



5 Privacy Tips for Mobile App Developers

by TRUSTe – April, 2011

Privacy concerns around mobile applications are higher than ever and consumer mistrust can limit app downloads and engagement levels. Here are five tips that can help you get privacy right and build a mobile audience through trust and respect for personal information:

1. Get Serious About Privacy

A TRUSTe consumer survey[†] found that 74 percent of consumers believe it's "very important" or "extremely important" to understand what personal information a mobile app collects. Moreover, 52 percent of consumers reported that they have read a privacy policy for a mobile app. Unfortunately, a separate TRUSTe analysis of the top free mobile apps found that only 19 percent have a privacy policy. App developers need to get serious about privacy. Creating a mobile privacy policy is a good start, but app developers need to look closely at their app data practices and identify areas where they can improve consumer privacy experiences.

Having a mobile privacy policy can help ensure that consumer privacy expectations meet the reality of your data practices. The length and density of a standard online privacy policy, however, will confuse and frustrate consumers on smaller mobile screens. A mobile privacy policy, just like a mobile app, should be mobile-optimized: think simple, visual and interactive. Consumers will thank you: in our survey 90 percent of consumers preferred TRUSTe's mobile-optimized privacy policy format to standard online privacy policies.

2. Always Ask *Before* Collecting Location Data

Mobile phones collect a great deal of personal information, location data being among the most sensitive type. There is a high degree of public discomfort with sharing location data – 40 percent of consumers report that they purposefully do not share location data with mobile applications.

An app's use of a consumer's location data should *always* be an opt-in process whereby a consumer grants explicit permission *prior* to the app's collection and use of this data. One method for obtaining consumer consent is creating a pop-up notice/request. Our survey found that app developers should do more in this regard as only 36 percent of consumers felt that they had a choice regarding the collection and use of their location data.

3. Offer Opt-Outs For Mobile Ad Targeting

Consumers are wary of mobile ad targeting. A solid majority of consumers – 74 percent – reported that they dislike being tracked for targeted mobile advertising. However, we also found a high degree of consumer awareness of the existence of mobile ad targeting (68 percent). Given the success of mobile apps these findings suggest that consumers warily accept the presence of mobile ad targeting in exchange for the convenience and entertainment value that apps offer. Consumer tolerance for mobile ad targeting

will presumably grow, but app developers can increase this tolerance by providing clear notice and choice for consumers when conducting mobile ad targeting.

You should provide a consistent, unified consumer opt-out experience: if you engage in targeted advertising on mobile devices *and* on the traditional web, then consumers should be able to opt-out of tracking on both devices from a single portal. Our survey found that 85 percent of consumers want to be able to opt-in or out of targeted mobile ads. Work with industry associations, like the Digital Advertising Alliance, to ensure that your targeted advertising privacy practices are consistent with industry standards.

4. Give Consumers Transparency & Choice

Consumers want choice regarding the use of their personal information. Our survey found that 98 percent of consumers believe it's important for mobile apps to provide easy access to controls for collecting and sharing personal information. Pop-up notices prompting users to grant/deny permission for data collection/use are an effective method for obtaining explicit consumer consent (opt-in). For data collection activities that are opt-out you can offer consumers choice by displaying opt-out mechanisms prominently within a mobile app's privacy and security settings.

Collect only the personal information that you need. It may be tempting to record every available data point about your app users, but the more you collect the more wary users become and the more responsibility and risk you assume with their personal data. If you collect information that a consumer might not necessarily expect, it's always a good idea to provide them with prominent notice of this collection.

5. Get Your App Privacy Certified

Only 1 in 3 consumers feel in control of their personal information when using their mobile devices, revealing a great deal of consumer mistrust in the mobile app space. Moreover, 52 percent of consumers list "privacy" and "unauthorized information sharing" as their primary concerns when using mobile apps. Getting your mobile app privacy certified by a reputable third-party like TRUSTe can help overcome consumer privacy concerns. In this way, privacy certification can be a competitive differentiator, helping to increase downloads and engagements by increasing consumer confidence and trust.

Unfortunately, not all mobile app marketplaces or stores enable the display of 3rd party privacy certifications. If they don't already, ask your app store or app marketplace to recognize 3rd party privacy certifications so that consumers can more easily identify trustworthy apps that protect their personal information.

If you are a mobile app or website developer and would like to learn about TRUSTe's mobile privacy certification, please visit www.truste.com/mobile or call 415-520-3490.

† TRUSTe Consumer Mobile Privacy Survey. April, 2011. Conducted by Harris Interactive.
<http://www.truste.com/harris-mobile-survey>