available on social media sites, it could be difficult to control how the information will be shared and used. Thus, businesses should think carefully about the information, images, marks and other content they post to these sites and put monitoring and policing policies in place.

Take Steps to Protect Your Data

In August, Twitter was rendered virtually inoperable for several hours, and its performance was hindered for all users for several days. This was caused by a denial of service (DOS) attack that had geo-political motivations. In addition, in June, Twitter's internal system was hacked, which resulted in the publication of several internal Twitter business documents. Other social media sites also have experienced similar attacks or lapses in data security.

For businesses using social media, this demonstrates an additional reason to closely examine the materials that are uploaded to such sites. Even if content is designated such that only a certain group of people can access that particular content, it is important to remember that an attack or flaw in data security could negate these designations and unauthorized persons could have access to the content. In addition, businesses should take measures to ensure that their networks and databases are not persistently connected to these sites and consider all necessary data security protections that should be put in place so that attacks on these sites also will not affect the business' networks. Businesses also should have contingency plans in place to connect with consumers in the event that these social media sites are rendered inoperable.

Old Laws Still Apply in the Brave New World of Social Media

Finally, businesses should ensure that the content uploaded to their social media accounts complies with all other applicable laws and business policies. Social media is a new and exciting way to interact with consumers; however, just because it presents a new way of interacting does not mean that "old" laws do not apply to this commercial activity. For example, the Federal Trade Commission has made clear in the recent proposed update to its Guides Concerning the Use of Endorsements and Testimonials in Advertising that such guidelines apply to online activities. The New York state attorney general recently settled for $300,000 with a plastic surgery company that planted "false" product reviews on its Web site and other third party sites. Additionally, as discussed above, courts have held that CANSPAM applies to commercial communications sent over social media networks. Thus, businesses need to evaluate what types of communications with its users need to be CANSPAM compliant. And businesses should ensure that they are not violating third party intellectual property rights (such as copyright, trademark or trade secrets) when they post material. In light of all these factors, businesses need to establish guidelines and policies for content posted to social media sites to ensure that their activities do not run afoul of the law.

Although these services are a great way to connect & market to consumers, it is important to remember that once information is made available on social media sites, it could be difficult to control how the information will be shared & used.

Businesses also should consider the privacy expectations of the consumers they interact with on these sites. When the launch of Facebook's Beacon feature last year resulted in considerable user backlash, companies who participated in the Beacon feature suffered as well. The lawsuit against Facebook over Beacon also included claims against the private companies who participated in Beacon. Thus, when using social media, and using the data obtained from social media, businesses should consider carefully whether the proposed use would be viewed by customers as violating their privacy or trust.

Social media can be a fun and useful way for businesses to interact with their consumers. However, businesses need a plan in place to make sure they avoid social media's potential pitfalls.

Heather Enlow is an associate in the Columbus office of Vorys, Sater, Seymour and Pease LLP, where she specializes in privacy, data security and copyright law. She can be reached at (614) 464-6466 or hjenlow@vorys.com.