THE WALL STREET JOURNAL.

WHAT THEY KNOW

Your Apps Are Watching You

A WSJ Investigation finds that iPhone and Android apps are breaching the privacy of smartphone users

By Scott Thurm and Yukari Iwatani Kane
December 17, 2010

Few devices know more personal details about people than the smartphones in their pockets: phone numbers, current location, often the owner's real name—even a unique ID number that can never be changed or turned off.

These phones don't keep secrets. They are sharing this personal data widely and regularly, a Wall Street Journal investigation has found.

An examination of 101 popular smartphone "apps"—games and other software applications for iPhone and Android phones—showed that 56 transmitted the phone's unique device ID to other companies without users' awareness or consent. Forty-seven apps transmitted the phone's location in some way. Five sent age, gender and other personal details to outsiders.

The findings reveal the intrusive effort by online-tracking companies to gather personal data about people in order to flesh out detailed dossiers on them.

Among the apps tested, the iPhone apps transmitted more data than the apps on phones using Google Inc.'s Android operating system. Because of the test's size, it's not known if the pattern holds among the hundreds of thousands of apps available.

Apps sharing the most information included TextPlus 4, a popular iPhone app for text messaging. It sent the phone's unique ID number to eight ad companies and the phone's zip code, along with the user's age and gender, to two of them.

Both the Android and iPhone versions of Pandora, a popular music app, sent age, gender, location and phone identifiers to various ad networks. iPhone and Android versions of a game called Paper Toss—players try to throw paper wads into a trash can—each sent the phone's ID number to at least five ad companies. Grindr, an iPhone app for meeting gay men, sent gender, location and phone ID to three ad companies.

"In the world of mobile, there is no anonymity," says Michael Becker of the Mobile Marketing Association, an industry trade group. A cellphone is "always with us. It's always on."

iPhone maker Apple Inc. AAPL 1.01% ▲ says it reviews each app before offering it to users. Both Apple and Google say they protect users by requiring apps to obtain permission

MORE

- What Can You Do? Not Much
- What Settings to Look For
- How One App Sees Location Without Asking
- Unique Phone ID Numbers Explained
- The Journal's Cellphone Testing Methodology
- **Complete Coverage:** What They Know

before revealing certain kinds of information, such as location.

"We have created strong privacy protections for our customers, especially regarding location-based data," says Apple spokesman Tom Neumayr. "Privacy and trust are vitally important."

The Journal found that these rules can be skirted. One iPhone app, Pumpkin Maker (a pumpkin-carving game), transmits location to an ad network without asking permission. Apple declines to comment on whether the app violated its rules.

Smartphone users are all but powerless to limit the tracking. With few exceptions, app users can't "opt out" of phone tracking, as is possible, in limited form, on regular computers. On computers it is also possible to block or delete "cookies," which are tiny tracking files. These techniques generally don't work on cellphone apps.

The makers of TextPlus 4, Pandora and Grindr say the data they pass on to outside firms isn't linked to an individual's name. Personal details such as age and gender are volunteered by users, they say. The maker of Pumpkin Maker says he didn't know Apple required apps to seek user approval before transmitting location. The maker of Paper Toss didn't respond to requests for comment.

JOURNAL COMMUNITY

Many apps don't offer even a basic form of consumer protection: written privacy policies. Forty-five of the 101 apps didn't provide privacy policies on their websites or inside the apps at the time of testing. Neither Apple nor Google requires app privacy policies.

To expose the information being shared by smartphone apps, the Journal designed a system to intercept and record the data they transmit, then decoded the data stream. The research covered 50 iPhone apps and 50 on phones using Google's Android operating system. (Methodology available here.)

The Journal also tested its own iPhone app; it didn't send information to outsiders. The Journal doesn't have an Android phone app.

Among all apps tested, the most widely shared detail was the unique ID number assigned to every phone. It is effectively a "supercookie," says Vishal Gurbuxani, co-founder of Mobclix Inc., an exchange for mobile advertisers.

On iPhones, this number is the "UDID," or Unique Device Identifier. Android IDs go by other names. These IDs are set by phone makers, carriers or makers of the operating system, and typically can't be blocked or deleted.

"The great thing about mobile is you can't clear a UDID like you can a cookie," says Meghan O'Holleran of Traffic Marketplace, an Internet ad network that is expanding into mobile apps. "That's how we track everything."

Ms. O'Holleran says Traffic Marketplace, a unit of Epic Media Group, monitors smartphone users whenever it can. "We watch what apps you download, how frequently you use them, how much time you spend on them, how deep into the app you go," she says. She says the data is aggregated and not linked to an individual.

