Alert!

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

Privacy | Emerging Companies

MAY 15, 2012

FTC Consent Order Requires Myspace Privacy Assessments for 20 Years: How Can You Keep the FTC Out of Your Space?

BY CYNTHIA J. LAROSE, CIPP/US AND ADAM M. VENESS

Once again, the Federal Trade Commission (FTC) has issued a warning to companies with online privacy policies: if your privacy policy misrepresents protection of users' personal information *either directly or indirectly*, you risk being charged with unfair and deceptive business practices under the FTC Act. Most recently, the FTC entered into an agreement with Myspace and issued a consent order to settle a complaint it filed against the social networking website. This alert will examine the important components of the FTC complaint, focusing on how Myspace indirectly shares its users' personally identifiable information (PII) in violation of its own privacy policy, and the FTC consent order, which provides yet another road map for companies to stay on the "right" side of the privacy road.

The Complaint

Specifically, the FTC alleged that Myspace's actions contradicted its own privacy policy in the following ways:

- ***Myspace Policy:*** Myspace's privacy policy represents that it will not share users' PII except as described in its privacy policy, including sharing that information with third parties, without first giving notice to and receiving permission from that user.
    - ***Violation:*** The FTC alleged, however, that Myspace violated its own privacy policy by providing the "FriendID" of its users to third-party advertisers. Advertisers could then use the FriendID to access a user's Myspace profile page and obtain the user's PII, which generally included the user's full name.
- ***Myspace Policy:*** Myspace's privacy policy promises users that the means through which it customizes ads does not allow advertisers to access PII or individually identify users.
    - ***Violation:*** Again, the FTC alleged that by providing advertisers with a user's FriendID, Myspace indirectly allowed advertisers to identify users and access their PII.
- ***Myspace Policy:*** Myspace's privacy policy represents that users' web browsing activity shared with advertisers is anonymized.
    - ***Violation:*** The FTC alleged that when Myspace provided a user's FriendID to an advertiser, which indirectly allowed the advertiser to access the user's PII, the advertiser can link the PII to tracking cookies it places on the user's computer that allow the advertiser to track a user's web browsing activity.

- ***Myspace Policy:*** Myspace claims in its privacy policy that it is compliant with the U.S.-E.U. Safe Harbor Framework which requires Myspace to provide users with notice regarding the purposes which it collects and uses information about the users, and choice regarding whether a user's PII is to be disclosed to a third party or used for a purpose which is incompatible for which it was originally collected.

    - ***Violation:*** The FTC alleged that Myspace failed to provide the requisite notice and choice under the U.S.-E.U. Safe Harbor by failing to provide notice or choice regarding the use of the users' PII.

The result of the FTC's analysis of each of these "misstatements" in the Myspace privacy policy was an FTC finding that Myspace made misrepresentations to its users and the allegation in the Complaint that Myspace's actions on this front were false and misleading and constituted unfair and deceptive business practices under the FTC Act.

The Agreement and Consent Order

To resolve the FTC's complaint and allegations listed above, Myspace and the FTC entered into an Agreement and Consent Order (FTC Order). The FTC Order requires Myspace to take the following actions to remedy its currently inadequate procedures related to how it protects and manages user PII, and how it discloses those procedures to users:

- Myspace shall not misrepresent the extent to which it maintains and protects the privacy and confidentiality of user PII, including the purposes for which it collects and discloses PII and the extent to which it makes or has made PII accessible to third parties.
- Myspace shall not misrepresent the extent to which it is a member of, adheres to, complies with, is certified by, is endorsed by or otherwise participates in any privacy, security, or any other compliance program sponsored by the government or other entity, including the U.S.-E.U. Safe Harbor Framework.
- Myspace must establish and maintain a comprehensive privacy program that is reasonably designed to address privacy risks and protect the privacy and confidentiality of PII, including:
    - designating an employee or employees to coordinate and be responsible for the privacy program;
    - indentifying reasonably foreseeable and material risks of disclosing PII;
    - designing and implementing reasonable privacy controls and procedures;
    - developing and using reasonable steps to select and retain service providers capable of appropriately protecting the privacy of PII they receive from Myspace and requiring those service providers to implement their own privacy protections; and
    - evaluating and adjusting Myspace's privacy program in light of its findings as a result of its new privacy controls and procedures or due to changes in Myspace's business.
- Myspace is required to obtain an initial and subsequent biennial assessment and report from a qualified and independent third-party professional that is approved by the FTC. Myspace must undergo the first assessment within 180 days of the FTC Order, and additional assessments each two-year period for twenty years thereafter.
- Myspace must maintain and make available to the FTC, for a period of five years, a copy of all widely disseminated statements that describe Myspace's privacy protections, consumer complaints relating to conduct prohibited by the FTC Order, subpoenas relating to Myspace's compliance with the FTC Order, documents questioning Myspace's compliance with the FTC Order, and all materials relied on by the third party in preparing its assessments.

