

CLICK HERE TO SAVE OVER **75%** ON A STUDENT GIFT SUBSCRIPTION

THE WALL STREET JOURNAL

Dow Jones Reprints: This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers, use the Order Reprints tool at the bottom of any article or visit www.djreprints.com

See a sample reprint in PDF format. Order a reprint of this article now

THE WALL STREET JOURNAL

WSJ.com

WHAT THEY KNOW | OCTOBER 18, 2010

Facebook in Privacy Breach

Top-Ranked Applications Transmit Personal IDs, a Journal Investigation Finds

By EMILY STEEL And GEOFFREY A. FOWLER



Kim White Bloomberg

Facebook founder and CEO Mark Zuckerberg addressed the F8 developer conference this spring.

Many of the most popular applications, or "apps," on the social-networking site Facebook Inc. have been transmitting identifying information—in effect, providing access to people's names and, in some cases, their friends' names—to dozens of advertising and Internet tracking companies, a Wall Street Journal investigation has found.

The issue affects tens of millions of Facebook app users, including people who set their profiles to Facebook's strictest privacy settings. The practice breaks Facebook's rules, and renews questions about its ability to keep identifiable information about its users' activities secure.

More From Digits

[Facebook Faces Suit Over Earlier Breach](#)
[How the Data Leaks Happen](#)

place. On Sunday, a Facebook spokesman said it is taking steps to "dramatically limit" the exposure of users' personal information.

"A Facebook user ID may be inadvertently shared by a user's Internet browser or by an application," the spokesman said. Knowledge of an ID "does not permit access to anyone's private information on Facebook," he said, adding that the company would introduce new technology to contain the problem identified by the Journal.

"Our technical systems have always been complemented by strong policy enforcement, and we will continue to rely on both to keep people in control of their information," the Facebook official said.

More From the Series

[Web's New Goldmine: Your Secrets](#)
[Personal Details Exposed Via Biggest Sites](#)
[Microsoft Quashed Bid to Boost Web Privacy](#)
[On Cutting Edge, Anonymity in Name Only](#)
[Stalking by Cellphone](#)
[Google Agonizes Over Privacy](#)
['Scrapers' Dig Deep for Data on Web](#)
[The Tracking Ecosystem](#)
[On the Web, Children Face Intensive Tracking](#)
[Complete Coverage: What They Know](#)

The problem has ties to the growing field of companies that build detailed databases on people in order to track them online—a practice the Journal has been examining in its What They Know series. It's unclear how long the breach was in

"Apps" are pieces of software that let Facebook's 500 million users play games or share common interests with one another. The Journal found that all of the 10 most popular apps on Facebook were transmitting users' IDs to outside companies.

The apps, ranked by research company Inside Network Inc. (based on monthly users), include Zynga Game Network Inc.'s FarmVille, with 59 million users, and Texas HoldEm Poker and FrontierVille. Three of the top 10 apps, including FarmVille, also have been transmitting personal

Most apps aren't made by Facebook, but by independent software developers. Several apps became unavailable to Facebook users after the Journal informed Facebook that the apps were transmitting personal information; the specific reason for their unavailability remains unclear.

The information being transmitted is one of Facebook's basic building blocks: the unique "Facebook ID" number assigned to every user on the site. Since a Facebook user ID is a public part of any Facebook profile, anyone can use an ID number to look up a person's name, using a standard Web browser, even if that person has set all of his or her Facebook information to be private. For other users, the Facebook ID reveals information they have set to share with "everyone," including age, residence, occupation and photos.

The apps reviewed by the Journal were sending Facebook ID numbers to at least 25 advertising and data firms, several of which build profiles of Internet users by tracking their online activities.

Defenders of online tracking argue that this kind of surveillance is benign because it is conducted anonymously. In this case, however, the Journal found that one data-gathering firm, RapLeaf Inc., had linked Facebook user ID information obtained from apps to its own database of Internet users, which it sells. RapLeaf also transmitted the Facebook IDs it obtained to a dozen other firms, the Journal found.



RapLeaf said that transmission was unintentional. "We didn't do it on purpose," said Joel Jewitt, vice president of business development for RapLeaf.

Facebook said it previously has "taken steps ... to significantly limit Rapleaf's ability to use any Facebook-related data."

Facebook prohibits app makers from transferring data about users to outside advertising and data companies, even if a user agrees. The Journal's findings shed light on the challenge of policing those rules for the 550,000 apps on its site.

The Journal's findings are the latest challenge for Facebook, which has been criticized in recent years for modifying its privacy rules to expose more of a user's information. This past spring, the Journal found that Facebook was transmitting the ID numbers to advertising companies, under some circumstances, when a user clicked on an ad. Facebook subsequently discontinued the practice.

"This is an even more complicated technical challenge than a similar issue we successfully addressed last spring on Facebook.com," a Facebook spokesman said, "but one that we are committed to addressing."

