User Privacy on iOS and OS X

Session 715

David Stites
Apple Product Security and Privacy

Katie Skinner
Apple Product Security and Privacy

© 2014 Apple Inc. All rights reserved. Redistribution or public display not permitted without written permission from Apple.
Agenda

Privacy and Reputation
Identifiers
Privacy Changes and Features
Prompting with Purpose
Data Isolation
Privacy Best Practices
Privacy and Reputation
Identifiers
Identifier APIs

Application Identifier

\[[\text{NSUUID UUID}]\]

Vendor Identifier

\[[\text{UIDevice currentDevice}] \text{identifierForVendor}]\]

Advertising Identifier

\[[\text{UIDevice currentDevice}] \text{identifierForAdvertising}]\]
| Identifier APIs | Protecting Your User’s Privacy | WWDC 2013 |
## Identifier APIs

<table>
<thead>
<tr>
<th>Identifier ID</th>
<th>Scope</th>
<th>Lifetime</th>
<th>Backed Up</th>
<th>Restores Across Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application ID</td>
<td>App</td>
<td>Uninstall app</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Vendor ID</td>
<td>Developer</td>
<td>Uninstall developer’s apps</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Advertising ID</td>
<td>Device</td>
<td>“Reset Advertising ID”</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
Advertising Identifier

Be transparent about advertising practices

Do not cache the Advertising ID

• The ID can be changed via “Reset Advertising ID” button in Settings > Privacy > Advertising

Advertising Identifier will be different every time the API is called for TestFlight apps
Limit Ad Tracking

Limit Ad Tracking gives customers a choice in how advertising is served

[[ASIdentifierManager sharedManager] advertisingTrackingEnabled]

Required to check the value of this property before using Advertising Identifier
Can be controlled by restrictions
Advertising Identifier

Limit Ad Tracking

When the value of `advertisingTrackingEnabled` is `NO`, the advertising identifier is not permitted to be used to collect data for or serve targeted advertising.
Advertising Identifier

Limit Ad Tracking

When the value of `advertisingTrackingEnabled` is NO, the advertising identifier is only permitted to be used for the purposes enumerated in the iOS Program License Agreement:

- Frequency capping
- Attribution
- Conversion events
- Estimating the number of unique users
- Fraud detection for advertising
- Debugging for advertising
Advertising Identifier

In iTunes Connect, select how your app is using the Advertising Identifier

• Serve advertisements
• Attribute app installation with previously served advertisement
• Attribute an action taken to a previously served advertisement
iTunes Connect and Advertising Identifier

---

Export Compliance

Have you added or made changes to encryption features since your last submission of this app?

- Yes
- No

Content Rights

Does your app contain, display, or access third-party content?

- Yes
- No

Advertising Identifier

Does this app use the Advertising identifier (IDFA)?

- Yes
- No

This app uses the Advertising identifier to (select all that apply):

- Serve advertisements within the app
- Attribute this app installation to a previously served advertisement
- Attribute an action taken within this app to a previously served advertisement

If you think you have another acceptable use for the Advertising identifier, [contact us](mailto:contact@app.com).

Limit Ad Tracking setting in iOS

- Link Appstore, configure the app, and any third-party that interfaces with this app, uses the Advertising identifier check and allows a user's Limit Ad Tracking setting in iOS and if it's enabled by a user, this app does not use Advertising Identifier, and no information obtained through the use of the Advertising identifier, in any way other than for "Limited Advertising Purposes" as defined in the iOS Developer Program License Agreement.
iTunes Connect and Advertising Identifier

**Advertising Identifier**

Does this app use the Advertising Identifier (IDFA)?

The Advertising Identifier (IDFA) is a unique ID for each iOS device and is the only way to offer targeted ads. Users can choose to limit ad targeting on their iOS device.

If your app is using the Advertising Identifier, check your code—including any third-party code—before you submit it to make sure that your app uses the Advertising Identifier only for the purposes listed below and respects the Limit Ad Tracking setting. If you include third-party code in your app, you are responsible for the behavior of such code, so be sure to check with your third-party provider to confirm compliance with the usage limitations of the Advertising Identifier and the Limit Ad Tracking setting.

This app uses the Advertising Identifier to (select all that apply):

- [ ] Serve advertisements within the app
- [ ] Attribute this app installation to a previously served advertisement
- [ ] Attribute an action taken within this app to a previously served advertisement

If you think you have another acceptable use for the Advertising Identifier, contact us.

