

# Protecting Your Users' Privacy

Session 714

**David Stites and Katie Skinner**

Apple Product Security

These are confidential sessions—please refrain from streaming, blogging, or taking pictures

# Agenda

- Reputation
- Identifiers
- Data isolation
- Privacy best practices

# Privacy and Reputation

# Identifiers

# UDID Replacement APIs

# Changes in iOS 6

**UDID**



	Scope
Application ID	App
Vendor ID	Developer
Advertising ID	Device

# UDID vs UUID

- UDID
  - Unique Device Identifier
  - Unique hardware identifier
- UUID
  - Universally Unique Identifier
  - Unique random identifier
- A single UDID, but many UUIDs

# UDID



- New apps or app updates that reference UDID no longer accepted
- As of iOS 7
  - API removed
  - Existing apps will receive the Vendor Identifier



# UDID



- UDID—46b74f03b8de6726e5f9c2889e84e32fe938e24c
- In iOS 7—FFFFFFFF<Vendor Identifier without dashes>

# UDID



- UDID—46b74f03b8de6726e5f9c2889e84e32fe938e24c
- In iOS 7—FFFFFFFF<Vendor Identifier without dashes>
- Vendor ID—                   BBBDD211-B69B-4FB4-9CB3-6D7A42FB5A6B
- In iOS 7—FFFFFFFFBBBDD211B69B4FB49CB36D7A42FB5A6B

# UDID



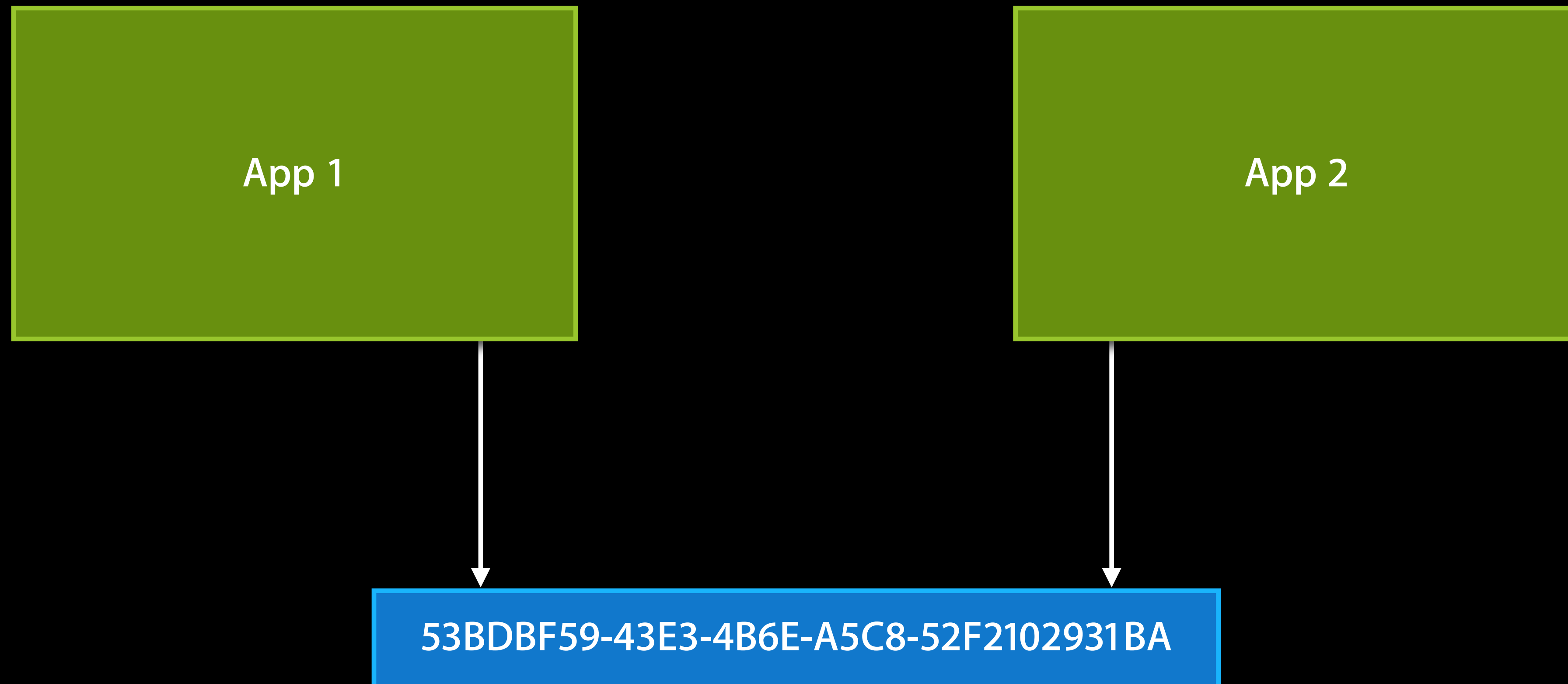
- Third-party libraries may contain the reference
- To locate the reference
  - Create an .ipa file that matches what you submitted to the App Store
  - Change the extension to .zip
  - Expand the .zip
  - Use the strings tool to search for **uniqueIdentifier**:
    - `$ strings - -a -arch armv7 "Payload/YourApp.app/YourApp" | grep uniqueIdentifier`

