

## To investors who want to retire comfortably.

If you have a \$500,000 portfolio, download the guide by *Forbes* columnist and money manager Ken Fisher's firm. It's called "The 15-Minute Retirement Plan." Even if you have something else in place right now, it *still* makes sense to request your guide! [Click Here to Download Your Guide!](#)

FISHER INVESTMENTS™

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](http://www.djreprints.com)

[See a sample reprint in PDF format.](#)

[Order a reprint of this article now](#)

**THE WALL STREET JOURNAL.**

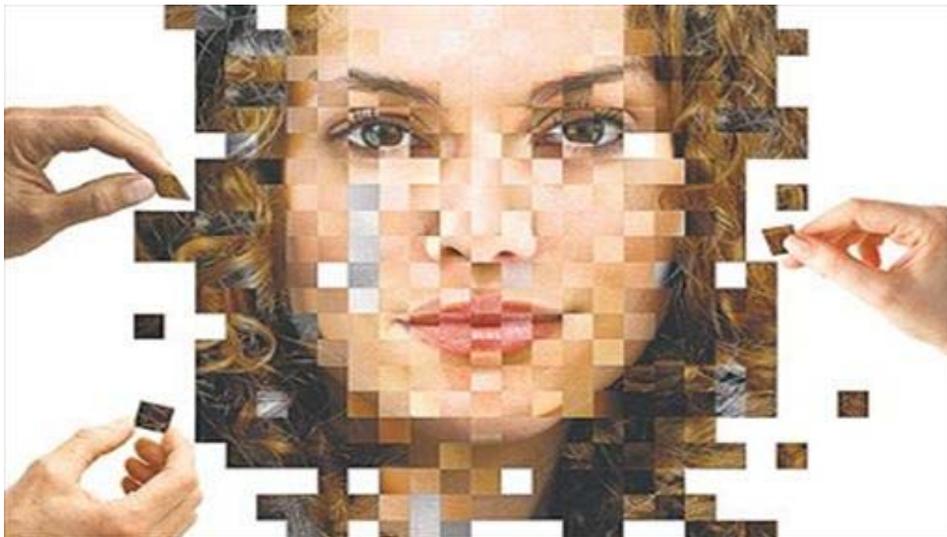
WSJ.com

TECHNOLOGY | Updated April 10, 2012, 7:48 p.m. ET

# Selling You on Facebook

*Many popular Facebook apps are obtaining sensitive information about users—and users' friends—so don't be surprised if details about your religious, political and even sexual preferences start popping up in unexpected places.*

By JULIA ANGIN and JEREMY SINGER-VINE



Apps on Facebook may be grabbing and sharing more personal information than many users realize. And even if people understand that they're sharing personal data, they often can't envision the ways it may be used in the future. WSJ's Julia Angwin explains.

Not so long ago, there was a familiar product called software. It was sold in stores, in shrink-wrapped boxes. When you bought it, all that you gave away was your credit card number or a stack of bills.

### Live Chat

[Ask your questions about Facebook apps and Digital Privacy in a live chat with the authors](#)

Now there are "apps"—stylish, discrete chunks of software that live online or in your smartphone. To "buy" an app, all you have to do is click a button. Sometimes they cost a few dollars, but many apps are free, at least in monetary terms. You often pay in another way. Apps are gateways, and when you buy an app,

there is a strong chance that you are supplying its developers with one of the most coveted commodities in today's economy: personal data.

Some of the most widely used apps on Facebook—the games, quizzes and sharing services that define the social-networking site and give it such appeal—are gathering volumes of personal information.

A Wall Street Journal examination of 100 of the most popular Facebook apps found that some seek the email addresses, current location and sexual preference, among other details, not only of app users but also of their

Facebook friends. One Yahoo service powered by Facebook requests access to a person's religious and political leanings as a condition for using it. The popular Skype service for making online phone calls seeks the Facebook photos and birthdays of its users and their friends.

### Interactive: How Grabby Are Your Facebook Apps?



### More

[Digits: How to Control What Facebook Apps See](#)

[Testing Facebook Apps: Our Methodology](#)

[What They Know: A Wall Street Journal Investigation](#)

Yahoo and Skype say that they seek the information to customize their services for users and that they are committed to protecting privacy. "Data that is shared with Yahoo is managed carefully," a Yahoo spokeswoman said.