Limit Ad Tracking setting in iOS

☐ I, John Appleseed, confirm that this app, and any third party that interfaces with this app, uses the Advertising Identifier checks and honors a user’s Limit Ad Tracking setting in iOS and, when it is enabled by a user, this app does not use Advertising Identifier, and any information obtained through the use of the Advertising Identifier, in any way other than for “Limited Advertising Purposes” as defined in the iOS Developer Program License Agreement.
Privacy Changes and Features
Family Sharing

There will be an increased number of accounts belonging to children.
Consider implications for your app under relevant laws.

- Example—COPPA (Children’s Online Privacy Protection Act) in the United States.
Related Session

- Kids and Apps

Nob Hill
Thursday 3:15PM
MAC Address

In iOS 8, Wi-Fi scanning behavior has changed to use random, locally administrated MAC addresses

- Probe requests (management frame sub-type 0x4)
- Probe responses (management frame sub-type 0x5)

The MAC address used for Wi-Fi scans may not always be the device’s real (universal) address
Safari Third Party Cookie Policy

New setting to block all third party cookies, regardless of whether the user has visited a site previously

Example—foo.com iframe on apple.com won’t be able to read or write foo.com cookies
Safari Third Party Cookie Policy

Cookies and website data:
- Remove All Website Data... (300 websites stored cookies or other data)

Block cookies and website data:
- Always
- Not from current website
- Not from current or previously visited websites
- Never

Limit access to location services:
- Prompt for each website once each day
- Prompt for each website one time only
- Deny without prompting

Website tracking:
- Ask websites not to track me

Smart Search Field:
- Do not preload Top Hit in the background
- Prevent search engines from providing suggestions
Safari Third Party Cookie Policy

Block Cookies

- Always
- Not From Current Website
- Not From Previously Visited
- Never

Cookies and website data:
- Remove All Website Data...
- 300 websites stored cookies or other data

Block cookies and website data:
- Always
- Not from current website
- Not from current or previously visited websites
- Never

Limit access to location services:
- Prompt for each website once each day
- Prompt for each website one time only
- Deny without prompting

Website tracking:
- Ask websites not to track me

Smart Search Field:
- Do not preload Top Hit in the background
- Prevent search engines from providing suggestions
In iOS 8, the people picker has a new mode that doesn’t prompt the user for access to Contacts.

If your app already has access to Contacts, a reference to the selected contact is returned from the address book.

If your app does not have access, the selected contact is returned as a temporary copy.

Some of the iOS 7 people picker delegate methods may be deprecated in a future seed.

People Picker
iOS 7 Delegate Methods

- [ABPeoplePickerNavigationControllerDelegate]
  peoplePickerController:shouldContinueAfterSelectingPerson:
- [ABPeoplePickerNavigationControllerDelegate]
  peoplePickerController:shouldContinueAfterSelectingPerson:property:identifier:]
People Picker

iOS 8 Properties and Delegates

ABPeoplePickerNavigationController.predicateForEnablingPerson
ABPeoplePickerNavigationController.predicateForSelectionOfPerson
ABPeoplePickerNavigationController.predicateForSelectionOfProperty

-[ABPeoplePickerNavigationControllerDelegate
peoplePickerNavigationController:didSelectPerson:]
-[ABPeoplePickerNavigationControllerDelegate
peoplePickerNavigationController:didSelectPerson:property:identifier:]
Privacy Changes
Understand the impact
Prompting with Purpose
Prompting with Purpose

Design the experience

Five core principles for “prompting with purpose”

- Consent
- Transparency
- Context
- Clarity
- Minimization
Prompting with Purpose

Consent

Allow “Calendar” to Access Your Location While You Use the App?
Your location is used to estimate travel times to events and improve location searches.

Don’t Allow  Allow

“Numbers.app” would like to access your contacts.
This will let Numbers use the name from your contact card in comments. You can change this later in System Preferences > Security & Privacy.

Don’t Allow  OK
Prompting with Purpose

Consent

Allow “Calendar” to Access Your Location While You Use the App?
Your location is used to estimate travel times to events and improve location searches.

Don’t Allow  Allow

“Numbers.app” would like to access your contacts.
This will let Numbers use the name from your contact card in comments. You can change this later in System Preferences > Security & Privacy.

