

Articles

Lessons from the Facebook Privacy Fiasco

Dean W. Harvey

IP and Technology Developments - January 2012

January 19, 2012

Facebook is a wildly popular social media site which allows users to share information about themselves, send messages to friends, play games and join common interest groups. It is the most visited site in the U.S., with over 100 million active U.S. users and hundreds of millions of active users worldwide.¹

During the week of April 18, 2010, Facebook made material changes to the way that its users' personal information was classified and disclosed. The changes resulted in complicated privacy settings that confused users, and in some cases, personal data which users had previously designated as private was allegedly made public. As a result, a group of petitioners, including the Electronic Privacy Information Center ("EPIC"), filed a complaint with the FTC requesting that the Commission investigate Facebook to determine whether it engaged in unfair or deceptive trade practices ("Complaint").

Allegations

The Complaint claimed that Facebook violated its own privacy policy, disclosed personal information of Facebook users without consent, and engaged in unfair and deceptive trade practices. Specifically, the Complaint alleged that among other things:

- Facebook made publicly available personal information which users had previously designated as private.²
- Facebook disclosed to third parties information that users designated as available to Friends Only (including to third-party websites, applications, other Facebook users and outsiders who happen on to Facebook pages).³
- Facebook claimed that none of user's information was shared with sites visited via a plug-in (such as the Like button, Recommend button, etc.). However, such plug-ins may reveal users' personal data to such websites without consent.⁴
- Facebook designed privacy settings "to confuse users and to frustrate attempts to limit the public disclosure of personal information . . ."⁵
- Although the Facebook terms which many users accepted indicated that developers would be limited to a 24-hour retention period for any user data, Facebook announced that the limit no longer exists.⁶

Angry End Users

Regardless of whether each of the above allegations is true, it is clear that Facebook's changes to its privacy practices inflamed some of its users. In support of its allegations, the EPIC Complaint included quotes from experts and users about Facebook's privacy practices such as:

"I shouldn't have to dive into complicated settings that give the fiction of privacy control but don't, since they are so hard to understand that they're ignored. I shouldn't need a flowchart to understand what friends of friends of friends can share with others. Things should be naturally clear and easy for me."⁷

"Facebook constantly is changing the privacy rules and I'm forced to hack through the jungle of their well-hidden privacy controls to prune out new types of permissions Facebook recently added. I have no idea how much of my personal information was released before I learned of a new angle the company has developed to give my information to others."⁸

"'Instant Personalization' is turned on automatically by default. That means instead of giving you the option to 'opt-in' and give your permission for this to happen, Facebook is making you 'opt-out,' essentially using your information how they see fit unless you make the extra effort to turn that feature off."⁹

Articles

“Facebook has become Big Brother. Facebook has succeeded in giving its users the allusion [sic] of privacy on a public site, leaving everyone to become complacent about keeping track of the myriad changes going on behind the scenes. The constant changes assure Facebook that you can never keep all your information private.”¹⁰

The Proposed Settlement

The FTC investigated the Complaint and ultimately agreed to a proposed settlement agreement containing a consent order.¹¹ Without admitting liability, Facebook has agreed to a settlement that among other things requires the following:

- Facebook must establish, implement and maintain a comprehensive privacy program designed to: (1) address privacy risks related to the development and management of new and existing product and services for consumers; and (2) protect the privacy and security of covered information.¹²
- Facebook must obtain an independent third-party audit every other year for the next 20 years certifying that the Facebook privacy program meets or exceeds the requirements of the FTC order;¹³
- Facebook is required to obtain express consent from a user before enacting changes that override the user's privacy preferences;¹⁴
- Facebook is required to prevent third parties from accessing user data after the user has deleted (with exceptions for legal compliance and fraud prevention).¹⁵

Lessons from the Complaint and Order

Facebook received significant negative publicity, incurred legal costs and business disruption associated with a government investigation, and will incur compliance costs for the next 20 years as a result of the proposed settlement. Businesses that deal with consumer information would be well advised to learn from Facebook's experience. There are several lessons that businesses can draw from the Facebook privacy fiasco in dealing with data privacy issues.