- Myspace must deliver a copy of the FTC Order to various parties, including all current and former employees, directors, and officers.
- Myspace must notify the FTC at least thirty (30) days before any change in the corporation that may affect Myspace's compliance obligations, including various change of control scenarios such as a merger or sale of the company.

Keeping the FTC Out of Your Space

Much can be learned from how the FTC has evaluated the adequacy of Myspace's privacy policy when compared to its actual day-to-day procedures. The most important thing to take away from the FTC Order and its allegations in the complaint is that companies must *practice what they promise*. Superficially complying with your privacy policy will not pass the FTC's strict standards when it comes to accurate and adequate privacy policy disclosure. Companies must evaluate how their current practices may even *indirectly* provide customer PII to third parties and violate the company's privacy policy. The following are a few important steps you should take to keep the FTC out of your space:

Review your privacy policy, and then review it again. When is the last time that your company undertook a review of its privacy policy and data collection activities? Two years ago? Longer? No idea? Although this seems obvious, many companies fail to continually update and review their privacy policies to ensure that they are still complying with the terms they have established. You should particularly focus on what you have promised your customers or users with regard to what PII you will disclose to third parties, and how you will disclose it. Then look at your actual practices with regard to how you manage and disclose customer PII to third parties and make sure you truly practice what you promise. If your privacy policy states that you comply with the U.S.-E.U. Safe Harbor Framework ensure that your data use and collection practices comply with *all seven* of the Safe Harbor Privacy Principles: Notice, Choice, Onward Transfer (transfer to third parties), Access, Security, Data Integrity, and Enforcement. You cannot pick and choose and still be Safe Harbor-compliant.

Don't Let Default Be Your Fault. Much of the FTC's complaint focused on Myspace's default settings which displayed a user's full name on their profile page. When advertisers obtained the FriendID from Myspace, they were almost certainly then given access to the user's full name because of the default setting. You should examine your default settings to ensure that your users are not disclosing PII to third parties unless they have expressly agreed to do so, and unless it is absolutely necessary. Ensuring that you maintain a high level of privacy protection under your default settings may prevent third parties from indirectly accessing users' PII. Default settings should be reviewed each time that new functionality is added, technical solutions or plug-ins are changed, and at least annually.

Indirect Access Can Still Mean Direct Liability. Aside from understanding the direct implications of how you share customer information with third parties, you should perform your own assessment regarding how third parties could use the limited information that you provide them as a stepping stone to greater access to customer PII. As Myspace now knows, the FTC will closely scrutinize even the *indirect* implications of how you handle customer PII compared to what you promise customers in your privacy policy.

Best Practices. Why wait until the FTC files a complaint against you to implement procedures and designate staff to handle privacy and PII concerns? The best way to prevent your company from falling asleep at the wheel is to implement formal privacy practices and procedures. The first step in doing so is to designate at least one person, either in-house or a friendly neighborhood Mintz Levin privacy attorney, to be in charge of all things privacy related. Going forward that person should regularly evaluate your company's privacy policy and compliance with that policy, and prepare a report concerning his or her evaluation. This process will ensure that your privacy policy talks the talk, and your procedures walk the walk.

* * *

View Mintz Levin's Privacy & Security attorneys.

View Mintz Levin's Venture Capital & Emerging Companies attorneys.

Follow Us

1912-0512-NAT-PRIV