Don’t Allow  OK
Prompting with Purpose

Transparency

Allow “Calendar” to Access Your Location While You Use the App?
Your location is used to estimate travel times to events and improve location searches.

Don’t Allow  Allow

“Numbers.app” would like to access your contacts.
This will let Numbers use the name from your contact card in comments. You can change this later in System Preferences > Security & Privacy.

Don’t Allow  OK
Prompting with Purpose
Transparency

Allow “Calendar” to Access Your Location While You Use the App?
Your location is used to estimate travel times to events and improve location searches.

“Numbers.app” would like to access your contacts.
This will let Numbers use the name from your contact card in comments. You can change this later in System Preferences > Security & Privacy.
Prompting with Purpose

Context

Tie prompting to a user-initiated action
Prompting with Purpose

Context

Tie prompting to a user-initiated action
Prompting with Purpose

Context

Tie prompting to a user-initiated action
Prompting with Purpose

Clarity

Distill the purpose of your request down to its essence
Be concise but include sufficient detail
Prompting with Purpose

Minimization

Only ask for what your application needs.
Conveying Purpose

All consent dialogs support purpose strings
Highly encouraged
One purpose data class
• Location Services in iOS 8 supports two
Set in your app’s Info.plist
• Add localized versions in Localizable.strings
Look for “Privacy—” keys and provide a value
• e.g. “Privacy—Contacts Usage Description”
### Custom iOS Target Properties

<table>
<thead>
<tr>
<th>Key</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bundle identifier</td>
<td>String</td>
<td>com.apple.$$[PRODUCT_NAME;rfc1034;identifier]</td>
</tr>
<tr>
<td>Privacy - Camera Usage Description</td>
<td>String</td>
<td>The camera is used to record video for your music video.</td>
</tr>
<tr>
<td>Privacy - Microphone Usage Description</td>
<td>String</td>
<td>The microphone is used to record audio for your music video.</td>
</tr>
<tr>
<td>Privacy - Photo Library Usage Description</td>
<td>String</td>
<td>Save the music videos you create to your Photo Library.</td>
</tr>
<tr>
<td>Privacy - Bluetooth Peripheral...</td>
<td>String</td>
<td>External microphones can capture audio over Bluetooth.</td>
</tr>
<tr>
<td>InfoDictionary version</td>
<td>String</td>
<td>6.0</td>
</tr>
<tr>
<td>Main storyboard file base name</td>
<td>String</td>
<td>Main</td>
</tr>
<tr>
<td>Bundle version</td>
<td>String</td>
<td>1</td>
</tr>
<tr>
<td>Required device capabilities</td>
<td>Array</td>
<td>$(EXECUTABLE_NAME)</td>
</tr>
<tr>
<td>Executable file</td>
<td>String</td>
<td>$(EXECUTABLE_NAME)</td>
</tr>
<tr>
<td>Application requires iPhone environment</td>
<td>Boolean</td>
<td>YES</td>
</tr>
<tr>
<td>Bundle versions string, short</td>
<td>String</td>
<td>1.0</td>
</tr>
<tr>
<td>Bundle creator OS Type code</td>
<td>String</td>
<td>???</td>
</tr>
<tr>
<td>Bundle OS Type code</td>
<td>String</td>
<td>APPL</td>
</tr>
<tr>
<td>Localization native development region</td>
<td>String</td>
<td>en</td>
</tr>
<tr>
<td>Bundle name</td>
<td>String</td>
<td>$(PRODUCT_NAME)</td>
</tr>
</tbody>
</table>
Conveying Purpose