The Journal also tested its own app, "WSJ Social," which seeks data about users' basic profile information and email and requests the ability to post an update when a user reads an article. A Journal spokeswoman says that the company asks only for information required to make the app work.

This appetite for personal data reflects a fundamental truth about Facebook and, by extension, the Internet economy as a whole: Facebook provides a free service that users pay for, in effect, by providing details about their lives, friendships, interests and activities. Facebook, in turn, uses that trove of information to attract advertisers, app makers and other business opportunities.



Getty Images

'Data is what anyone wants access to,' says the maker of an app that collects information about users and their friends.

Up until a few years ago, such vast and easily accessible repositories of personal information were all but nonexistent. Their advent is driving a profound debate over the definition of privacy in an era when most people now carry information-transmitting devices with them all the time.

Capitalizing on

personal data is a lucrative enterprise. Facebook is in the midst of planning for an initial public offering of its stock in May that could value the young company at more than \$100 billion on the Nasdaq Stock Market.

Facebook requires apps to ask permission before accessing a user's personal details. However, a user's friends aren't notified if information about them is used by a friend's app. An examination of the apps' activities also suggests that Facebook occasionally isn't enforcing its own rules on data privacy.

---

## What they Know

A Wall Street Journal Investigation



reached for comment.

- Dozens of apps allow advertisers that haven't been approved by Facebook within their apps, which enables advertisers including Google to track users of the apps, according to data collected by PrivacyChoice, which offers privacy services. Google said app-makers control which technology they use to deliver online ads.

---

## Related Video



Nasdaq has scored Facebook's shares, according to people familiar with the matter, winning what has been seen as the most-coveted listing among a new guard of Web businesses. Steven Russolillo has details on The News Hub. Photo: Mike Segar/Reuters



Facebook is preparing its initial public offering for May, in what is shaping up to be the largest-ever U.S. Internet offering. Randall Smith has details on The News Hub. Photo: Agence France-Presse/Getty Images.

personal-data economy. The \$28 billion online advertising industry is fueled largely by data collected about users' Web behavior that allow advertisers to create customized ads.

The "app economy," which includes Facebook as well as smartphone apps, is estimated to have generated \$20 billion in revenue in 2011 by selling downloads, advertising, "virtual goods" and other products, according to estimates from Rubinson Partners, a market researcher.

By virtue of its size and user base of 800-million-plus people, Facebook is at the heart of the personal data economy. Popular apps can quickly go "viral" there and gain millions of users—but can also flame out just as quickly. This explains why some apps seek to cash in by gathering as much data as possible and hoping to find ways to make money from it.

Brendan Wallace, co-founder of a Facebook app called "Identified" that provides career networking, said his

Among the possible transgressions of Facebook policies that the Journal identified:

- The app that sought the widest array of personal information of the 100 examined, "MyPad for iPad," has a two-paragraph privacy policy that says it is "adding Privacy settings shortly." Privacy policies that describe how they collect, use and share data are required by Facebook. The app maker couldn't be

- Such apps as the popular quiz games "Between You and Me" and "Truths About You" sought dozens of personal details—including the sexual preferences of users and their friends—that don't appear to be used by the app in the questions it poses to users about their friends. The makers of the apps, whose quizzes ask questions like "Is your friend's butt cute?" couldn't be reached for comment. Facebook requires apps to collect only the information they need to operate.

On Thursday, after Journal inquiries, "Between You and Me" began asking users for much less personal data.

In a statement, a Facebook spokesman said: "We're focused on helping people make informed decisions about the apps they choose to use. App developers agree to our policies when they register. If we find an app has violated our policies—through our automated systems, internal policy teams, or user reports—we take action."

It is no surprise, of course, that Facebook can gain deep knowledge of people's lives. It is, after all, a social network where users voluntarily share their names, closest friendships, snapshots, sexual preferences ("interested in men," "interested in women"), schools attended and countless other details, including moment-to-moment thoughts in the form of "status updates."