# Vendor Identifier

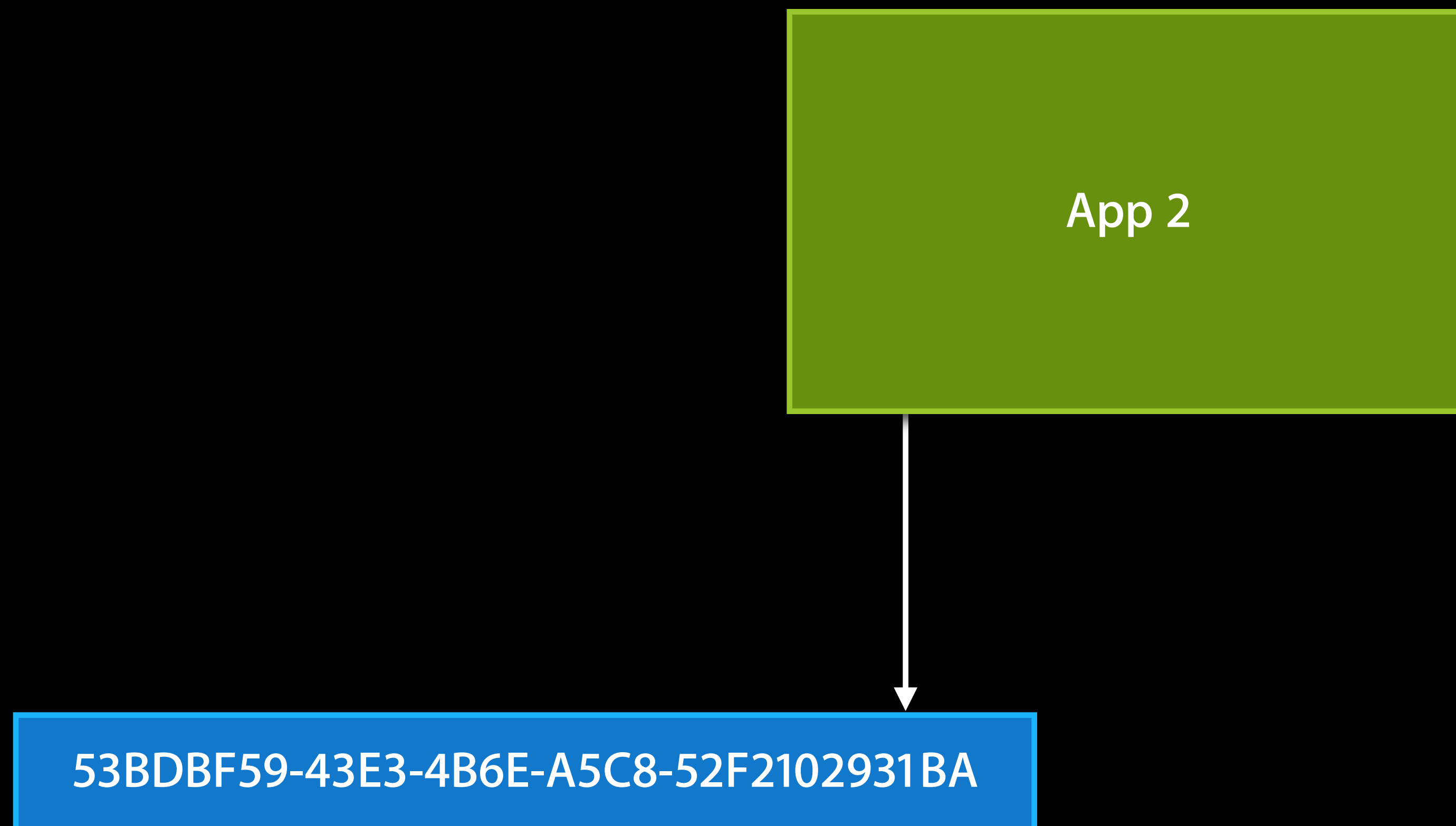
- Introduced in iOS 6
- `[[UIDevice currentDevice] identifierForVendor]`
  - UUID
- Provides a device-unique identifier per Team ID
- Mapping stored and managed by iOS
- Erased with removal of the last app for that Team ID
- Backed up
- Will not be restored across devices