Xcode

<table>
<thead>
<tr>
<th>Key</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy - Camera Usage Description</td>
<td>String</td>
<td>The camera is used to record video your new music video.</td>
</tr>
<tr>
<td>Privacy - Microphone Usage Description</td>
<td>String</td>
<td>The mic is used to record audio for your new music video.</td>
</tr>
<tr>
<td>Privacy - Photo Library Usage Description</td>
<td>String</td>
<td>Save the music videos you create to your Photo Library.</td>
</tr>
<tr>
<td>Privacy - Bluetooth Peripheral Access</td>
<td>String</td>
<td>External microphones can capture audio over Bluetooth.</td>
</tr>
<tr>
<td>InfoDictionary version</td>
<td>String</td>
<td>6.0</td>
</tr>
<tr>
<td>Main storyboard file base name</td>
<td>String</td>
<td>Main</td>
</tr>
<tr>
<td>Bundle version</td>
<td>String</td>
<td>1</td>
</tr>
<tr>
<td>Required device capabilities</td>
<td>Array</td>
<td>$(EXECUTABLE_NAME)</td>
</tr>
<tr>
<td>Executable file</td>
<td>String</td>
<td>$(EXECUTABLE_NAME)</td>
</tr>
<tr>
<td>Application requires iPhone environment</td>
<td>Boolean</td>
<td>YES</td>
</tr>
<tr>
<td>Bundle versions string, short</td>
<td>String</td>
<td>1.0</td>
</tr>
<tr>
<td>Bundle creator OS Type code</td>
<td>String</td>
<td>???:</td>
</tr>
<tr>
<td>Bundle OS Type code</td>
<td>String</td>
<td>APPL</td>
</tr>
<tr>
<td>Localization native development region</td>
<td>String</td>
<td>en</td>
</tr>
<tr>
<td>Bundle name</td>
<td>String</td>
<td>$(PRODUCT_NAME)</td>
</tr>
</tbody>
</table>
# New Purpose String Keys

<table>
<thead>
<tr>
<th>Data Class</th>
<th>Info.plist Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location (iOS)</td>
<td>NSLocationAlwaysUsageDescription</td>
</tr>
<tr>
<td></td>
<td>NSLocationWhenInUseUsageDescription</td>
</tr>
<tr>
<td>Camera</td>
<td>NSCameraUsageDescription</td>
</tr>
<tr>
<td>Health Kit</td>
<td>NSHealthKitUsageDescription</td>
</tr>
<tr>
<td>Motion Activity (available in iOS 7)</td>
<td>NSMotionActivityUsageDescription</td>
</tr>
</tbody>
</table>

Search for the Information Property List Key Reference in the Apple Developer Library for a complete list.
Privacy Settings

Photos stored on your iPhone may contain other information, such as when and where the photo was taken.

Apps that have requested access to your photos will appear here.
Directing Users to Settings

Users may want to update their privacy settings.
New in iOS 8, your app can direct users directly to settings.
Users may want to update their privacy settings

New in iOS 8, your app can direct users directly to settings

```objective-c
[[UIApplication sharedApplication] openURL:[NSURL URLWithString:UIApplicationOpenSettingsURLString]];
```
Your App's Privacy Settings
Your App's Privacy Settings

- Photos: On
- Motion Activity: On
- Camera: On

Control the types of data that this application can access.
Data Isolation

OS mediates between application and data
Transparent to application
Existing APIs trigger user consent
• Application receives no data if denied
New and Updated Data Classes in iOS 8

<table>
<thead>
<tr>
<th>Category</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>Updated</td>
</tr>
<tr>
<td>Contacts</td>
<td>Updated</td>
</tr>
<tr>
<td>Calendars</td>
<td></td>
</tr>
<tr>
<td>Reminders</td>
<td></td>
</tr>
<tr>
<td>Photos</td>
<td></td>
</tr>
<tr>
<td>Bluetooth</td>
<td></td>
</tr>
<tr>
<td>Microphone</td>
<td></td>
</tr>
<tr>
<td>Camera (worldwide)</td>
<td>Updated</td>
</tr>
<tr>
<td>Motion Activity</td>
<td>Updated</td>
</tr>
<tr>
<td>Health Kit</td>
<td>New</td>
</tr>
<tr>
<td>Social (Facebook, Twitter, etc.)</td>
<td></td>
</tr>
</tbody>
</table>
## Current Support on OS X

<table>
<thead>
<tr>
<th>Data Class</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td></td>
</tr>
<tr>
<td>Contacts</td>
<td></td>
</tr>
<tr>
<td>Calendars</td>
<td></td>
</tr>
<tr>
<td>Reminders</td>
<td></td>
</tr>
<tr>
<td>Social (Facebook, Twitter, etc.)</td>
<td></td>
</tr>
</tbody>
</table>
New Support

Applies to existing applications
No resubmission, recompilation
Changes can improve user experience
Data Isolation on OS X
OS X

Permission request is handled by the OS

• e.g., Address Book framework
  
  `[ABAddressBook sharedAddressBook]`
  
  `[[ABPerson alloc] init]`
  
  ...

