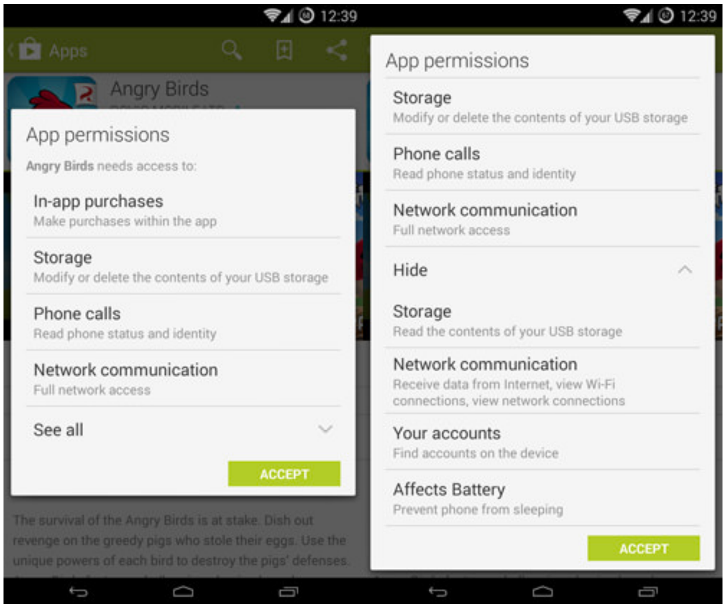
Mobile In-App Tracking and Advertising

Carnegie Mellon University **Data Privacy Day 2017**

How do I manage app permissions?

In recent versions of iOS and in Android Marshmallow (6.x), applications must ask the user for permission before using sensitive resources. These permissions can also be managed after the app has been installed. However, in Android Lollipop (5.x), all permissions are automatically granted once you install the app.


12:39
Apps
Angry Birds
The survival of the Angry Birds is at stake. Dish out revenge on the greedy pigs who stole their eggs. Use the unique powers of each bird to destroy the pigs' defenses.
12:39

App permissions

Angry Birds needs access to:

In-app purchases
Make purchases within the app

Storage
Modify or delete the contents of your USB storage

Phone calls
Read phone status and identity

Network communication
Full network access

See all

ACCEPT

App permissions

Storage
Modify or delete the contents of your USB storage

Phone calls
Read phone status and identity

Network communication
Full network access

Hide

Storage
Read the contents of your USB storage

Network communication
Receive data from Internet, view Wi-Fi connections, view network connections

Your accounts
Find accounts on the device

Affects Battery
Prevent phone from sleeping

ACCEPT

iOS (6+)	By app: Settings → App name By resource: Settings → Privacy
Android Marshmallow (6.x)	By app: Settings → Apps → App name → App permissions By resource: Settings → Apps → Tap the gear icon in the upper-right corner → App permissions
Android Lollipop (5.x)	To view app permission in the Google Play store, search for the app and look for the "Permissions" section in the app description To view permissions of apps installed on the device: Settings → Apps → Tap on app name

image: http://media02.hongkiat.com/android-app-permissions/app-permissions.jpg

How does in-app tracking work?

• • •

Similar to online tracking, mobile applications are able to record information about you, which is typically used to serve targeted ads. To learn more about you, mobile applications often use resources from your phone's operating system, such as your location, photos, and contacts list.

Android and iOS operating systems also have built-in advertising platforms used by apps to provide you with targeted ads. Each device is associated with an advertising ID, which is used to place you in a targeting group. These advertising IDs are associated with information such as your Apple or Google account profile (including your age and gender), downloads to your device, and activities in apps.

How can I control in-app tracking?

	How it works	How to do it
Reset advertising identifiers	This control works much like deleting cookies in a browser — the device is harder to associate with past activity, but tracking can start anew using the new advertising identifier.	**iOS**: Settings → Privacy → Advertising → Reset Advertising Identifier **Android:** Google settings → Ads → Reset advertising ID
Limit use of identifiers	If you turn on this setting, apps are not permitted to use the advertising identifier to serve consumers targeted ads. Although this tool will limit the use of tracking data for targeting ads, companies may still be able to monitor your app usage for other purposes, such as research, measurement, and fraud prevention.	**iOS:** Settings → Privacy → Advertising → Limit Ad Tracking **Android:** Google Settings → Ads → Enable "Opt Out of Interest-Based Ads"
Enable Do Not Track (DNT)	DNT is a setting in your browser that sends a signal to websites that you wish not to be tracked. However, many websites see this signal as an opt-out of targeted advertising and not necessarily tracking.	**Chrome (only Android):** In the Chrome browser, tap the menu icon (three dots to the right of the address bar) → Settings → Privacy → "Do Not Track" → Toggle "Off" to "On" **Safari (iOS):** Settings → Safari → Enable "Do Not Track"
Clear browser cookies	Clearing your browser cookies will remove any cookies, including advertising and tracking cookies, that had been previously set on your browser. Without these cookies, third-parties will not be able to link you to your previous online activity. Note that these cookies will be set again when you browse.	**Chrome (Android & iOS):** In the Chrome browser, tap the menu icon (three dots to the right of the address bar) → Settings → Privacy → Clear browsing data → Change "Clear data from the" to "beginning of time" (if necessary)→ Make sure "Cookies and site data" is checked → Tap "Clear Data" **Safari (iOS):** Settings → Safari → Clear History and Website Data
Install a content blocker (iOS only)	Similar to tracker blocking browser extensions, content blockers are apps which can be used to block different tracking technologies on Safari, including ad, analytics, and social trackers.	**iOS:** Install and configure a content blocking app to your preferences. Popular apps include: • Firefox Focus • Purify • 1Blocker • Sanitize • Adguard