# Vendor Identifier

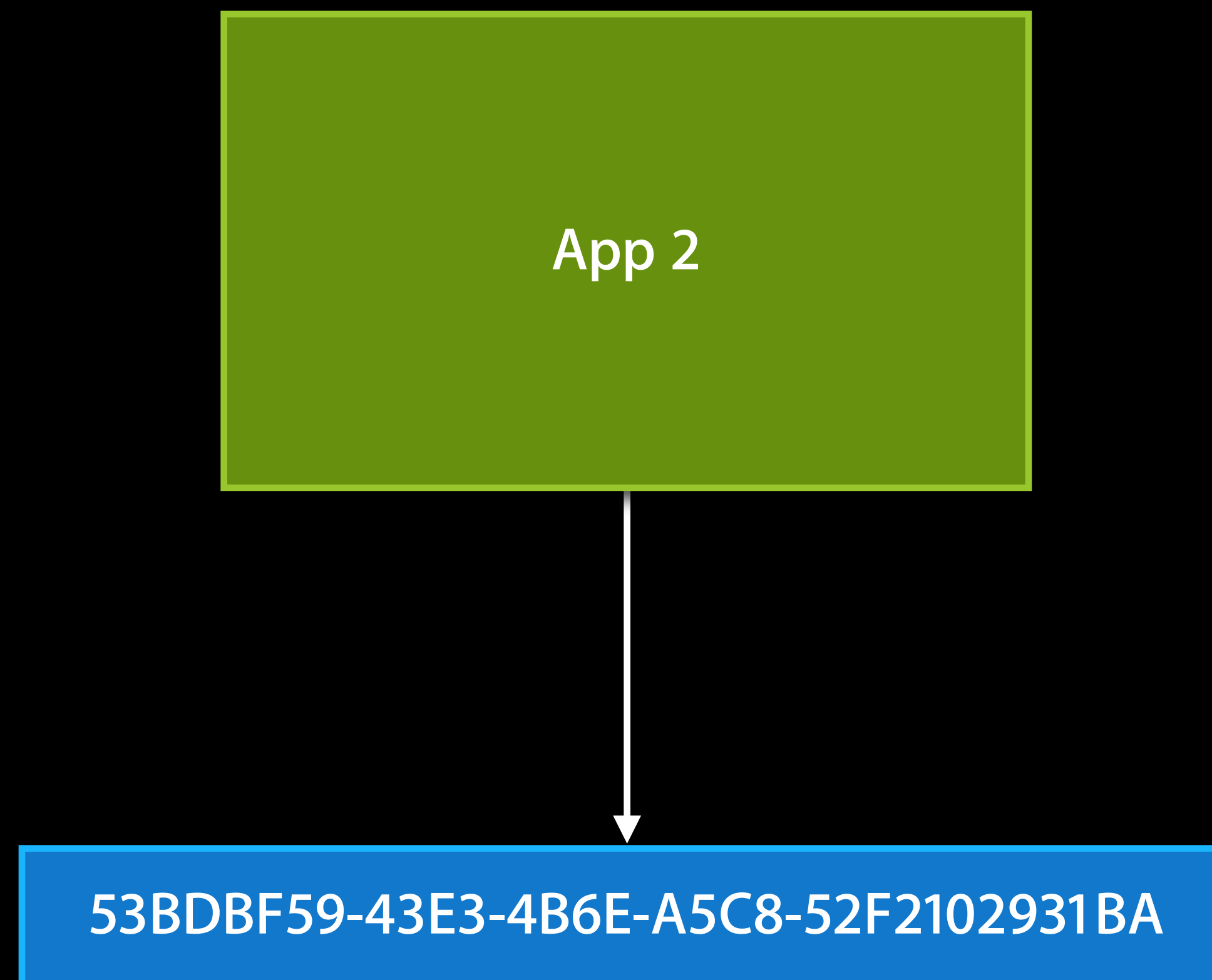
# Vendor Identifier



# Vendor Identifier



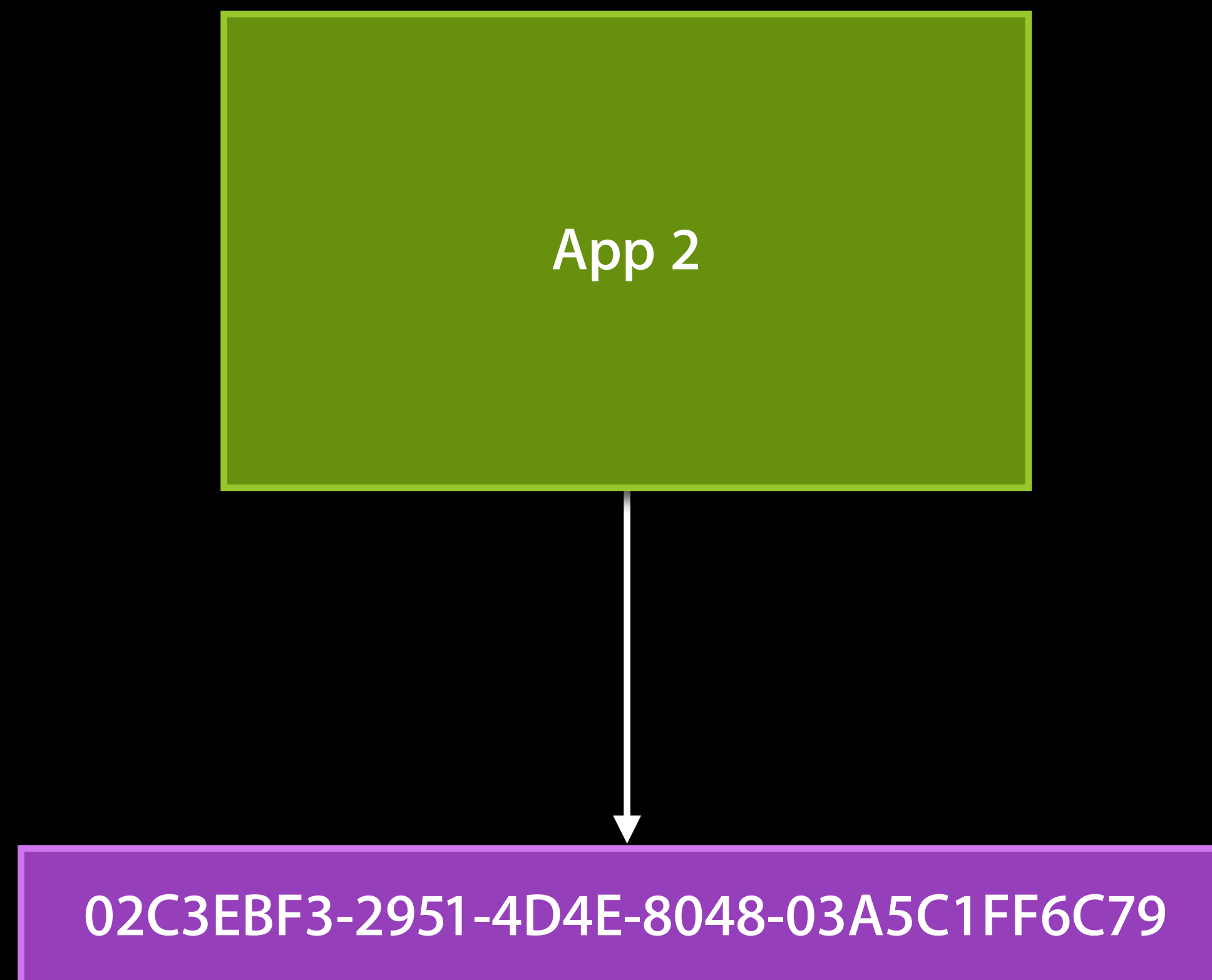
# Vendor Identifier



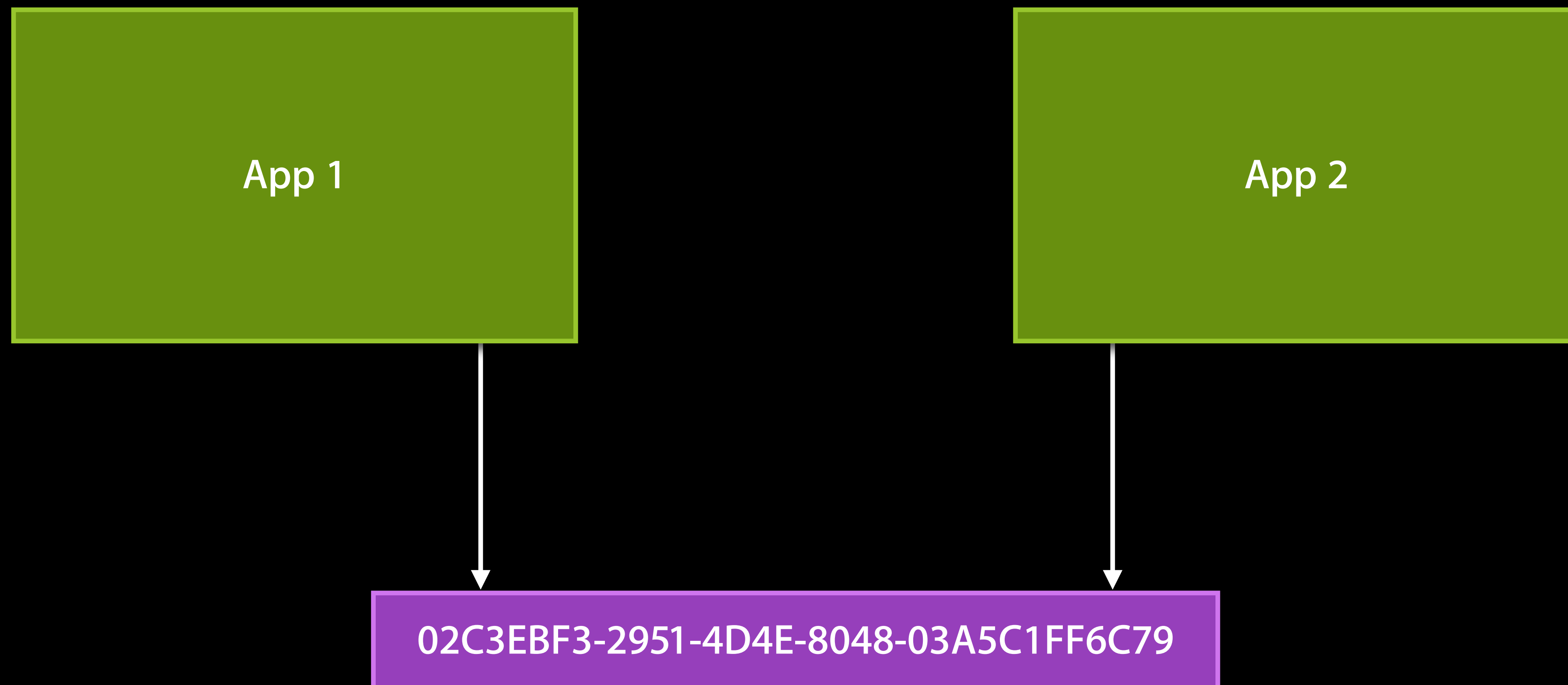


# Vendor Identifier

# Vendor Identifier



# Vendor Identifier



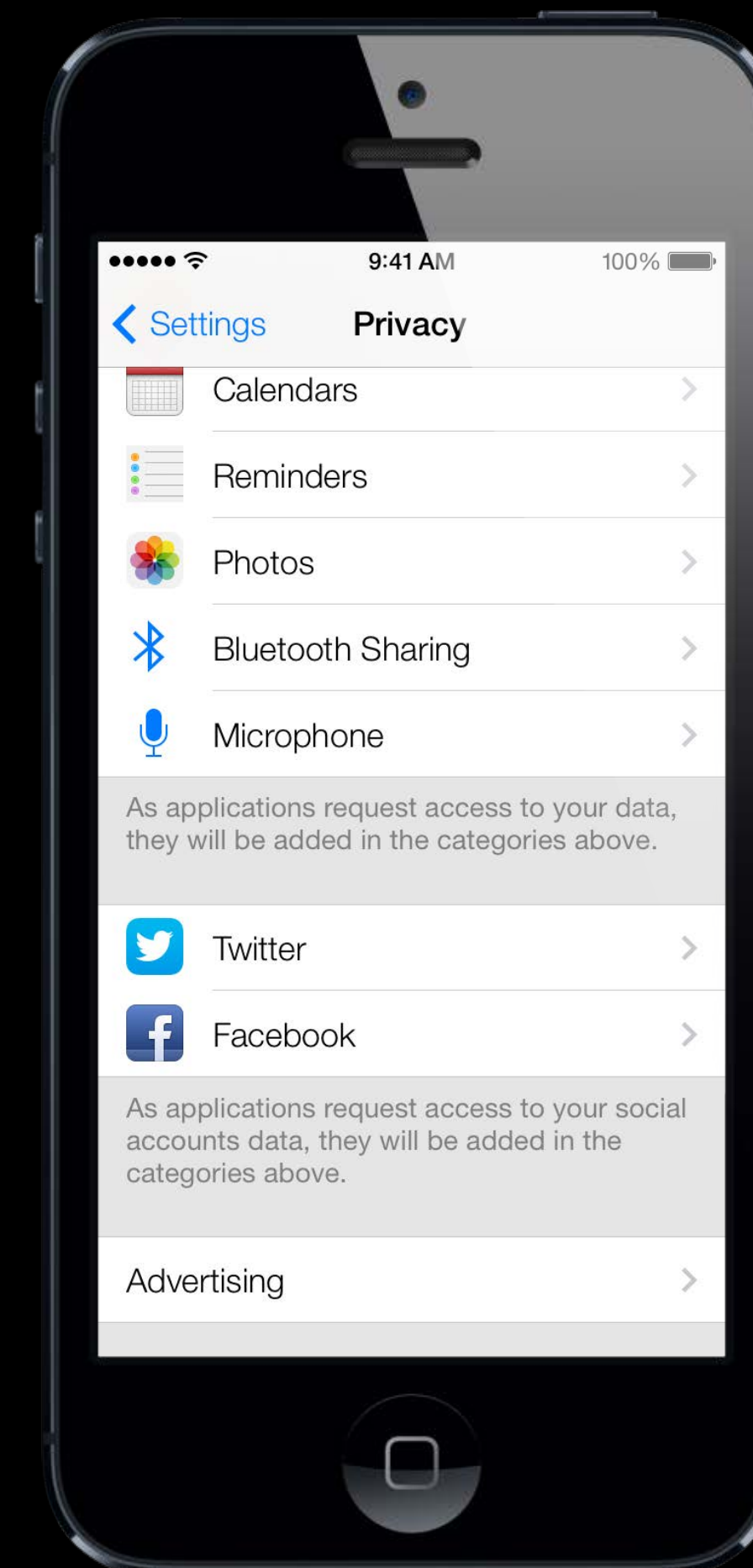