Call blocks while permission is requested from the user

• Wrap in a dispatch block

• Subsequent calls return immediately
Granted access—populated object
Denied access—nil return value
For explicit data access, the permission request is handled by the OS
  • Sync Services
  • Spotlight
  • AppleScript
OS X Sandbox

Sandboxed apps require entitlements
If permissions change, the system may SIGKILL your app
Build with only the entitlements your app needs
Related Session

A Practical Guide to the App Sandbox

WWDC 2012
OS X

App Sandbox in Xcode

PROJECT
- MyApp
- MyAppTests

TARGETS
- MyApp
- MyAppTests
- MyAppDesktop
- MyAppDesktopTests

Capabilities

Network:
- Incoming Connections (Server)
- Outgoing Connections (Client)

Hardware:
- Camera
- Microphone
- USB
- Printing

App Data:
- Contacts
- Location
- Calendar

File Access:
<table>
<thead>
<tr>
<th>Type</th>
<th>Permission &amp; Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Selected File</td>
<td>None</td>
</tr>
<tr>
<td>Downloads Folder</td>
<td>None</td>
</tr>
<tr>
<td>Pictures Folder</td>
<td>None</td>
</tr>
<tr>
<td>Music Folder</td>
<td>None</td>
</tr>
<tr>
<td>Movies Folder</td>
<td>None</td>
</tr>
</tbody>
</table>

Steps: Add the *App Sandbox* entitlement to your entitlements file
OS X

App Sandbox in Xcode

Steps: Add the "App Sandbox" entitlement to your entitlements file
Data Isolation on iOS
Participation in the App Sandbox is required
Initial access will asynchronously return
Data returned to block or via delegate call
Need to handle change notifications
# New APIs in iOS

<table>
<thead>
<tr>
<th>Data Type</th>
<th>System Authorization Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>-[@CLLocationManager requestAlwaysAuthorization]</td>
</tr>
<tr>
<td></td>
<td>-[@CLLocationManager requestWhenInUseAuthorization]</td>
</tr>
<tr>
<td>Photos</td>
<td>-[[PhotoKit alloc] init]</td>
</tr>
<tr>
<td>Camera</td>
<td>-[AVCaptureDeviceInput deviceInputWithDevice:error:]</td>
</tr>
<tr>
<td>Health Kit</td>
<td>-[HKHealthStore authorizationStatusForDataType:]</td>
</tr>
<tr>
<td></td>
<td>-[HKHealthStore requestAuthorizationToShareTypes:readTypes:completion:]</td>
</tr>
</tbody>
</table>
Location Services in iOS 8

Location Services supports two different modes of updating device location

• “When In Use”
• “Always”

Depending on which versions of iOS you target, you may need additional logic.

Allow “Reminders” to Access Your Location While You Use the App?
- Reminders that alert you when you arrive or leave need access to your location.
- Don’t Allow
- Allow

Allow “Weather” to Access Your Location Even When You Are Not Using the App?
- Your location is used to show local weather in the “Weather” app and in Notification Center.
- Don’t Allow
- Allow
Location Services in iOS 8

“When In Use” Authorization

- `[CLLocationManager requestWhenInUseAuthorization]`  
  `NSLocationWhenInUseUsageDescription`

Privacy-friendly mode

Cannot update location in background

No access to region monitoring, Significant Location Change or Visits API

Double height status bar
Location Services in iOS 8

“Always” Authorization

```swift
-[CLLocationManager requestAlwaysAuthorization]

NSLocationAlwaysUsageDescription

Increased privacy impact for the user

App can start accessing location data in background

App has access to region monitoring, SLC and Visits API

Default mode for applications linked to iOS 7 or prior

iOS will occasionally re-prompt user for access to location
```
Location Services in iOS 8
Location Services in iOS 8

NSLocationUsageDescription ➔ Deprecated
Location Services in iOS 8

NSLocationUsageDescription
NSLocationWhenInUseUsageDescription
NSLocationAlwaysUsageDescription
CLLocationManager *manager = [CLLocationManager sharedManager];
[manager startUpdatingLocation];
CLLocationManager *manager = [CLLocationManager sharedManager];
if ([manager respondsToSelector:@selector(requestWhenInUseAuthorization)]) {
    [manager startUpdatingLocation];
} else {
    [manager requestWhenInUseAuthorization];
}
CLLocationManager *manager = [CLLocationManager sharedManager];
if ([manager respondsToSelector:@selector(requestWhenInUseAuthorization)]) {
    [manager startUpdatingLocation];
} else {
    [manager requestAlwaysAuthorization];
}
## Location Services in iOS 8

