

## Digital Privacy By The Numbers

45%

Portion of American adults who own smartphones

23%

Share of teenagers who own smartphones

699,200

Apps added to Apple store between July 2008 and September 2012

25 billion

App downloads from Google Play Store since October 2008

47%

Share of popular paid apps that lack a basic privacy policy

2

States that prohibit businesses from giving false statements in online privacy policies

7

States considering bills on online privacy issues

80%

Portion of Internet users who don't read privacy policies

Sources: *Pew Internet and American Life Project, The Internet Society, NCSL and The Future of Privacy Forum, September 2012.*

# App-losion!

Smartphones and apps are proliferating and getting smarter and smarter. Do they know too much?



## BY PAM GREENBERG

**M**obile apps—software applications that can be downloaded to your smartphone or tablet—can tell you the weather, give you breaking news, help you keep fit and healthy, guide you to the nearest drug store, find the lowest priced product, or even serve as a flashlight, binoculars, magnifying glass or mirror.

They also can provide businesses and advertisers with information about your age, gender, location, web searches, and your phone number or contacts list, sometimes without you even knowing it.

Many are concerned that all this clandestine sharing of information might not be a good idea. In California, the attorney general is applying a 2003 state privacy law, originally aimed at websites and passed before most mobile apps even existed, to cover apps as well.

“The explosion in the use of mobile devices and the hundreds of thousands of apps for them present a new threat to consumer privacy,” says former California Senator Joe Simitian (D), sponsor of the original law. “These apps must be subject to the law in the same way websites are.”

### 400+ Apps a Day

Growth in the mobile apps industry has been explosive. When the Apple App Store opened in July 2008, it offered 800 varieties to download. Today, the “store” has more than 700,000 apps, and they have been downloaded more than 35 billion times. Likewise, the Android Market launched with some 50 apps in October 2008. Known as the Google Play Store now, it offers 675,000 applications and hit 25 billion downloads in September 2012. Gartner, a technology research and advisory company, predicts that, by 2016, mobile app stores will reach 310 billion downloads and \$74 billion in revenue.

“The app economy is in its infancy, but is growing at an exponential rate,” according to CTIA—the

Wireless Association. Its October 2012 study, released with the Application Developers Alliance, found that the apps economy has created 519,000 jobs nationwide and is a significant economic driver for a number of states.

### Users in the Dark

The problem for some is that many of these apps collect personal information from unknowing users. The Juniper Networks security company found “a significant number of applications contain permissions and capabilities that could expose sensitive data” or gain access to functions on a device unrelated to the app. The study, which looked at 1.7 million Android apps in 2012, found that free apps were much more likely than purchased ones to access personal information such as the user’s location and address book. Some apps send age, gender and other details to advertisers. Apps also can access a device’s camera or even surreptitiously initiate phone calls or send messages.

Some mobile app developers also are coming under fire for collecting personal information on children. The Federal Trade Commission (FTC) recently brought a complaint against a company that developed an app of children’s games for illegally collecting and disclosing personal information from tens of thousands of children under age 13 without their parents’ consent.

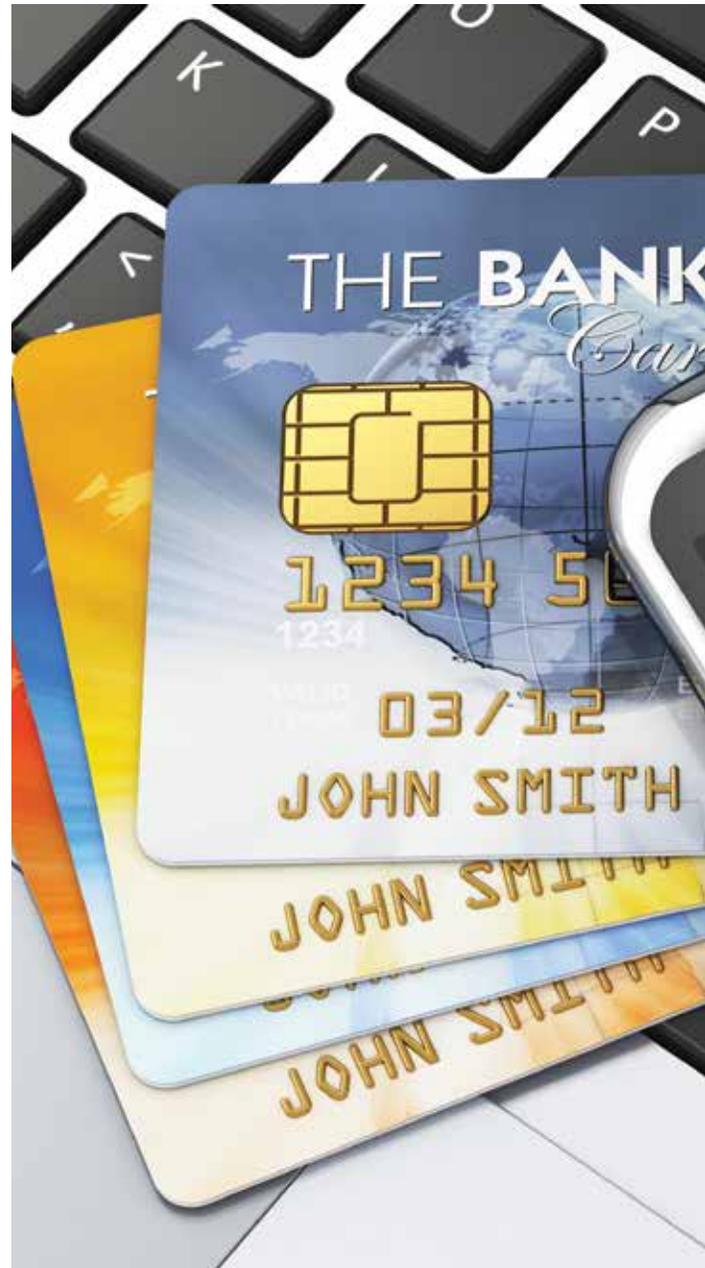
According to a recent study by the commission, most mobile apps “failed to provide any information about the data collected through the app, let alone the type of data collected, the purpose of the collection, and who would obtain access to the data.” The study also discovered that many of the apps shared information about children with third parties—such as device ID, geolocation or phone number—without disclosing that fact to parents. The FTC in December 2012 adopted new rules to address these concerns and released a report with recommendations for informing users about mobile data practices.