# Advertising Identifier

- Used for advertising
- Limit ad tracking
  - `[[ASIdentifierManager sharedManager] advertisingTrackingEnabled]`
  - Required to check the value of this property before use
    - If the value is NO, the identifier can only be used for the purposes enumerated in the Program License Agreement
- Backed up
- Will not be restored across devices

# Advertising Identifier



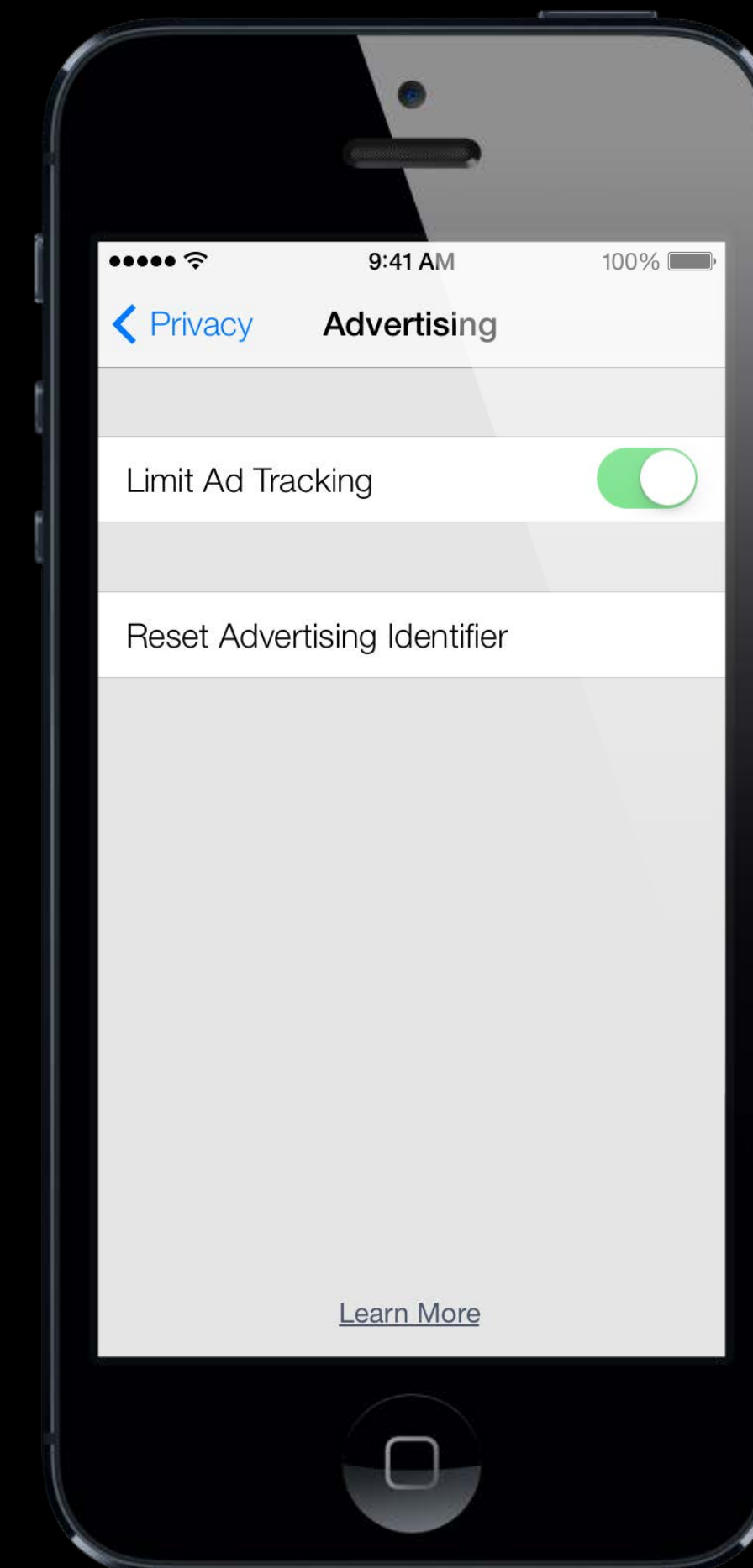
- Limit ad tracking under Settings > Privacy
- Can be controlled by restrictions
- Do not cache the Advertising ID
  - The ID can be changed via the reset button in Advertising