A. Don't Make Your Customers Angry

Facebook's intentions in making the changes to its privacy settings may have been entirely good. For example, Facebook may have honestly been trying to improve its user experience. However, the changes significantly angered some of its customers. The lesson to be learned here is that intentions don't matter if you anger your customers with your changes. The ultimate user experience may be better, the site may objectively offer more functionality, but none of that matters if users are offended by the process.

Businesses need to achieve innovations and improvements in the use of consumer data with user consent, and without breaking prior promises. Keeping your customers satisfied isn't just good business, it also greatly reduces the likelihood that they will be filing deceptive trade practice complaints with the FTC.

B. Keep the Privacy Settings Simple

Much of the Complaint is dedicated to showing how complicated the Facebook settings are, and many of the quoted user statements underscore that issue as well. Such complexity often leads to errors (such as permitting applications to access personal information of a user through the user's friends). Even when the settings work perfectly, the average person may find such complexity frustrating, leading to angry end users.

It is important to keep privacy policies simple and establish privacy settings so that they can be easily understood by an average user. Informed consent is really only obtained when the user understands the policy or setting to which he or she is consenting.

Articles

C. Consider How Applications Access User Data

When drafting a privacy policy, it is easy to focus on the organization's use of data for internal purposes and with its vendors and subcontractors. However, special care must be taken with use of consumers' data by software applications. For example, it is alleged that Facebook indicated applications only had access to the user information necessary for their operation, when the applications in fact had access to all user information.

In order to accurately describe how applications use consumer data in your privacy policy, you have to investigate the operation of the applications on your site, document that operation, and establish IT policies and procedures governing the use of data by new or modified applications. If you do not take these steps, it is likely that any promise regarding the use of data by applications will become misleading over time as the applications change and are updated.

D. Monitor Linking and Other Advertising Arrangements

Linking and advertising arrangements are the lifeblood of many sites. In order to make accurate statements about the types of data shared in such arrangements, it is necessary to review the contracts to understand what types of user data will be shared through business processes. However, this is not sufficient to ensure that the full use of data is understood. Just as with applications, it is necessary to investigate what data is collected or shared in the process of passing the user to the third party. Similar to applications, it is important to document what user data is permitted to be shared with advertisers and other third parties, and to establish IT policies and procedures to enforce such permitted uses.

E. Don't Make User Data Public Without Consent.

One of the problems many businesses face with privacy policies is that as their business changes, the types of user data that they want to access or use may change as well. However, it is important to remember that no matter what the motive, if you have promised to keep certain elements of user data private in your privacy policy, you should not make it public by default without first obtaining affirmative user consent.

Privacy compliance is difficult in a changing online environment, even for businesses that don't have hundreds of millions of users. The Complaint and Order in the Facebook matter highlight some of the many ways that a business can go wrong in protecting private consumer information. In order to successfully protect such information, a business which deals extensively with consumer data should establish, maintain, update and enforce a comprehensive privacy and security program, which takes into account material risks as well as lessons learned from the experience of other companies, such as Facebook.

For more information, please email IPandTech@andrewskurth.com.

Click the link below to contact the author of this article.

Dean W. Harvey

Other articles from this issue of *IP and Technology Developments*.

- The America Invents Act—From the Perspective of the Small Business
- Post-Grant Review Aspect of New Patent Law
- Taiwan IP Update

Download a PDF of the entire issue.

Articles

1. *In the Matter of Facebook, Inc.*, Complaint paragraph 31 (May 5, 2010); available at http://epic.org/privacy/facebook/EPIC_FTC_FB_Complaint.pdf.
2. *Id.* at paragraph 55.
3. *Id.* at paragraph 59.
4. *Id.* at paragraph 65.
5. *Id.* at paragraph 64.
6. *Id.* at paragraphs 92-94.
7. *Id.* at paragraph 95.
8. *Id.* at paragraph 97.
9. *Id.* at paragraph 98.
10. *Id.* at paragraph 106.
11. *In the Matter of Facebook, Inc.* File No. 092 3184, Agreement Containing Consent Order (“Order”); available at <http://www.ftc.gov/os/caselist/0923184/111129facebookagree.pdf>.
12. *Id.* at paragraph IV.
13. *Id.* at paragraph V.
14. *Id.* at paragraph II.
15. *Id.* at paragraph III.