App Data Elements

This document is intended to inform this discussion rather than be the end of it. The starting point for a broad examination of data elements requires a clear understanding of the details of how an app developer interacts with app stores and app store customers. This document lays out those interactions and details how data can be exchanged at each stage (including what kind of permissions are necessary). It assumes that the app is legitimate, follows app store requirements, and does not exploit security holes or hacking techniques to obtain information. It has been reviewed by developers for all the platforms and broadly reflects the processes of each store and OS.

When Submitting the App

Public Information:

- App name
- Description
- What's new in this version
- Keywords (for searching)
- Support URL
- Marketing URL (optional)
- Privacy Policy URL (optional)
- Screen shots: up to 3 for each type of device (phone, tablet, …)
- EULA: text and countries for which it applies. If not provided, default EULA applies.

Private Information (not listed in store)

- Developer Contact name, email, phone
- Review notes
- Demo account information

At Point of Purchase

The developer does not receive any personal information at the point of purchase. The only information that is shared is that a copy of the app was downloaded or sold at a certain price.

On App First Use

When the app is first run the complete application programming interface (API) is becomes available. Available information can be categorized based on the level of user interaction.

Technically no user permission required

- Physical characteristics of the device (model, screen size, memory, etc.)
- Network information (MAC address, IP addresses, Wifi Network, Bluetooth

devices) and any information that may be derived from it. For example, the IP address may give an indication of approximate location.
- In-app purchases for the installed app.
- Detect if certain other apps are installed that enable sharing through custom URL schemas.
- Vendor specific identifier of the user
- Advertising only identifier of the user
- Sound recorded through the microphone
- Orientation of the device, including tilting
- All data and usage contributed by the user of the app.

Attempting access prompts the user for permission

On Android this is typically done when the app is installed. Apps running on iOS devices often ask for “just-in-time permission”, prompting the user at the moment the information is needed.

- Permission to send push notifications.
- The location of the device.
- Contacts listed in the phone’s address book.
- Photos
- Camera
- Password/key storage
- Posting on certain OS-integrated services, such as Facebook, Twitter, or Google+.
- Composing emails

Access requires the user to log in

- Access to services that require login, such as Facebook, Twitter, Google+, providing full access to the service API.
- Access to apps that use Game Center.
- Once the user has logged in, any data associated with the account that is made available by the service to the app.

Through continued use of the app

- Usage data gathered while the app is running, including user interactions (buttons tapped, data entered, photos selected, etc.).
- Some apps have the ability to run in the background.

When the app is removed from the device

The app does not get any notification that it has been removed from the device. This makes it difficult to implement data retention policies since there is no way of knowing if the user has any intention to use the app (and any associated data that may be stored in the cloud) in the future.