# Advertising Identifier



- Limit ad tracking under Settings > Privacy
- Can be controlled by restrictions
- Do not cache the Advertising ID
  - The ID can be changed via the reset button in Advertising



# UDID Replacement APIs



	Scope	Lifetime	Backed Up	Restores Across Devices
Application ID	App	Uninstall app	Yes	Yes
Vendor ID	Developer	Uninstall developer's apps	Yes	No
Advertising ID	Device	Erase all Content and Settings	Yes	No

# Other Identifiers



# MAC Address



- Access to the device's MAC addresses is restricted
- The API is not deprecated
  - `sysctl(NET_RT_IFLIST)`
  - `ioctl(SIOCGIFCONF)`
- A constant value is returned for all devices
  - `02:00:00:00:00:00`
- Applies to existing apps

# gethostuuid()



- API removed
- Existing apps will receive the vendor ID

# Push Token



- Push tokens are scoped to an application
- The push token was never guaranteed to be a stable value
- Do not cache the value of the push token
- Always use the value provided in `application:didRegisterForRemoteNotificationsWithDeviceToken:`

# Pasteboard



- Named pasteboards are scoped per Team ID
- No change to system-provided pasteboards

# Identifier Updates

Understand the impact, test on iOS 7

# Data Isolation

# Consent and Transparency



# Consent

**“Camera” Would Like to Use  
Your Current Location**

Photos and videos will be tagged with  
the location where they were taken.

Don't Allow

OK



# Transparency

**“Camera” Would Like to Use  
Your Current Location**

Photos and videos will be tagged with  
the location where they were taken.

Don't Allow

OK

# Transparency

“Camera” Would Like to Use  
Your Current Location

Photos and videos will be tagged with  
the location where they were taken.

