Best Practices for Mobile Applications Developers

July 12, 2012
Tags: Array

Supporting Documents

This is the final version of this report, released by the Center for Democracy & Technology and the Future of Privacy Forum.

"Mobile applications" — the software programs written to execute on one or more mobile device operating systems (such as Android, Blackberry OS, iOS,Symbian or Windows Phone OS) – can collect and transfer end users' personal information from their mobile devices. Such transfer of personal information raises privacy issues. And privacy in mobile applications can be a challenge. Mobile platforms may have terms of use related to privacy but it is not always clear what those terms mean.

Most developers are not experts in privacy law and policy and do not have the resources to hire lawyers or privacy consultants. The small screens of mobile devices limit the amount of information that can be easily communicated to users. Moreover, it may be difficult to understand how the third-party services incorporated into apps, such as analytics packages and those from advertising networks, use and access end users' information.

The guidelines presented in this 20-page report are intended to serve as a road map for you, the mobile app developer, to build privacy into your apps, better inform and empower end-users, and foster trust and confidence in the mobile app ecosystem.

-
- mobile apps privacy

Copyright © 2013 by Center for Democracy & Technology.
The content on this website that originates with 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/report/best-practices-mobile-applications-developers