This kind of information is the coin of the realm in the

company aims to build up a repository of data. He is unsure how he will use the information but said, "data is what anyone wants access to." "Identified," which isn't in the top 100 apps, obtains from each of its users birthday, city, education and work history, and also the same set of information from its users' friends.

The unconstrained collection of digital data is stirring feelings of distrust among some users. "Consumers are being pinned like insects to a pinboard, the way we're being studied," said Jill Levenson, a creative project manager at Boys & Girls Clubs of America in Atlanta. She recently deleted nearly 100 apps on Facebook and Twitter, she said, because she was uncomfortable with the way details about her life might be used.

Not only are apps obtaining data directly from people's Facebook accounts, some apps are also letting unapproved advertising companies track users, according to data collected from PrivacyChoice, a start-up that offers privacy services. This could be a violation of Facebook's advertising policies.

Facebook's policies restrict app makers from using any ad companies that haven't signed an agreement with Facebook—an agreement that prevents the advertiser from collecting personal information. However, the data from PrivacyChoice show that several dozen widely used apps are using unapproved companies, most notably Google, the biggest online ad company. That means app users can be tracked within their apps by Google and others. Google said advertisers using its DoubleClick ad services agree to terms that prohibit the collection of any personally identifiable information.

Apps are required to ask people's permission to access their Facebook data. But the way they ask plays on a fundamental human tendency—namely, that people who see frequent warnings come to disregard them. Science has a word for this: habituation. Habituation occurs when people become accustomed to simply pressing the "yes" button when faced with an alert or warning.

"If people see a warning a lot, but then nothing bad happens in the average case, it decreases the alarm level" and people won't pay attention even when they need to, said Adrienne Porter Felt, a Ph.D. student in computer science at the University of California, Berkeley, who has studied requests for personal data by apps on smartphones.

Studies also suggest that people have trouble understanding long lists of permissions, especially if the terms are technical. But there is a larger issue: Even if people understand the permissions they grant, they might not grasp the unexpected ways that their data may be used in the future.

A case in point came just this past week, in a scandal involving an iPhone app called "Girls Around Me." The app used publicly available information from Foursquare, a location-based social network, to enable men to locate nearby women on a map and view the personal data and photos from their Facebook profiles.

Foursquare is a service that allows users to "check in" from their smartphones at coffee shops, bars and other locations. It is designed as a service for people who want to alert their friends who might be in the neighborhood. "Girls Around Me" was making it easier, however, for strangers to potentially identify nearby women. The app triggered an uproar, and Foursquare revoked its access to users' locations. In an email to the Journal, the developer of "Girls Around Me" said that the app "gives the user nothing more than the Foursquare app can provide itself."

The flap suggests that the debate over making your data "public" or "private" on Facebook (or other online services) can miss the point. The real issue is how the data will be used.

Helen Nissenbaum, a New York University professor who studies privacy, said that "Girls Around Me" generated outrage because it violated social norms against stalking women. If social norms were fences, she said, "any ethical, law-abiding person won't step over the fence." In the absence of data-usage laws or norms, she said, some tech companies feel unconstrained about using information in new ways that can seem creepy.

Ms. Nissenbaum, author of the book "Privacy in Context," has called for the development of what she calls digital "fences" around data usage. She argues that rules for data use should be based on context. Information

shared in a certain context—such as between a doctor and patient—should not then be shared in a way that would violate the context of the original situation.

"These rules that we think of as privacy rules are not only for the sake of the individual," Ms. Nissenbaum argues. "For instance, keeping voting confidential protects the integrity of democracy."

The White House included "respect for context" in its blueprint for a Privacy Bill of Rights that would set some guidelines for the use of personal data. The guidelines call for people to be given more information about what data are collected about them and to have some control over how it is used. Currently, the U.S. doesn't have a law providing comprehensive privacy protections.

Meantime, the app economy is on a tear. Facebook apps are generally free, but they are also big business—particularly games that sell "virtual goods." The software company Zynga, maker of popular apps including "FarmVille" and "CityVille," had revenue of \$1.14 billion in 2011 (although it wasn't profitable). The company went public this past December, and its stock-market capitalization is currently more than \$8 billion.

Facebook is considered to have one of the most advanced privacy models for its apps because it lists nearly every type of data sought—and provides users with the ability to reject apps' requests for some types of data. Smartphone apps often lack privacy policies and don't offer as much information and control over their use of personal data.

