Improving Mobile Device Privacy Disclosures

Neal Walters
AARP Public Policy Institute

There is increasing concern about the amount of personal information that mobile device users may be revealing without their knowledge. Studies show that older consumers are one of the fastest-growing groups of mobile device users, and they express high levels of concern about the privacy of their information. For that reason, legislators, regulators, and consumer advocates are seeking to increase the transparency of mobile data collection and sharing.

“Always on and always on you” accurately describes how deeply many consumers have integrated mobile devices (such as cell phones, smartphones, and tablets) into their daily lives. Mobile devices allow consumers to connect to the Internet, to make audio and video phone calls, to take and send photographs and videos, and to use location-based services such as GPS mapping and navigation services.

Rapid Growth of Mobile Devices

Industry estimates suggest that by the end of 2013, the worldwide number of mobile-connected devices will be greater than the number of people on earth. In 2012, the amount of mobile data traffic was nearly 12 times the amount of global Internet traffic in 2000. As of this writing, 91 percent of adult Americans own a cell phone, 56 percent own a smartphone, and 34 percent own a tablet. Smartphone use continues to increase as more consumers upgrade to those devices. According to industry analysis of smartphone adoption rates, the rate of growth in smartphone use during 2012 was especially high among several demographic groups of consumers, including consumers ages 55–64, retired individuals, and large households. Experts expect those numbers to grow rapidly as consumers continue to integrate mobile devices into their daily lives.

Collection of Sensitive Personal Data by Mobile Devices

Mobile devices are specifically associated with an individual user and are frequently carried by the user wherever he or she goes. Consequently, it is possible to collect a great deal of information about the movements and behavior of device owners. Data gathered can include precise geographic location, thus allowing the creation of detailed profiles of the device owner’s movements and activities. For example, it may be possible to identify where individuals work, where they live, and what recreational activities they pursue. Such data are useful for
targeting behavioral advertisements or for perpetrating identity theft or stalking. As a result, the U.S. Government Accountability Office (GAO) notes that locational data are extremely sensitive. Moreover, GAO recommends that the Federal Trade Commission (FTC) develop detailed guidelines on how companies should manage mobile locational data.

Other sensitive information that can be potentially captured includes whom the owner is communicating with, the subject of Internet searches, access to photos and videos taken by the owner, and calendar activities scheduled. Such highly personal data may be available to third parties without the knowledge of the device owner. Without clear disclosure of what data are collected, who has access to those data, and how those data are used, device users have a difficult time making informed privacy decisions.

Of particular concern is the use of software applications (apps) designed to work on mobile devices. Apps allow consumers to make their mobile devices more useful by providing improved functionality. Apps can make use of any or all of the device’s functions, including contact lists, calendars, phone and messaging logs, locational information, Internet searches and usage, video and photo galleries, and more. Use of apps is a concern for consumers because an app may be accessing sensitive information without their knowledge. For example, an app that allows the device to function as a scientific calculator may be accessing contact lists, locational data, and phone records even though such access is unnecessary for the app to function properly.

Estimates place the current number of apps available for download at more than 1.5 million, and that number is growing daily. Projections indicate that the number of apps downloaded worldwide will exceed 81 billion in 2013. Because no standards currently exist for providing privacy notice disclosure for apps, consumers may find it difficult to understand what data the app is collecting, how those data will be used, and what rights users have in limiting the collection and use of their data. Many apps do not provide users with privacy policy statements, making it impossible for app users to know the privacy implications of using a particular app. Other apps may have privacy policies that are confusing or misleading. For example, an analysis of health and fitness apps found that more than 30 percent of the apps studied shared data with someone not disclosed in the app’s privacy policy.

Recent research indicates that mobile device users have concerns about the privacy implications of using apps. The research finds that almost 60 percent of respondents ages 50 and older decided not to install an app because of privacy concerns (see figure 1).

Current Barriers to Effective Mobile Privacy Disclosures

One barrier to mobile privacy disclosures is that many mobile devices have small screens that limit the effectiveness of long privacy statements that are meant to inform users about data collection and use. For example, one study found that the average length of app privacy policies was 3,068 words. Standardized terminology is also lacking, as is a format for privacy disclosures, both of which cause confusion for device users who are trying to understand the implications of using a particular website or app on their mobile device.

A second barrier can be the timing of the privacy disclosure. Currently, many websites and apps bury the details of
Improving Mobile Device Privacy Disclosures

Figure 1. Consumer Reactions to Privacy Implications of Using Apps, by Age


Note: Survey was conducted between March 15 and April 3, 2012 (n = 714).

their privacy policy in long, general privacy disclosures that mobile device users are unlikely to read or understand. The recently released FTC privacy framework recommends that consumers should be able to make privacy choices about their data at a relevant time and context.\textsuperscript{13} For example, before a particular app or service collects precise geographic location, the user should be notified that the information collection will occur if he or she proceeds. The FTC framework further notes that data use that is inconsistent with the original context of collection should require a separate disclosure to consumers at a relevant time and outside the general privacy policy.