The main companies setting ground rules for app data-gathering have big stakes in the ad business. The two most popular platforms for new U.S. smartphones are Apple's iPhone and Google's Android. Google and Apple also run the two biggest services, by revenue, for putting ads on mobile phones.

MORE FROM THE SERIES

- A Web Pioneer Profiles Users by Name
- 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
- On the Web, Children Face Intensive Tracking
- 'Scrapers' Dig Deep for Data on Web
- Facebook in Privacy Breach
- Insurers Test Data Profiles to Identify Risky Clients
- Shunned Profiling Technology on the Verge of Comeback
- Race Is On to 'Fingerprint' Phones, PCs
- The Tracking Ecosystem
- Follow **@whattheyknow** on Twitter
- **Complete Coverage:** What They Know

Apple and Google ad networks let advertisers target groups of users. Both companies say they don't track individuals based on the way they use apps.

Apple limits what can be installed on an iPhone by requiring iPhone apps to be offered exclusively through its App Store. Apple reviews those apps for function, offensiveness and other criteria.

Apple says iPhone apps "cannot transmit data about a user without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used." Many apps tested by the Journal appeared to violate that rule, by sending a user's location to ad networks, without informing users. Apple declines to discuss how it interprets or enforces the policy.

Phones running Google's Android operating system are made by companies including Motorola Inc. and Samsung Electronics Co. Google doesn't review the apps, which can be downloaded from many vendors. Google says app makers "bear the responsibility for how they handle user information."

Google requires Android apps to notify users, before they download the app, of the data sources the app intends to access. Possible sources include the phone's camera, memory, contact list, and more than 100 others. If users don't like what a particular app wants to access, they can choose not to install the app, Google says.

"Our focus is making sure that users have control over what apps they install, and notice of what information the app accesses," a Google spokesman says.

Neither Apple nor Google requires apps to ask permission to access some forms of the device ID, or to send it to outsiders. When smartphone users let an app see their location, apps generally don't disclose if they will pass the location to ad companies.

Lack of standard practices means different companies treat the same information differently. For example, Apple says that, internally, it treats the iPhone's UDID as "personally identifiable information." That's because, Apple says, it can be combined with other personal details about people—such as names or email addresses—that Apple has via the App Store or its iTunes music services. By contrast, Google and most app makers don't consider device IDs to be identifying information.

ILLUSTRATION BY RAY BARTKUS FOR THE WALL STREET JOURNAL

A growing industry is assembling this data into profiles of cellphone users. Mobclix, the ad exchange, matches more than 25 ad networks with some 15,000 apps seeking advertisers. The Palo Alto, Calif., company collects phone IDs, encodes them (to obscure the number), and assigns them to interest categories based on what apps people download and how much time they spend using an app, among other factors.

By tracking a phone's location, Mobclix also makes a "best guess" of where a person lives, says Mr. Gurbuxani, the Mobclix executive. Mobclix then matches that location with spending and demographic data from Nielsen Co.

In roughly a quarter-second, Mobclix can place a user in one of 150 "segments" it offers to advertisers, from "green enthusiasts" to "soccer moms." For example, "die hard gamers" are 15-to-25-year-old males with more than 20 apps on their phones who use an app for more than 20 minutes at a time.

Mobclix says its system is powerful, but that its categories are broad enough to not identify individuals. "It's about how you track people better," Mr. Gurbuxani says.

Some app makers have made changes in response to the findings. At least four app makers posted privacy policies after being contacted by the Journal, including Rovio Mobile Ltd., the Finnish company behind the popular game Angry Birds (in which birds battle egg-snatching pigs). A spokesman says Rovio had been working on the policy, and the Journal inquiry made it a good time to unveil it.

Free and paid versions of Angry Birds were tested on an iPhone. The apps sent the phone's UDID and location to the Chillingo unit of Electronic Arts Inc., which markets the games. Chillingo says it doesn't use the information for advertising and doesn't share it with outsiders.

Apps have been around for years, but burst into prominence when Apple opened its App Store in July 2008. Today, the App Store boasts more than 300,000 programs.

Other phone makers, including BlackBerry maker Research in Motion Ltd. and Nokia Corp. , quickly built their own app stores. Google's Android Market, which opened later in 2008, has more than 100,000 apps. Market researcher Gartner Inc. estimates that world-wide app sales this year will total $6.7 billion.