Industry associations have been working to establish voluntary privacy best practices and rating systems for mobile applications. CTIA—The Wireless Association, for example, developed a rating system that uses the age rating icons the Entertainment Software Rating Board assigns to computer and video games to provide parents and consumers with information about the age-appropriateness of applications.

The Association for Competitive Technology, which is also working to educate app developers about best privacy practices, released a statement that sheds some light on the nature of the industry. “The rapid growth of the mobile app industry has been fueled by start-ups and first-time developers, some of whom are still in high school. In fact, 87 percent of apps are developed by small or micro-businesses that do not have legal departments or privacy experts on staff. This report reminds us how important it is for the industry to focus attention on educating developers on privacy best practices.”

### Protecting Privacy

A large majority of smartphone owners say they want apps to be more transparent and to give them a say about personal information that is collected and shared, according to a 2011 Harris



Interactive poll.

California’s Online Privacy Protection Act, passed 10 years ago, requires commercial online services or websites that collect personal information from California residents to post a privacy policy on their websites. Although it’s difficult for law to keep pace with technology, the California act may have done so.

In early 2012, California Attorney General Kamala Harris negotiated an agreement with major online companies, such as Amazon, Apple, Facebook, Google and Microsoft, to address privacy concerns about apps. The companies agreed to a set of privacy principles, including requiring mobile apps that collect personal information to show a privacy policy before an app is downloaded.

In October 2012, Harris began notifying mobile app developers and companies that they were violating the law and that



they had 30 days to post a privacy policy “conspicuously” within their mobile app. They were to inform users of what personally identifiable information they were collecting and what they were doing with it. Harris also released a report with privacy practice recommendations for app developers, advertisers and others involved with mobile apps.

A coalition of advertising associations expressed concerns, however, with the attorney general’s recommendations. “Matters of mobile privacy are best addressed through codes of conduct developed through broad industry consensus that include mechanisms for responding to shifting technologies, practices and consumer preferences,” it said in a letter to Harris. “Industry has already been working diligently to address mobile data practices through various self-regulatory forums, including a broad and open multi-stakeholder process within the Department of Com-

## Best Practices

The Federal Trade Commission has released a set of best practices for businesses, including mobile companies, to protect consumers’ privacy. The commission calls on companies handling consumer data to adhere to these three core principles.

**Privacy by Design:** Companies should build in privacy at every stage in developing their products.

**Simplified Consumer Choice:** For practices not consistent with the context of a transaction or a consumer’s relationship with the business, companies should provide consumers with choices at a relevant time and context.

**Greater Transparency:** Companies should disclose details about their collection and use of consumers’ information.

merce, a process that has involved extensive public notice and comment periods.”

But former Senator Simitian says he supports Harris’ plan to bring the millions of users of mobile apps under the law’s protection. “My goal in 2003 was simple: Make sure folks doing business online knew what their privacy protections were and make sure those guarantees were honored,” he says.

### In Love With Apps

Not all information collected is a privacy concern of consumers, who love what apps enable them to do with their personal information. Even when privacy policies are available on websites, most people—80 percent—don’t even read them, according to a 2012 survey of more than 10,000 Internet users by the Internet Society.

Still, 54 percent of app users say they have decided not to install a cell phone app and 30 percent have uninstalled an app because they were concerned about it collecting personal information they didn’t wish to share, according to a telephone survey conducted in spring 2012 by the Pew Research Center’s Internet & American Life Project.

It’s not the first time that California, home to Silicon Valley, has spotlighted digital privacy issues. Although it is the only state that requires commercial websites to post a privacy policy, its influence extends to other states, since it applies to any website accessible by California residents. The state also was the first to enact a security data breach disclosure law and also has laws that protect the personal information of Californians who browse or read ebooks or use online library resources, and the privacy of personal social media accounts of employees and students.

Next time you go to download an interesting-looking app and it asks you to hit the INSTALL button, you might want to consider what kind of information you are willing to share. Check to see if it offers a privacy policy. If the policy is too tiny, long and impossible to read, that’s a whole other story. 