A third barrier to mobile privacy disclosure is the complexity of the mobile ecosystem. The number of companies involved in the mobile ecosystem that have potential access to personal data of device users has expanded since the introduction of the first cell phones. Initially, only device manufacturers and cellular carriers had access to personal data. With the advent of smartphones and tablets, personal data are now available to device manufacturers, device operating system developers,\textsuperscript{14} wireless service providers, app developers, and advertising networks. The complex mobile ecosystem makes it difficult for consumers to understand who has access
to their data, what use is made of those data, and what rights they may have to limit such use.\textsuperscript{15}

\textbf{Greater Transparency through Improved Privacy Disclosure}

Improving mobile device privacy disclosures to provide greater transparency for device users is an important issue that privacy advocates and regulators are working to address. The FTC developed a specific set of recommendations for addressing mobile device privacy issues. Those recommendations serve to provide the major participants in the mobile ecosystem with a road map for improving mobile device privacy.\textsuperscript{16}

For privacy concerns associated with the use of mobile apps, the FTC notes that device operating systems have the greatest ability to improve app privacy disclosures. Because the device operating systems approve apps for distribution on devices running their software, they can establish privacy requirements that app developers must meet before accepting an app. Such requirements include the ability to ensure that app privacy disclosures (a) are clear and concise, (b) follow a standard format, and (c) provide just-in-time notifications before the app collects any sensitive data (such as geolocation). Just-in-time notification allows the user to block the app from gathering any sensitive information before its collection. Further, a device operating system–based do-not-track mechanism would give users a comprehensive way to prevent third-party advertising networks from tracking their activities.

Although the device operating system may be the gatekeeper, the FTC notes that app developers can also work to provide transparent and easy-to-understand privacy disclosures about their apps before a user downloads the app. If an app may collect particularly sensitive data (such as financial or health information), the app developers should require affirmative consent from app users before collecting those types of data. Privacy disclosures should also provide clear notice about data sharing with third parties while explaining what data are shared and how such data might be used. The FTC recommends that trade associations consider developing standardized icons (figure 2) to depict app privacy practices that will create more effective privacy disclosures.\textsuperscript{17}

\textbf{Current Efforts to Address Mobile Device Privacy Issues}

In addition to the FTC recommendations, legislators and state regulators are working to address mobile device privacy issues. For example, California requires mobile apps that collect personal information to have a privacy policy available on the app platform so consumers may view the privacy policy before downloading an app.\textsuperscript{18} In addition, California regulators recommend that app developers follow a “surprise minimization”\textsuperscript{19} approach to notify app users about data practices that involve sensitive information or that collect data unrelated to the app’s basic functionality.\textsuperscript{20} Such notifications need to be short, easy to understand, and delivered at a relevant time so app users can make informed decisions.

The National Telecommunications and Information Administration (NTIA) led efforts to create an industry-backed enforceable code of conduct for mobile app privacy disclosures to improve transparency. The NTIA process used a multistakeholder effort, including industry groups, consumer groups, and government regulators.\textsuperscript{21} However, consumer groups have criticized both the process of creating the code and the resulting code of conduct as being seriously flawed.\textsuperscript{22} In addition, Congress
Improving Mobile Device Privacy Disclosures

is considering bipartisan legislation to provide greater transparency and greater user control over mobile app privacy practices.23

Conclusions and Recommendations

Providing greater transparency for mobile device privacy is a key part of protecting the privacy of consumers who use mobile devices. Mobile device owners need greater clarity regarding the privacy implications of using their mobile devices. As more consumers continue to integrate mobile devices into their daily lives, mobile device users need to make informed decisions about limiting the types of personal data that are collected, about limiting how those data are used, and about how to exercise any rights they have to limit the collection. For that reason, regulators, legislators, and industry groups must continue to work toward improving transparency in the collection and use of personal information in the mobile device ecosystem.

The following approaches are recommended:

- Require privacy disclosure notices that are short, standardized, and easily accessible on smaller screens.
- Develop standards governing the collection, transfer, use, and disposal of sensitive data, such as locational data gathered through mobile devices.
- Notify app users about data practices that involve sensitive information

Figure 2. Potential Standardized Privacy Icons

Source: National Telecommunications and Information Administration, Short Form Notice Code of Conduct user interface mockups.
or that collect data unrelated to the app’s basic functionality before the collection of any such data.

- Create a do-not-track mechanism to give device users a comprehensive way to prevent the tracking of their activities by third-party advertising networks.
- Develop consumer education programs that teach mobile device users about their privacy options and how to implement them.

Endnotes

2 Ibid.
12 “More than a Quarter of the Top 100 Free Mobile Apps Don’t Have a Privacy Policy,” Spotlight on Mobile Privacy Policies (blog), MEF, August 20, 2013, http://mefminute.com/2013/08/20/infographic-more-than-a-quarter-of-the-top-100-free-mobile-apps-dont-have-a-privacy-policy/.
14 Device operating system developers design the software that runs the mobile device, for example, Apple, Google, Microsoft, and Blackberry.
16 Ibid.
17 Ibid.
Improving Mobile Device Privacy Disclosures


19 For example, a mobile device user could reasonably expect a social networking app to access the user’s contact list, but the user would likely be surprised to find that a solitaire game app does so as well.

20 “Privacy on the Go.”

21 Details regarding the NTIA code of conduct are available at http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency.


23 See, for example, the Application Privacy, Protection, and Security Act of 2013 (HR 1913). Also, the Mobile Device Privacy Act was released as a discussion draft in the 112th Congress.