D&G | Davis & Gilbert LLP
ATTORNEYS AT LAW

DECEMBER 2011

ADVERTISING, MARKETING & PROMOTIONS

>>ALERT

FACEBOOK-FTC SETTLEMENT RESOLVES MULTIPLE PRIVACY COMPLAINTS WITH THE DOMINANT SOCIAL NETWORK

Facebook's settlement of Federal Trade Commission (FTC) allegations that it misrepresented its privacy practices to consumers resolves numerous complaints over Facebook's privacy practices and may be viewed as a model for how interactive companies in the United States should handle consumer privacy issues.

The settlement, which is open for comment until December 30, stems from an FTC investigation following complaints filed with the FTC over Facebook's privacy practices.

Under the settlement, Facebook is required to take a number of specific remedial steps over the next 20 years, as discussed below.

THE COMPLAINT

The FTC alleged a number of violations of the Federal Trade Commission Act (the FTC Act) in its complaint, including that:

- Facebook misrepresented how a user's profile information would be used based upon the user's privacy settings. Third party platform applications and advertisers had access to user profile information through Facebook despite user settings to control or restrict access that might indicate the contrary.
- Facebook made material changes to its privacy policy without making proper disclosures to users.
- Facebook applied these material changes retroactively to previously collected information.
- Facebook's "Verified Apps Program" did not in fact verify the security of third party applications on Facebook.
- Facebook continued to provide access to photos and videos via unique content URLs after a user had deleted or deactivated his or her account.
- Facebook failed to comply with the U.S.-EU Safe Harbor Framework.

THE SETTLEMENT

The Consent Order resolving the investigation by the FTC into these Facebook practices imposes a number of requirements on Facebook.

No Further Misrepresentations

Facebook is prohibited from misrepresenting how it maintains the privacy and security of what the FTC calls "Covered Information." Covered Information includes personally identifiable information such as name, address, photos, videos, telephone numbers and other persistent identifiers. It also includes the Internet Protocol (IP) address assigned to the user.

>> continues on next page

THE BOTTOM LINE

With the FTC active in this area, and with privacy legislation pending in Congress, companies must develop, maintain, and follow clear privacy practices to limit the risk of becoming immersed in a federal investigation or proceeding, or of having to admit – as Facebook founder Mark Zuckerberg did in a blog post the day the settlement was announced – that "we've made a bunch of mistakes."

Prior Consent

The settlement requires that Facebook obtain a user's affirmative express consent (i.e., an opt-in) prior to any sharing by Facebook of the user's nonpublic user information with any third party, when that sharing would "materially exceed" the restrictions imposed by the user's privacy setting. While this requirement also applies to new products and services that Facebook may develop over the next 20 years, Facebook may seek a modification to this requirement based upon technological changes in the future.

It is important to note that to obtain a user's consent, Facebook must disclose the information practices to the user "separate and apart from any privacy policy, data use policy, statement of rights and responsibilities page, or other similar document." Therefore, even an accurate and clearly drafted privacy policy would be insufficient. This information may not be buried in a privacy policy, but rather, must be presented to the user in a more intuitive manner.

Privacy Program

The settlement also requires that Facebook develop a written "comprehensive privacy program" reasonably designed to address privacy risks related to the development and management of new and existing products and services for consumers, and to protect the privacy and confidentiality of Covered Information. This requirement matches the trend in state and federal laws to require written information security programs (click here to see the prior Davis & Gilbert alert regarding the Massachusetts Data Security Regulations).

Facebook agreed that it would designate an employee to be in charge of the privacy program, and it has already announced that one attorney will serve as Chief Privacy Officer for Policy and a second attorney will serve as Chief Privacy Officer for Products.

Terminate Access to User Profile Information

Facebook must implement a system to ensure that Covered Information cannot be accessed by a third party (such as an advertiser) 30 days after a user has deleted this information or his or her account.

20 Years of Assessments and Reports

A key aspect of the settlement requires that Facebook obtain independent initial and biennial privacy assessments and reports. The initial privacy assessment will cover the first 180 days after the settlement and is to be delivered to the FTC. Thereafter, privacy assessments must be conducted every 2 years for the next 20 years.

FOR MORE INFORMATION

Gary A. Kibel
Partner
212.468.4918
gkibel@dglaw.com

or the D&G attorney with whom you have regular contact.

Davis & Gilbert LLP
T: 212.468.4800
1740 Broadway, New York, NY 10019
www.dglaw.com