Many developers offer apps for free, hoping to profit by selling ads inside the app. Noah Elkin of market researcher eMarketer says some people "are willing to tolerate advertising in apps to get something for free." Of the 101 apps tested, the paid apps generally sent less data to outsiders.

Ad sales on phones account for less than 5% of the $23 billion in annual Internet advertising. But spending on mobile ads is growing faster than the market overall.

Central to this growth: the ad networks whose business is connecting advertisers with apps. Many ad networks offer software "kits" that automatically insert ads into an app. The kits also track where users spend time inside the app.

Some developers feel pressure to release more data about people. Max Binshtok, creator of the DailyHoroscope Android app, says ad-network executives encouraged him to transmit users' locations.

Mr. Binshtok says he declined because of privacy concerns. But ads targeted by location bring in two to five times as much money as untargeted ads, Mr. Binshtok says. "We are losing a lot of revenue."

Other apps transmitted more data. The Android app for social-network site MySpace sent age and gender, along with a device ID, to Millennial Media , a big ad network.

In its software-kit instructions, Millennial Media lists 11 types of information about people that developers may transmit to "help Millennial provide more relevant ads." They include age, gender, income, ethnicity, sexual orientation and political views. In a re-test with a more complete profile, MySpace also sent a user's income, ethnicity and parental status.

A spokesman says MySpace discloses in its privacy policy that it will share details from user profiles to help advertisers provide "more relevant ads." My Space is a unit of News Corp . , which publishes the Journal. Millennial did not respond to requests for comment on its software kit.

App makers transmitting data say it is anonymous to the outside firms that receive it. "There is no real-life I.D. here," says Joel Simkhai, CEO of Nearby Buddy Finder LLC, the maker of the Grindr app for gay men. "Because we are not tying [the information] to a

name, I don't see an area of concern."

Scott Lahman, CEO of TextPlus 4 developer Gogii Inc., says his company "is dedicated to the privacy of our users. We do not share personally identifiable information or message content." A Pandora spokeswoman says, "We use listener data in accordance with our privacy policy," which discusses the app's data use, to deliver relevant advertising. When a user registers for the first time, the app asks for email address, gender, birth year and ZIP code.

Google was the biggest data recipient in the tests. Its AdMob, AdSense, Analytics and DoubleClick units collectively heard from 38 of the 101 apps. Google, whose ad units operate on both iPhones and Android phones, says it doesn't mix data received by these units.

Google's main mobile-ad network is AdMob, which it bought this year for $750 million. AdMob lets advertisers target phone users by location, type of device and "demographic data," including gender or age group.

A Google spokesman says AdMob targets ads based on what it knows about the types of people who use an app, phone location, and profile information a user has submitted to the app. "No profile of the user, their device, where they've been or what apps they've downloaded, is created or stored," he says.

Apple operates its iAd network only on the iPhone. Eighteen of the 51 iPhone apps sent information to Apple.

Apple targets ads to phone users based largely on what it knows about them through its App Store and iTunes music service. The targeting criteria can include the types of songs, videos and apps a person downloads, according to an Apple ad presentation reviewed by the Journal. The presentation named 103 targeting categories, including: karaoke, Christian/gospel music, anime, business news, health apps, games and horror movies.

People familiar with iAd say Apple doesn't track what users do inside apps and offers advertisers broad categories of people, not specific individuals.

Apple has signaled that it has ideas for targeting people more closely. In a patent application filed this past May, Apple outlined a system for placing and pricing ads based on a person's "web history or search history" and "the contents of a media library." For example, home-improvement advertisers might pay more to reach a person who downloaded do-it-yourself TV shows, the document says.

The patent application also lists another possible way to target people with ads: the contents of a friend's media library.

How would Apple learn who a cellphone user's friends are, and what kinds of media they prefer? The patent says Apple could tap "known connections on one or more social-networking websites" or "publicly available information or private databases describing purchasing decisions, brand preferences," and other data. In September, Apple introduced a social-networking service within iTunes, called Ping, that lets users share music preferences with friends. Apple declined to comment.

Tech companies file patents on blue-sky concepts all the time, and it isn't clear whether Apple will follow through on these ideas. If it did, it would be an evolution for Chief Executive Steve Jobs, who has spoken out against intrusive tracking. At a tech conference in June, he complained about apps "that want to take a lot of your personal data and suck it up."

—Tom McGinty and Jennifer Valentino-DeVries contributed to this report.

Write to Scott Thurm at scott.thurm@wsj.com and Yukari Iwatani Kane at yukari.iwatani@wsj.com