<table>
<thead>
<tr>
<th>Feature</th>
<th>iOS 7</th>
<th>When In Use</th>
<th>Always</th>
</tr>
</thead>
<tbody>
<tr>
<td>Triggers user consent dialog</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>Access to region monitoring, SLC &amp; Visits API</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Can start accessing device location in the background</td>
<td>•</td>
<td></td>
<td></td>
</tr>
<tr>
<td>iOS presents double height status bar</td>
<td></td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>App receives authorization status callbacks</td>
<td>•</td>
<td>•</td>
<td>•</td>
</tr>
<tr>
<td>What’s New in Core Location</td>
<td>Marina</td>
<td>Tuesday 2:00PM</td>
<td></td>
</tr>
</tbody>
</table>
Camera

AVCaptureSession *captureSession = [[AVCaptureSession alloc] init];
AVCaptureDevice *camera;
NSError *error;

AVCaptureDevice *captureDevice = [AVCaptureDevice defaultDeviceWithMediaType:AVMediaTypeVideo];
AVCaptureDeviceInput *captureInput = [AVCaptureDeviceInput deviceInputWithDevice:camera error:&error];

if (captureInput) {
    [captureSession addInput:captureInput];
    // handle success, video input stream should be live
} else {
    // handle failure
}
if ([HKHealthStore isHealthDataAvailable]) {
    HKHealthStore *hs = [[HKHealthStore alloc] init];
    HKObjectType *hrt = [HKObjectType
        quantityTypeForIdentifier:HKQuantityTypeIdentifierHeartRate];
    [healthStore requestAuthorizationToShareTypes:nil readTypes:[NSSet
        setWithObject:hrt] completion:^(BOOL success, NSError *error) {
        if (success) {
            // attempt to query the datastore
        } else {
            // handle the failure
        }
    }];
}
Health Kit
Writing data

HKAuthorizationStatus status = [hs authorizationStatusForDataType:hrt];
if (status == HKAuthorizationStatusNotDetermined) {
  // need to prompt here
} else if (authStatus == HKAuthorizationStatusSharingAuthorized) {
  // attempt to modify data store
} else {
  // handle failure
}
Health Kit

Writing data

```objective-c
[hs saveObject:hkObject withCompletion:^(BOOL success, NSError *error) {
    if (success) {
        // save the object
    }
}];

[hs deleteObject:hkObject withCompletion:^(BOOL success, NSError *error) {
    if (success) {
        // delete the object
    }
}];
```
Testing

Just run your app
Test on device
• The Simulator supports a subset of data classes
Apps can only trigger the prompt once
• Settings > General > Reset > Reset Location & Privacy on iOS
• tccutil(1) on OS X
Test All Cases
Test All Cases

- Permission being sought and denied
- Permission being sought and granted
- Permission previously denied
- Permission restricted
Failing Gracefully

iOS APIs help your app fail gracefully when your data access request is denied
Code should be resilient to lack of data returned
Send users to Settings
Restrictions can prevent users from changing privacy settings
  • Enterprise and on-device restrictions
Restrictions

<table>
<thead>
<tr>
<th>PRIVACY:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location Services</td>
</tr>
<tr>
<td>Contacts</td>
</tr>
<tr>
<td>Calendars</td>
</tr>
<tr>
<td>Reminders</td>
</tr>
<tr>
<td>Photos</td>
</tr>
<tr>
<td>Share My Location</td>
</tr>
<tr>
<td>Bluetooth Sharing</td>
</tr>
<tr>
<td>Microphone</td>
</tr>
<tr>
<td>Twitter</td>
</tr>
<tr>
<td>Facebook</td>
</tr>
<tr>
<td>Advertising</td>
</tr>
</tbody>
</table>
Restrictions

Allow Changes

Don’t Allow Changes
Disallowing changes locks the settings shown below and prevents new apps from using your photos.

Photos stored on your iPhone may contain other information, such as when and where the photo was taken.

