

Joint CDT, FPF Statement on the Development of App Privacy Guidelines

May 19, 2011

WASHINGTON, DC – Today, the Center for Democracy & Technology (CDT) and the Future of Privacy Forum (FPF) released the following statement in response to this morning’s Senate hearing on “Consumer Privacy and Protection in the Mobile Marketplace.” CDT and FPF are working together to improve mobile and app privacy and take the opportunity of the Senate hearing to make this statement on app privacy:

Today’s hearing demonstrated that the collection of personal information through Apps operating on mobile devices raises serious privacy issues. “Apps,” a shorthand for “applications” commonly used to refer to programs on mobile devices, are booming in popularity. Apps are also beginning to appear on Internet-linked televisions, on desktop computer operating systems and on the Web.

Apps often collect, use, share, and retain a variety of information, including location data. Sometimes this data is important to the app’s functionality. Sometimes, however, the data is not actually needed for app functionality and may be collected inadvertently. In other cases, the data is collected for targeted advertising, helping developers provide free and low-cost programs. However, any data collection practices can pose privacy issues, especially when the user is not aware of or has not consented to the collection. For users of mobile devices, a recent survey shows that privacy is their number one concern.

Accordingly, CDT and FPF are currently engaged with major stakeholders in the mobile ecosystem—app developers, device manufactures, and mobile platforms—to develop best practices and privacy principles for mobile devices. Once complete, we hope these principles will provide guidance to developers, platforms, and policymakers. For developers who are not familiar with the complex concerns surrounding user privacy, the CDT and FPF process will address the following fundamental issues:

1. **Privacy Policy.** Every app should have a written Privacy Policy explaining to users, in plain language, what data is collected, how it is used, how it will be displayed, shared, or transferred, and how long it will be retained. If data is collected, even incidentally, for the financial benefit of the app developer, e.g. for advertising, this should be disclosed. The Privacy Policy should be readily accessible. At a minimum, a link to the Privacy Policy should be provided prominently on the app itself and the contents of the Privacy Policy should be easy for the user to read and understand. Consideration should be given to layered privacy notices that summarize and link to the more detailed contents of a Privacy Policy. Other means of summarizing privacy practices, such as symbols or icons, should also be considered.
2. **Meaningful User Choice.** Users should be provided meaningful choices about the collection, disclosure, and use of the personal or device information. These choices should be explained in the Privacy Policy, but also presented “just-in-time” to users, when data is about to be collected.
3. **Data Minimization and Limited Retention.** Developers should only collect as much data as is necessary to perform the functions of the app and only retain this data for as long as it is needed, unless the user clearly has consented to greater collection and retention.
4. **Appropriate Data Security.** Developers should employ all reasonable physical, technical and administrative methods to protect the integrity and security of collected data.
5. **Education.** Developers should educate users about the types of data an app collects, and ways they can protect their privacy using the app. Developers should educate themselves about the laws they are subject to and take note of possible obligations under COPPA, as well as self regulatory initiatives such as those proposed by CTIA, MMA and the GSMA.
6. **Privacy by Design.** Developers should think about privacy from the beginning of the app

development process. Developers should consider what personal or device data is needed for app functionality and design the app to collect only what is needed, share it only with those needed to perform the functions of the app, and retain it only for as long as is necessary, and only after proper notice and choice for the user has been provided. This also means ensuring that needed physical, technical and administrative protections are in place for the data collected, and that accountability principles are employed to ensure that data is handled properly, including regular auditing and training of employees and contractors.

CDT and FPF are seeking input from platforms, carriers, device manufacturers, app developers and others on these issues and plan on expanding the forgoing concepts in order to provide the detail and specificity necessary for them to be effectively implemented. Given the incredible growth in the number of apps and the immediate need for a basic set of rules for developers, we urge all stakeholders to participate.

-
- [apps](#)
- [app_privacy](#)

Copyright © 2013 by Center for Democracy & Technology. CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. [Details](#).

Source URL:

https://www.cdt.org/pr_statement/joint-cdt-fpf-statement-development-app-privacy-guidelines