Today it can be difficult to remember how revolutionary apps seemed a few years ago, when Facebook unveiled them at its first-ever developers conference on May 24, 2007. At the time, MySpace had twice as many monthly users as Facebook, and it owed some of its success to the fact that MySpace users could trick out their Web pages with graphics, music and slide shows.

The companies that helped to customize MySpace profiles were the predecessors to apps—known at the time as "widget" makers. There were slide-show widgets and colorful-wallpaper widgets and the ultimate widget, YouTube, which let people put videos on their MySpace pages. But MySpace (which was owned by The Wall Street Journal's parent company, News Corp., between 2005 and 2011) had a rocky relationship with the widget makers. It didn't provide them with technical help and also didn't let the makers display ads within their widgets.

In 2007, Facebook's young CEO, Mark Zuckerberg, welcomed widget makers by providing the kind of help that would ensure that their software could operate smoothly within Facebook. It also offered widget makers the opportunity to sell ads within Facebook and renamed widgets "applications," or "apps." Within two months, developers had built more than 2,000 Facebook apps. Venture capitalists began pouring money into app start-ups. In 2008, Apple opened its own app store to offer software for the iPhone and iPod Touch.

It soon became clear that some apps had a cost to privacy. In July 2009, the Office of the Privacy Commissioner of Canada investigated Facebook and discovered that it was sharing too much of users' personal data with app makers without informing users. "This is no trivial issue: There are close to a million developers out there, scattered across some 180 countries," said Elizabeth Denham, who was then Canada's assistant privacy commissioner.

At the time, Facebook informed app users only that they were required to let the third-party app developer "know who I am and access my information." It didn't specify what information was being shared.

The Canadian officials wanted Facebook to require consent for each category of data that an app sought. The officials also wanted Facebook to specifically require apps to obtain the consent of a user's friends before granting access to the friends' information. In addition, Canada called for Facebook to develop technology that would give developers access only to the user information required for an app to work properly.

Facebook agreed to make some changes, such as adding more disclosure, but didn't agree to seek permission from friends when their data were disclosed to an app. Ms. Denham wrote at the time that she relented on that

point because she "was persuaded by Facebook's argument that many applications are designed to be social and interactive."

Facebook profiles are now set by default to let apps obtain all data from a user's friends except sexual preference, religion and political views. That means, for instance, even if a user has set his or her birthday, location and "online status" messages to be private to friends, their friends can approve an app that will also obtain that information.

In 2010, Facebook rolled out its new disclosure notices in apps. Users who attempted to acquire an app were met with a pop-up screen listing the types of information the app was seeking.

Amy Vernon, a freelance writer and digital consultant in Elizabeth, N.J., said that she used to use more apps on Facebook, but the permissions screens have made her more cautious. "Very often I get an invitation from a friend for a game and I'll click it and see the permissions, and decide, I'm not really that curious about this app," she said. "I almost always hit decline."

But even after the permissions screens appeared, most Facebook users still didn't understand what was happening with their data, according to a study last year by researchers at UC Berkeley. More than half the people surveyed couldn't tell which types of data a sample app could collect. And about 40% didn't understand that when an app was allowed to get personal data, it could actually transfer that data out of Facebook and store it elsewhere.

Still, some app developers say they are seeking less personal data than they could. Rick Marini, chief executive of the professional-networking app "BranchOut," said that more than 20 million people have signed up for the app. What users may not realize is that professional information about all of their friends is also now a part of the app's database. That lets "BranchOut" tout that it has more than 400 million profiles.

Mr. Marini said that his company seeks minimal data about users and their friends. "If we start asking for information like pictures and videos, we're going to hurt our business long term because users won't trust us," he said.

—Jennifer Valentino-DeVries, Shayndi Raice and Courtney Schley contributed to this article.

**Write to** Julia Angwin at [julia.angwin@wsj.com](mailto:julia.angwin@wsj.com)

*A version of this article appeared April 7, 2012, on page C1 in some U.S. editions of The Wall Street Journal, with the headline: The SellingofYou.*

Copyright 2012 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](http://www.djreprints.com)