Lawsuit Claims Facebook Is Reading Your Private Messages

MSN news

Facebook could be reading your private messages to help advertisers figure out what you want to buy.

Facebook could be reading your private messages to help advertisers figure out what you want to buy, so you know there are definitely going to be users (and lawyers) who aren't happy about that.

The company was hit this week with a class action lawsuit alleging it is scanning private messages for links and passing the information along to advertisers, in violation of California's Electronic Communications Privacy Act . The suit, brought by Matthew Campbell and Michael Hurley on behalf of all Facebook users, claims that the sneaky practice is extremely lucrative:

"Representing to users that the content of Facebook messages is "private" creates an especially profitable opportunity for Facebook, because users who believe they are communicating on a service free from surveillance are likely to reveal facts about themselves that they would not reveal had they known the content was being monitored. Thus, Facebook has positioned itself to acquire pieces of the users' profiles that are likely unavailable to other data aggregators".

The suit alleges that Facebook uses private messages to "mine user data and profit from those data by sharing them with third parties – namely, advertisers, marketers, and other data aggregators." Campbell and Hurley relied on information from an independent security researcher that shows that Facebook clicked on links sent through private messages. According to the court filing:

"Contrary to its representations, "private" Facebook messages are systematically intercepted by the Company in an effort to learn the contents of the users' communications. In the course of the last year, independent security researchers discovered that Facebook reviews the contents of its users' private Facebook messages for purposes unrelated to the facilitation of message transmission. When a user composes a Facebook message and includes a link to a third party website (a "URL"), the Company scans the content of the Facebook message, follows the enclosed link, and searches for information to profile the message-sender's web activity".

The suit further explains that Facebook will "like" the link – when possible – in this way passing the secret information along to the company whose page has been "liked":

"Upon information and belief, where a web page does contain a "Like button, the web crawlers transmit this information back to Facebook. Upon information and belief, Facebook then uses these data to register the URL sent via private message as a "Like" for the web page. Upon information and belief, Facebook further provides these data to the web page at issue, in the

form of analytical analysis of web traffic to that site by Facebook users. Upon information and belief, Facebook further uses these data to build and refine user profiles. Upon information and belief, Facebook's interception occurs in transit, in transmission, and/or in transfer of users' private messages."

PCWorld explains that Swiss information security firm High-Tech Bridge (HTB) did some research in August that outs Facebook for looking at messages between users. HTB sent trackable links through the private messaging services of 50 social media sites, and checked to see which of these clicked on the embedded URL. After 10 days of the experiment, they found that only 6 companies took the bait – but those six include Facebook, Twitter and Google +.

A Facebook spokesperson denied the claims made by Campbell and Hurley, saying "We believe the allegations are without merit and we will defend ourselves vigorously," and at least one security expert has come to the firm's defense. Graham Cluley writes on his blog that Facebook might be clicking on links to protect users, not to boost ad sales:

"I don't see anything necessarily wrong in principle with online services automatically scanning messages between individuals, and examining the links that they are sharing. Indeed, if Facebook's security team didn't have such systems in place I would believe them to be disturbingly lax in their duty of care for users. After all, if you didn't properly scan and check links there's a very real risk that spam, scams, phishing attacks, and malicious URLs designed to infect recipients' computers with malware could run rife".

This doesn't explain, however, why 44 other prominent social media sites like LinkedIn, Gmail, and AOL didn't click on private links. Or why Facebook has already been criticized for its privacy policy in the form of a separate class action suit finalized in September.