EXHIBIT 6

Facebook Can Track Web Browsing Without Cookies

By DJ Pangburn Tuesday, October 11, 2011

According to the Electronic Frontier Foundation, quoting various posts and papers by hackers and researchers, Facebook has two types of cookies for data collection and one method that works without cookies.

The Electronic Frontier Foundation cites a September 25th, 2011 blog post by hacker and writer Nik Cubrilovic that proved Facebook's session cookie was not being deleted upon log-out. Facebook responded with a "fix-it," but it raises serious concerns about whether one can effectively log-out of Facebook and whether or not Facebook can track users without the benefit of cookies.

According to Cubrilovic, he waited for a year to hear from Facebook on this privacy issue that he discovered, emailing them and reaching multiple dead-ends.

Two days later, on September 27th, Cubrilovic noted, "In summary, Facebook has made changes to the logout process and they have explained each part of the process and the cookies that the site uses in detail... They want to retain the ability to track browsers after logout for safety and spam purposes, and they want to be able to log page requests for performance reasons etc."

EFF, however, is unequivocal in stating, "Facebook can track web browsing history without cookies."

"Facebook is able to collect data about your browser – including your IP address and a range of facts about your browser – without ever installing a cookie. They can use this data to build a record of every time you load a page with embedded Facebook content," added the EFF.

This ability to track users outside of Facebook is particularly troubling.

EFF states, "It's clear that Facebook does extensive cross-domain tracking, with two types of cookies and even without. With this data, Facebook could create a detailed portrait of how you use the Internet: what sites you visit, how frequently you load them, what time of day you like to access them. This could point to more than your shopping habits – it could provide a candid window into health concerns, political interests, reading habits, sexual preferences, religious affiliations, and much more."

That Facebook keeps this data on file for 90 days (before it's discarded or made anonymous) is a legitimate privacy concern and it could certainly be useful in the event U.S. intelligence services desires to build a profile of a particular user's web browsing.

This sort of ability has already raised concerns amongst lawmakers and privacy advocates.

Four days after Cubrilovic posted on the privacy concern, Reps. Edward Markey and Joe Barton stated that they "remain concerned about the privacy implications for Facebook's 800 million subscribers," asking the Federal Trade Commission to investigate the issue.

In the meantime, what can Facebook users do to avoid the watchful eye of Facebook? EFF provides the following advice:

- Install Firefox addons like Ghostery, ShareMeNot, Abine's Taco, and/or AdBlockPlus to limit online tracking. None of these is perfect and each works a little different; check out this guide for a discussion. Also consider installing the Priv3 Firefox extension, which is still in beta.
- Use private browsing mode.
- Adjust the settings in your browser to delete all cookies upon closing. Clear your cookies when leaving a social networking site, and log out of Facebook before browsing the web. You should consider having one browser strictly for logging into your Facebook account and one browser for the rest of your web usage.
- Send a quick complaint to the Federal Trade Commission via their online web complaint form. The FTC uses its complaint form to gauge what issues concern consumers and may launch investigations if there is sufficient user interest.
- Support privacy legislation like the Rockefeller Do Not Track bill, which will give users a voice when it comes to online tracking.