Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

WSGR ALERT

MAY 2012

MYSPACE REACHES CONSENT AGREEMENT WITH FTC OVER MISREPRESENTATIONS IN PRIVACY POLICY

The Federal Trade Commission (FTC) on May 8, 2012, announced that it has reached a consent agreement with the social networking site Myspace. The agreement settled charges that Myspace misled its users about the extent to which the site shared personal information with third-party advertisers, and it signals increased scrutiny by the FTC on how social networks share information about their users with advertisers. The consent order prohibits Myspace from making misrepresentations regarding the extent to which it maintains the privacy of its users' information and the extent to which it complies with the U.S.-EU Safe Harbor Framework and similar programs. The order also requires Myspace to establish a "comprehensive privacy program" and obtain biennial assessments of the program by an independent auditor for the next 20 years. The consent order is the third such order specifically requiring a comprehensive privacy program, following similar privacy consent orders the FTC entered into with Google and, more recently, Facebook.

Background

The FTC alleged that, contrary to representations made in its privacy policy, Myspace shared users' personally identifiable information (PII) with third-party advertisers by providing those advertisers with users' "Friend IDs." A Myspace Friend ID is a persistent, unique number that easily can be used to access a Myspace user's profile page. Depending on a user's privacy settings, different types of information may be publicly available on that user's profile page. According to the complaint, Myspace designated certain profile information, including a user's profile picture, location, gender, age, display name, and full name, as "basic profile information" outside the scope of its privacy settings, and thus made that information publicly viewable. While a user could change Myspace's default setting, which shows the user's full name publicly, allegedly only approximately 16 percent of users had made their full names private as of July 2010. Thus, as of July 2010, the Friend ID allegedly could be used to access, at a minimum, the basic profile information of Myspace users, including the full names of approximately 84 percent of those users.

Since January 2009, Myspace allegedly shared the Friend IDs, ages, and genders of users viewing the Myspace site with third-party advertisers. According to the complaint, Myspace transmitted this information to third-party advertisers from January 2009 to June 2010 whenever its affiliated advertising network did not have an appropriate ad to serve. While Myspace allegedly started encrypting the Friend IDs, ages, and genders of users viewing the Myspace site in June 2010, it provided the encryption key to its affiliated ad network so that this information could be used to target advertising to those users. On October 29, 2010, Myspace's affiliated ad network was sold to a third party, and Myspace allegedly continued to provide the encryption key to the new owners of the ad network for the following year.

In its privacy policy, which was applicable at the time this information sharing was occurring, Myspace allegedly represented that it would not share a user's PII with unaffiliated third parties. Myspace further allegedly represented the following: (a) that while some users' profile information might have been used to customize ads delivered to them, the information provided for this purpose could not be used to personally identify each user; (b) that anonymous web traffic and aggregated demographic information could be shared with advertisers; and (c) that Myspace maintained a current self-certification to the U.S.-EU Safe Harbor Framework from December 9, 2010, until the present, and the company complied with the framework in its privacy policy.[1]

The FTC's Claims

In its complaint, the FTC alleged that four of Myspace's representations were false or misleading, thereby qualifying as deceptive acts or practices that violated Section 5 of the FTC Act. Key to the FTC's claims were that third-party advertisers receiving a user's Friend ID could use that ID to access the user's public profile and obtain PII about that user. Specifically, the FTC alleged that Myspace misrepresented that:

[1] The U.S.-EU Safe Harbor Framework serves as a method that U.S. companies may use to transfer personal data outside of the European Union, consistent with the requirements of the European Union Data Protection Directive. The framework is a voluntary program through which a company self-certifies to the U.S. Department of Commerce that it complies with the framework's principles and requirements.

Continued on page 2...

Myspace Reaches Consent Agreement . . .

Continued from page 1...

1. Myspace would not share a user's PII with third parties without giving notice to and receiving permission from the user. The FTC claimed, however, that by providing third parties with a user's Friend ID, Myspace gave those third parties access to that user's PII without providing the user with notice or obtaining permission.

2. The means Myspace used to customize ads did not allow advertisers to access PII or individually identify users. Again, the FTC claimed that by providing third parties with a user's Friend ID, Myspace gave those third parties access to that user's PII.

3. Information about users' web browsing activity was anonymized when shared with advertisers. The FTC claimed, however, that by providing advertisers access to a user's PII via that user's Friend ID, advertisers could link web browsing activity collected via cookies stored on that user's browser to PII available on that user's Myspace profile.

4. It complied with the U.S.-EU Safe Harbor privacy principles of notice and choice. The FTC claimed, however, that Myspace did not adhere to these principles.

Settlement Terms

Myspace's settlement with the FTC is similar in its terms to the previous privacy consent orders the FTC entered into with Facebook and Google. As noted above, the consent order prohibits Myspace from making misrepresentations regarding user privacy and compliance with the U.S.-EU Safe Harbor Framework. Myspace also must establish a comprehensive privacy program and obtain biennial assessments of the program by an independent auditor for the next 20 years. The specific requirements of the privacy program and the required contents of the biennial assessments are virtually identical to the programs and assessments imposed by the FTC's settlements with Google and Facebook.

One subtle but notable addition to the Myspace consent order that distinguishes it from the previous privacy consent orders is the explicit inclusion of "device ID" as "covered information" within the definitions in the order. The order prohibits misrepresentations regarding the privacy of covered information, and the required comprehensive privacy program must be designed to protect such information. The FTC's definition of "covered information" has included persistent identifiers in the past, but this order represents the first time that "device ID" specifically has been identified as a persistent identifier in a privacy order. This subtle inclusion may be a signal that the agency intends to scrutinize the use of device IDs in the targeted advertising context going forward, which could have a significant impact on companies developing mobile applications supported by such advertising.

Implications

This settlement has important implications for businesses engaged in targeted advertising, particularly those also engaged in the social media space. Companies should take care that representations made in their privacy policies regarding data collection, sharing, and use are accurate. Additionally, companies that self-certify compliance with the U.S.-EU Safe Harbor Framework or other self-regulatory codes should ensure that they understand the requirements of those programs and are acting accordingly. Companies that share personally identifiable information about their users, even if only indirectly, may find themselves subject to regulatory scrutiny if they do not provide their users with what the FTC believes to be adequate notice and choice regarding information-sharing practices.

Wilson Sonsini Goodrich & Rosati's privacy and data security practice routinely advises clients on privacy and data security matters, including defending companies under investigation by the FTC for privacy issues and assisting companies with compliance with FTC privacy and data security orders. The firm also regularly assists companies with all legal matters associated with the collection, use, and disclosure of consumer data. For more information on our privacy and data security practice, please visit: http://www.wsgr.com/WSGR/Display.aspx?SectionName=practice/privacy.htm.

For additional information about privacy-related FTC investigations and settlements or any other questions, please contact Lydia Parnes at lparnes@wsgr.com or (202) 973-8801; Seth Silber at ssilber@wsgr.com or (202) 973-8824; Gerry Stegmaier at gstegmaier@wsgr.com or (202) 973-8809; Edward Holman at eholman@wsgr.com or (202) 973-8804; or Matt Staples at mstaples@wsgr.com or (206) 883-2583.

WSGR

Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

This WSGR Alert was sent to our clients and interested parties via email on May 10, 2012.
To receive future WSGR Alerts and newsletters via email, please contact Marketing at wsgr_resource@wsgr.com and ask to be added to our mailing list.

650 Page Mill Road
Palo Alto, CA 94304-1050
Tel: (650) 493-9300 Fax: (650) 493-6811
email: wsgr_resource@wsgr.com

www.wsgr.com