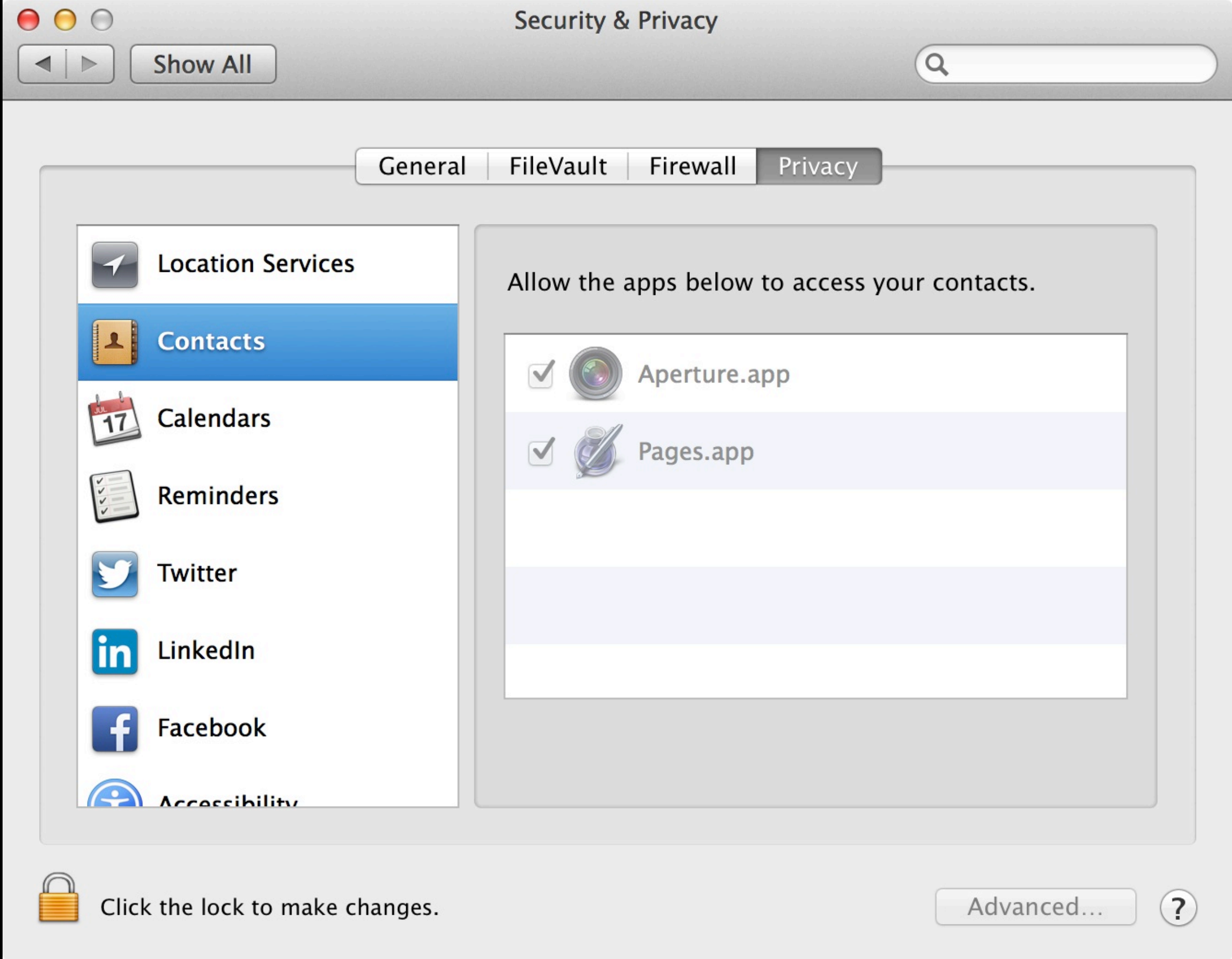
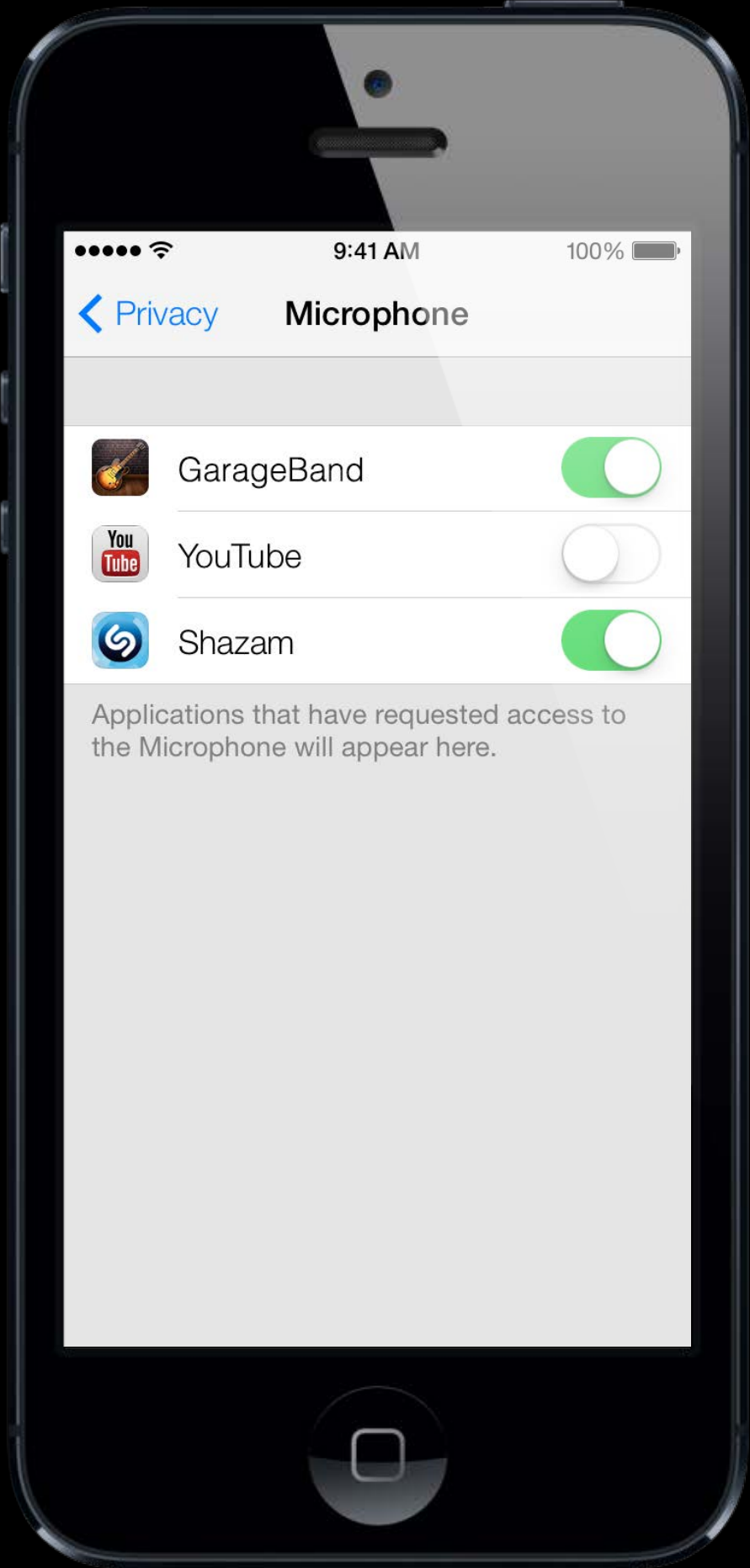
Don't Allow

