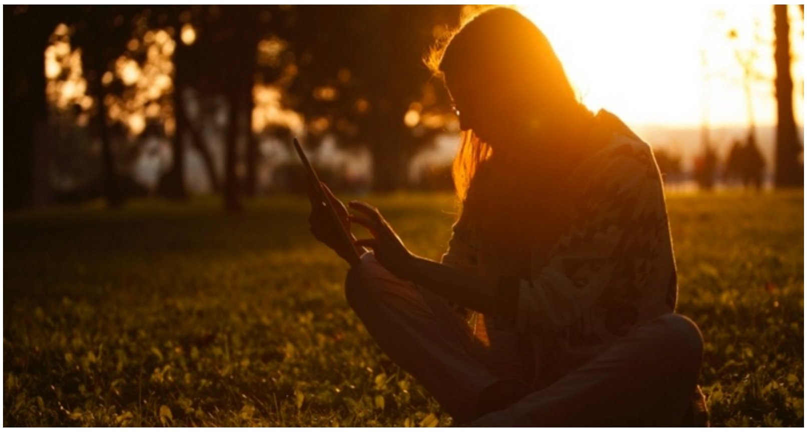
New American

Written by C. Mitchell Shaw on April 18, 2015

Facebook Tracks Users Without Consent, but Users Can Take Control



Facebook has spent years earning a notorious reputation for sacrificing users' privacy for increased advertising revenue. Now the social networking giant may be in serious legal trouble with the European Union for violating EU laws about tracking Internet users without their consent.

A report issued by ICRI/CIR and iMinds-SMIT for the Belgian Privacy Commission claims that Facebook is tracking Internet users — even those who are not logged into a Facebook account — and capturing their browsing habits across the web. In many cases, the tracking involves users who do not even have a Facebook account.

The method by which Facebook tracks users is the ubiquitous "Like" button found on most websites. Sites that have the button must allow certain computer scripts to run. These scripts allow Facebook to see what websites users visit even if the users do not click the button. Facebook then uses that information to allow advertisers to direct their ads to targeted users. The practice is controversial in the United States and illegal in the European Union. The issue at stake is that if users agree to have their browsing habits tracked across the Web, it is a valuable service; if they do not, it is an invasion of their privacy. The "Like" button simply appearing on a website does not amount to a user's consent.

To make matters worse, Facebook also ignores "Do Not Track" requests from users who activate that setting in browsers such as Chrome, Firefox, and Safari. In doing so, Facebook joins ranks with Google and Yahoo as well as a slew of disreputable sites.

These tracking policies — which went into effect June 2014 — are a reversal of the social network's previous policies which were introduced after a $15-billion class action suit for invasive practices in 2011. With the introduction of the "Like" button on non-Facebook pages, Facebook initially claimed the privacy issue to be a bug in the software. The company now sells the bug as a feature to advertisers.

The issue is deeper than just whether Facebook can see what other sites users visit — though that is disturbing enough on its own. There are serious security concerns as well, because the scripts used create a back door that hackers and others can manipulate to further invade the privacy and security of users.

After coming under fire for using persistent cookies (small programs that are loaded on users' computers to maintain certain settings and allow tracking), Facebook introduced the "Tracking Pixel." It is a 1×1 gif file, invisible to the naked eye in most cases, which allows the company to track users even after they leave the site. Since users who do not even have a Facebook account and have not agreed to Facebook's privacy policy are tracked as well, such tracking cannot be consensual. Because the pixel is invisible, very few users (whether they have an account or not) could even be aware of it.

As the EU case continues to be investigated, it is likely that Facebook will face serious legal problems and sizable fines. EU laws do more to protect the privacy of individuals than do those in America. Fortunately, there are steps American Internet users can take to protect themselves while they wait for their laws to catch up to those in the European Union. In a previous article, *The New American* outlined several methods for Internet users to protect themselves from privacy-invading tools used by both overreaching governments and nosy corporations.

Many of the tips in that article would secure users from the types of security issues related to Facebook's invasion of users' privacy. Downloading and installing a browser that is more privacy-friendly would be a great starting point. The Firefox browser, which can be downloaded for free from www.mozilla.org, fits the bill nicely. It is much more secure than Internet Explorer, even with the default settings, and can be made even more secure by changing a few settings and installing a few add-ons.

By disabling all third-party cookies and setting Flash to run only on sites the user approves, many of the scripts required for tracking will not work. To make it even more difficult for governments and corporations to track users, we also recommend downloading and installing the HTTPS Everywhere plugin from www.eff.org. This will force a secure connection on all sites that offer it. It's not perfect, but it's the same level of security/encryption used by banking websites.

For blocking ads altogether, users can install the AdBlock Plus add-on from Firefox's settings and never see another ad. The practical benefit of this (besides getting rid of Internet clutter in the form of ads and popups) is that each of those ads may have its own tracking capabilities. Preventing them from working goes a long way to protecting users' identities and systems.

Finally, to lock down all the types of scripts that aid in tracking, users can install the NoScript add-on and block all scripts from running. Be aware that this may cause some features of websites to stop working and other websites to not display at all. The settings can be adjusted on a site-by-site basis, though, and at least users will have both knowledge about — and control over — what is happening on their machines and with their data.

Users who take these steps will be much more difficult (if not impossible) to track. The cost in convenience is a worthwhile tradeoff for the added security and privacy.