- Notes
- Twitter
- Chase
- Facebook
- Lose It!
iOS Sample Code

Available on the iOS Developer Library today
“Checking and Requesting Access to Data Classes in Privacy Settings” project
Privacy Best Practices
Privacy Best Practices

Transparency
Data collection techniques
Avoid fingerprinting
Data protection
Transparency

Give the user opportunity to inspect data

- Crashes
- Data stores
- Logging
Transparency
Privacy policy

Important for all apps to have one, required for some app categories

• Apps that link against HealthKit
• Apps that link against HomeKit
• Third party keyboards
• Kids

Can submit a link to Apple in iTunes Connect
Link visible on the App Store
The iTunes Connect Mobile app allows developers and iBookstore providers to access their catalog and sales data anywhere on their iPhone, iPad, or iPod touch. iTunes Connect users can also view the metadata for all of their titles and set specific titles as Favorites for easier tracking.

Minor bug fix for push notifications.

Adds support for iPhone 5.
<table>
<thead>
<tr>
<th><strong>App Name</strong></th>
<th>iTunes Connect Mobile</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Description</strong></td>
<td>The iTunes Connect Mobile app allows developers and iBookstore providers to access their catalog and sales data anywhere on their iPhone, iPad, or iPod touch. iTunes Connect users can also view the metadata for all of their titles and set specific titles as Favorites for easier tracking.</td>
</tr>
<tr>
<td><strong>What's New in this Version</strong></td>
<td>Minor bug fix for push notifications. Adds support for iPhone 5.</td>
</tr>
<tr>
<td><strong>Keywords</strong></td>
<td>iTunes, Connect, Sales, Trends, Apps, Updates, Revenue, Developer, Tools</td>
</tr>
<tr>
<td><strong>Support URL</strong></td>
<td><a href="http://itunesconnect.apple.com">http://itunesconnect.apple.com</a></td>
</tr>
<tr>
<td><strong>Marketing URL (Optional)</strong></td>
<td><a href="http://itunesconnect.apple.com">http://itunesconnect.apple.com</a></td>
</tr>
</tbody>
</table>

A URL that links to your company's privacy policy. Privacy policies are recommended for all apps collecting user or device related data, and required for apps that offer auto-renewable or free subscriptions, or as otherwise required by law.
Privacy Policy

App Store
Data Collection
Data Collection

All data collection reduces privacy to some extent
• Does not imply all collection is bad/evil/wrong/misguided
Weigh the positives of your collection against the negative
True both for apps and servers
Holding on to rich data has risks
Data Collection Techniques

Anonymize
Aggregate
Sample
De-resolve
Decay
Minimize
Data Collection Techniques

Protecting Your User’s Privacy

WWDC 2013
Fingerprinting

A collection of data that forms a unique, persistent “fingerprint” for a specific user or device.

Does not need to be personal information.

Easy to do accidentally.
Initial user population
OS X Yosemite installed
PST timezone
Java installed
Cookies enabled
User-Agent Safari OS X Yosemite
Alice
Data Protection

Store important application credentials in the keychain
- Make a conscious decision whether the data will be synchronized among devices

Encrypt client-server communication using Transport Layer Security (TLS)

Use Data Protection for the data your application stores to disk

Local Authentication Framework
Summary

Test to understand the impact of the privacy related changes
Prompt users well by designing the experience and utilizing purpose strings
Consider new and updated data classes, such as Core Location and HealthKit
Submit a privacy policy link to the App Store
Maintain your reputation by thinking through privacy implications in your design
More Information

Paul Danbold
Core OS Technologies Evangelist
danbold@apple.com

Sample Code
Checking and Requesting Access to Data Classes in Privacy Settings

People Picker
More Information

Documentation
Best Practices for Maintaining User Privacy

Apple Developer Forums
http://devforums.apple.com
## Related Sessions

<table>
<thead>
<tr>
<th>Session</th>
<th>Location</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kids and Apps</td>
<td>Nob Hill</td>
<td>Thursday 3:15PM</td>
</tr>
<tr>
<td>What’s New in Core Location</td>
<td>Marina</td>
<td>Tuesday 2:00PM</td>
</tr>
<tr>
<td>Keychain and Authentication with Touch ID</td>
<td>Nob Hill</td>
<td>Wednesday 10:15AM</td>
</tr>
<tr>
<td>Protecting Your User’s Privacy</td>
<td></td>
<td>WWDC 2013</td>
</tr>
<tr>
<td>Protecting User’s Data</td>
<td></td>
<td>WWDC 2013</td>
</tr>
<tr>
<td>A Practical Guide to the App Sandbox</td>
<td></td>
<td>WWDC 2012</td>
</tr>
</tbody>
</table>
Labs

• Security and Privacy Lab
  Core OS Lab B
  Thursday 3:15PM