Social Media Law Blog
Highlighting Legal Issues Regarding Social Media
Presented By SheppardMullin

Facebook's Settlement With the FTC is a Wake Up Call for Businesses to Review and Update Their Website Privacy Policy and Agreements

December 27, 2011 by Michelle Sherman

The Federal Trade Commission ("FTC") is working hard to make sure consumers are not being misled about how websites and social networking sites are using their personal information. Companies that do not follow their own privacy policies are finding themselves the subject of FTC complaints. It is therefore even more important for businesses to review and update their "privacy policy," "terms of use," and other legal agreements on their websites. This review should also include any company apps.

1. When Businesses Do Not Comply With The Terms Of Their Website Privacy Policy, Then They May Be In Violation Of Section 5(a) Of The FTC Act

The recent consent decrees that the FTC entered into with Facebook, Google and online advertiser ScanScout highlight the need for businesses to make sure they are acting in accordance with their privacy policies. Businesses are well advised to take the following actions:

(1) Ensure that the published policies on their websites for terms of use and privacy reflect what information the businesses are collecting from consumers, and that the disclosures are clearly stated without unnecessary and lengthy legalese;

(2) Examine how the businesses are using personal information or anticipate using it, and that these uses are being fully disclosed to consumers; and

(3) Take reasonable measures to safeguard consumer information. Because of the risks of cyberhacking, it is also worthwhile to conduct an audit on how consumer information

is being safeguarded, and what information is being stored and for how long a period. The FTC settled a complaint against Twitter for its alleged failure to take reasonable safeguards to protect users' accounts against hackers.

In all of these complaints, the FTC alleged that the respondents made false or misleading representations about their privacy policies in violation of Section 5(a) of the FTC Act. The FTC Act prohibits unfair or deceptive acts or practices. 15 U.S.C. § 45(a).

The consent decrees entered into by Facebook, Google and ScanScout in order to avoid more costly litigation and possibly stiffer penalties are similar in some key respects, and include some terms that will increase their costs of doing business. As is sometimes the case with the FTC, the FTC conditioned the settlements on these businesses agreeing to change their business practices in ways that may place them at a competitive disadvantage to their competitors because some of the additional privacy measures they must now take are not required under current law.

2. Lessons To Be Learned From The FTC Settlements With Facebook And Others

It is instructive to know how these businesses allegedly violated the terms of their privacy policies with users because the same may be true for many companies.

(a) Facebook Complaint

In its complaint against Facebook, the FTC alleged:

(1) Facebook told its users that third-party apps that users installed – such as Farmville by Zynga– would have access only to user information that they needed to operate. In fact, the apps could access nearly all of the users' personal data.

(2) Facebook told users that they could restrict sharing of data to limited audiences – for example, with "Friends Only." In fact, selecting "Friends Only" did not prevent their information from being shared with the third-party applications their friends used.

(3) Facebook promised users it would not share their personal information with advertisers. Facebook did according to the FTC.

(4) Facebook claimed that when users deactivated or deleted their accounts, their photos and videos would be inaccessible, when in fact Facebook allowed access to the content according to the FTC.

(5) Facebook also claimed that it complied with the U.S. – EU Safe Harbor Framework that governs data transfer between the U.S. and the European Union, but it did not.

(b) Google Complaint

Google is also faulted for making use of its users' data in ways that was contrary to what Google was telling users about the launching of Google's Buzz social network through its Gmail web-based email product. The FTC alleged that "Google led Gmail users to believe that they could choose whether or not they wanted to join the [Buzz] network, [but] the options for declining or leaving the social network were ineffective." Google was apparently trying to immediately ramp up its social network in order to compete with Facebook. The Buzz launch ended up being a public relations nightmare for Google with thousands of consumers reportedly complaining that they were concerned about public disclosures of their email contacts from which Google tried to create immediate Buzz connections for users. In some cases, use of the emails disclosed ex-spouses, therapists, employers or competitors.

According to the FTC, Google breached its privacy policy when it launched Buzz, its social networking site, because Google's policy told Gmail users that "[w]hen you sign up for a particular service that requires registration, we ask you to provide personal information. If we use this information in a manner different than the purpose for which it was collected, then we will ask for your consent prior to such use." According to the FTC, Google used Gmail users' information for a different purpose without telling them by starting a social networking site with the information.

(c) Online Advertiser ScanScout Complaint

The FTC is not just pursuing these actions against social media behemoths such as Facebook and Google. In November 2011, the FTC reached a settlement with an online advertiser ScanScout. ScanScout is an advertising network that places video ads on websites for advertisers. ScanScout collects information about consumers' online

activities (aka behavioral advertising) in order to post video ads targeted to the people visiting the website. In ScanScout, the FTC alleged that there was a discrepancy between the online service and their website privacy policy:

"[F]rom at least April 2007 to September 2009, ScanScout's website privacy policy discussed how it used cookies to track users' behavior. The privacy policy stated, 'You can opt out of receiving a cookie by changing your browser settings to prevent the receipt of cookies.' However, changing browser settings did not remove or block the Flash cookies used by ScanScout…. The claims by ScanScout were deceptive and violated Section 5(a) of the FTC Act."

In the ScanScout action, the company Tremor Video, Inc. is also subject to the settlement order because ScanScout merged with Tremor Video. This settlement also highlights the importance of doing an audit of a target company's social media activity before acquiring or merging with it so your company will have more information concerning the legal risks of the deal.

3. Business Costs Of Not Updating Your Privacy Policy And Following It

In each of these cases, the FTC is making the settling party do some things that are more than they would have been required to do in the normal course of business, thereby, making it more challenging and expensive for them to do business.

These consent decrees require the settling party to do the following:

(1) Tell users what information is being collected and for what purpose, with the right to "opt out" of the targeted advertising (ScanScout);

(2) Obtain consumers' affirmative express consent before enacting changes that override their privacy preferences (Facebook; Google);

(3) Establish and maintain a comprehensive privacy program to address privacy risks associated with new and existing products and service, and protect the privacy and confidentiality of consumers' information (Facebook; Google); and

(4) Every two years, for the next 20 years, obtain independent, third party audits certifying that the privacy program meets or exceeds the requirements of the FTC order (Facebook; Google).

4. Conclusion

Considering that the vast majority of consumers simply click through the legal agreements to get to the applications on a website, there is no real downside to companies spending a little time and money to ensure that their privacy policy, terms of use and other legal agreements reflect their current practices. Similarly, updating these agreements should be a routine part of changing how the company is collecting and using information from its users. It should be coordinated between marketing, IT and legal with each checking off on the updates being accurate. And, finally, the website should clearly indicate that the privacy policy and/or agreements have been updated so users have the option to review any changes. If experience is any indicator, virtually all users will continue to visit the website notwithstanding the updated policy or agreements.

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