The privacy issue follows Facebook's effort just this month to give its users more control over its apps, which privacy activists had cited as a potential hole in users' ability to control who sees their information. On Oct. 6, Facebook created a control panel that lets users see which apps are accessing which categories of information about them. It indicates, for example, when an application accesses a user's "basic information" (including a user ID and name). However, it doesn't detail what information friends' applications have accessed about a user.

Video From 'What They Know' Series
 All 'What They Know' videos



It's rarely a coincidence when you see Web ads for products that match your interests. WSJ's Christina Tsuei explains how advertisers use cookies to track your online habits.



Facebook apps transform Facebook into a hub for all kinds of activity, from playing games to setting up a family tree. Apps are considered an important way for Facebook to extend the usefulness of its network. The company says 70% of users use apps each month.

Applications are also a growing source of revenue beyond advertising for Facebook itself, which sells its own virtual currency that can be used to pay for games.

Following an investigation by the Canadian Privacy Commissioner, Facebook in June limited applications to accessing only the public parts of a user's profile, unless the user grants additional permission. (Canadian officials later expressed satisfaction with Facebook's steps.) Previously, applications could tap any data the user had access



A new report in the Wall Street Journal's "What They Know" series illustrates how companies like Microsoft must balance conflicting interests: helping people surf the Web with its browser to keep their mouse clicks private, and helping advertisers who want to see those clicks. WSJ's Julia Angwin, Nick Wingfield, and Jessica Vascellaro join host Simon Constable as panelists on this special Digits live show.

Facebook in Online Privacy Breach; Ap...
to, including detailed profiles and information about a user's friends.

It's not clear if developers of many of the apps transmitting Facebook ID numbers even knew that their apps were doing so. The apps were using a common Web standard, known as a "referrer," which passes on the address of the last page viewed when a user clicks on a link. On Facebook and other social-networking sites, referers can expose a user's identity.

The company says it has disabled thousands of applications at times for violating its policies. It's unclear how many, if any, of those cases involved passing user information to marketing companies.

Facebook also appeared to have shut down some applications the Journal found to be transmitting user IDs, including several created by LOLapps Media Inc., a San Francisco company backed with \$4 million in venture capital. LOLapp's applications include Gift Creator, with 3.5 million monthly active users, Quiz Creator, with 1.4 million monthly active users, Colorful Butterflies and Best Friends Gifts.

Since Friday, users attempting to access those applications received either an error message or were reverted to Facebook's home screen.

"We have taken immediate action to disable all applications that violate our terms," a Facebook spokesman said.

A spokeswoman for LOLapps Media declined to comment.

The applications transmitting Facebook IDs may have breached their own privacy policies, as well as industry standards, which say sites shouldn't share and advertisers shouldn't collect personally identifiable information without users' permission. Zynga, for example, says in its privacy policy that it "does not provide any Personally Identifiable Information to third-party advertising companies."

A Zynga spokeswoman said, "Zynga has a strict policy of not passing personally identifiable information to any third parties. We look forward to working with Facebook to refine how web technologies work to keep people in control of their information."

The most expansive use of Facebook user information uncovered by the Journal involved RapLeaf. The San Francisco company compiles and sells profiles of individuals based in part on their online activities.

The Journal found that some LOLapps applications, as well as the Family Tree application, were transmitting users' Facebook ID numbers to RapLeaf. RapLeaf then linked those ID numbers to dossiers it had previously assembled on those individuals, according to RapLeaf. RapLeaf then embedded that information in an Internet-tracking file known as a "cookie."

RapLeaf says it strips out the user's name when it embeds the information in the cookie and shares that information for ad targeting. However, The Wall Street Journal found that RapLeaf transmitted Facebook user IDs to a dozen other advertising and data firms, including Google Inc.'s Invite Media.

All 12 companies said that they didn't collect, store or use the information.

Ilya Nikolayev, chief executive of Familybuilder, maker of the Family Tree application, said in an email, "It is Familybuilder's corporate policy to keep any actual, potential, current or prior business partnerships, relationships, customer details, and any similar information confidential. As this story relates to a company other than Familybuilder, we have nothing further to contribute."

Write to Emily Steel at emily.steel@wsj.com and Geoffrey A. Fowler at geoffrey.fowler@wsj.com

More From 'What They Know'

[Web's New Goldmine: Your Secrets](#)

[Personal Details Exposed Via Biggest Websites](#)

[Microsoft Quashed Bid to Boost Web Privacy](#)

[On Web's Cutting Edge, Anonymity in Name Only](#)

[Stalking by Cellphone](#)

[Google Agonizes Over Privacy](#)

['Scrapers' Dig Deep for Data on Web](#)

[The Tracking Ecosystem](#)

On the Web, Children Face Intensive Tracking

Complete Coverage: What They Know

Copyright 2009 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our [Subscriber Agreement](#) and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com

