Facebook â€˜Invisibleâ€™ Sharing Worries Privacy Advocates

As Facebook officials unveiled dozens of new applications this week for automatic sharing of profile content, privacy advocates warn that users should worry not only about what is openly shared, but also about what they claim is shared behind-the-scenes to the owners of those applications.

“Our objection is that users generally have no idea how much personal information is being transferred to the application partners and co-hosts,” said Marc Rotenberg, executive director of the Electronic Privacy Information Center. “We are most concerned with the invisible part of the sharing."

Facebook on Jan. 18 introduced a suite of more than 60 Open Graph applications for Timeline with partners including eBay, TripAdvisor, Zynga, Ticketfly and Ticketmaster. The social media company also invited more partners to develop applications for the site.

The Open Graph application are being made available through Facebook Timeline, a new profile format that currently is optional for most users, but is expected to be mandatory soon.

Users of Open Graph applications on Facebook will be able to automatically share status updates on what music they are listening to, films they are watching and items they are buying, among other activities. The Open Graph applications currently are voluntary and are managed with Facebook privacy controls.

Nonetheless, concerns are being raised about privacy, mostly about possible inadvertent public sharing or oversharing of information, once the automatic sharing applications are turned on. The privacy risks of content leaking to third parties applies to all Facebook users, but federal employees and executives need to be particularly watchful of what information they share. Those in sensitive positions, such as in law enforcement or counterterrorism, or with security clearances, face heightened risks.

While the impact of the new features isn't yet clear, Facebook in general poses risks for federal employees in sensitive positions. Even semeingly innocent friend connections or app use could lead to trouble in some cases. For example, security clearance forms require the applicant to disclose associations with foreign nationals. Do Facebook friends count, especially if they're only distant acquaintances?

"I had a client who lost her security clearance after using an online chat room," wrote attorney Greg Rinckey in a column

published in 2009. "She was seeking advice on how to beat a computer game while attending a gaming convention. The gaming experts she chatted with online were foreign intelligence agents working out of China."

Initial information available about the Open Graph applications did not specify whether, or

how much, user information would be shared with the application providers and how that would be managed. Facebook officials were not immediately available for clarification.

Technical experts and privacy advocates are warning of potential privacy risks because of the possibility of Facebook personal profile content being shared with the application providers.

“Having ‘apps’ connected to your Facebook, LinkedIn or Twitter profiles provides an open door for the third party behind the app to access your profile and all of your personal data within,” according to a Jan. 20 article

in SiteProNews.

The article also quotes Neil Lathwood, technical director for UKFast, a tech company in the United Kingdom, cautioning that personal information leaked to application providers could be fodder for cyber thieves.

“Facebook acts as a narration of our lives and with the introduction of the new Timeline feature, more people are filling the gaps in their profiles, adding illnesses, significant events and employment details to name a few. This information is incredibly valuable to identity thieves and cybercriminals,” Lathwood said in the article.

Officials in Germany also have expressed privacy concerns about Facebook application providers having access to personal information on the site through the use of the “Like” button, according to a HuffingtonPost article

.

In August, a regional data protection commissioner ordered the shut down of Facebook fan pages for state institutions and removal of “Like” buttons from those pages. The commissioner said the Facebook “Like” button policies violated German and European privacy laws.