OK

# Data Isolation

- OS mediates between application and data
- Transparent to application
- Existing APIs trigger user consent
  - Application receives no data if denied

# Managing Data Isolation



# Existing and New Support on OS X

Data Class	Mountain Lion	Mavericks
Contacts	●	●
Location	●	●
Calendars		●
Reminders		●

# Existing and New Support on OS X

Data Class	Mountain Lion	Mavericks
Facebook	●	●
Twitter	●	●
Sina Weibo	●	●
LinkedIn		●
Tencent Weibo		●

# Existing and New Support on iOS

Data Class	iOS 6	iOS 7
Contacts	●	●
Location	●	●
Calendars	●	●
Reminders	●	●
Photos	●	●
Bluetooth	●	●
Microphone		●
Camera (only some regions)		●

# Existing and New Support on iOS

Data Class	iOS 6	iOS 7
Facebook	●	●
Twitter	●	●
Sina Weibo	●	●
Tencent Weibo		●



# New Support

- Applies to existing applications
  - No resubmission, recompilation
- Changes can improve user experience

# Privacy Support in OS X

# OS X



- For purpose-specific API, user permission gathered by OS X
  - e.g., Address Book framework

```
[ABAddressBook sharedAddressBook]
[[ABPerson alloc] init]
...
```
- Aid to developers
- Call blocks while permission is requested from the user
  - Wrap in a dispatch block
  - Subsequent calls return immediately

# OS X



- Granted access—populated object
- Denied access—nil return value
- For explicit data access, user permission gathered by OS X
  - Sync Services
  - Spotlight
  - AppleScript

# OS X Sandbox



- Sandboxed apps have additional checks
- Access is disallowed without proper entitlement
- If permissions change, OS may kill your app
- Build with only the entitlements your app needs

# OS X



General Capabilities Info Build Settings Build Phases Build Rules

PROJECT  
SandboxApp

TARGETS  
SandboxApp  
SandboxAppTests  
Add Target...

App Sandbox ON

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

Hardware:  Camera  
 Microphone  
 USB  
 Printing

App Data:  Contacts  
 Location  
 Calendar

File Access:

Type	Permission & Access
User Selected File	None
Downloads Folder	None
Pictures Folder	None
Music Folder	None
Movies Folder	None

Steps: ✓ Add the "App Sandbox" entitlement to your entitlements file

# OS X



## Capabilities

SandboxApp

ON

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

- Hardware:  Camera
- Microphone
- USB
- Printing

App Data:  Contacts  
 Location  
 Calendar

File Access	Type	Permission & Access
User Selected File		None
Downloads Folder		None
Pictures Folder		None
Music Folder		None
Movies Folder		None

Steps:  Add the "App Sandbox" entitlement to your entitlements file

# Privacy Support in iOS



# iOS



- Participation is obligatory
- Initial access will synchronously return
- Access permission will come later
- Data returned in block or via delegate call
- Need to handle change notifications
  - A good idea anyway

# APIs in OS X and iOS

Data Type	System Authorization Support
Location	+[CLLocationManager authorizationStatus] -[CLLocationManager startUpdatingLocation]
Photos, videos, and other media	-[ALAssetLibrary enumerateGroupsWithTypes:usingBlock:failureBlock:] -[[UIImagePickerController alloc] init]
Contacts	ABAddressBookGetAuthorizationStatus() ABAddressBookRequestAccessWithCompletion(ABAddressBookRef, ABAddressBookRequestAccessCompletionHandler)

# APIs in OS X and iOS

## Data Type

## System Authorization Support

Reminders

```
- [EKEventStore  
requestAccessToEntityType:completion:]  
+ [EKEventStore authorizationStatusForEntityType]
```

Calendars

```
- [EKEventStore  
requestAccessToEntityType:completion:]  
+ [EKEventStore authorizationStatusForEntityType]
```

Bluetooth

```
- [CBCentralManager initWithDelegate:queue:]  
- [CBCentralManager scanForPeripheralsWithService:options:]
```

# APIs in OS X and iOS

## Data Type

## System Authorization Support

Social

```
-[ACAccountStore  
requestAccessToAccountsWithType:completion:]  
-[ACAccountType accessGranted]
```

Camera

```
-[AVCaptureDeviceInput deviceInputWithDevice:error:]
```

Microphone

```
-[AVAudioSession setCategory:error]  
-[AVAudioSession requestRecordPermission]
```

# Microphone



```
AVAudioSession *audioSession = [[AVAudioSession alloc] init];  
[audioSession setCategory:AVAudioSessionCategoryRecord  
error:&error];
```

# Microphone



```
AVAudioSession *audioSession = [[AVAudioSession alloc] init];  
[audioSession setCategory:AVAudioSessionCategoryPlayAndRecord  
error:&error];
```

# Microphone



```
dispatch_async(dispatch_get_global_queue(
DISPATCH_QUEUE_PRIORITY_BACKGROUND, 0), ^{
    BOOL granted = [audioSession requestRecordPermission];
    // do something with the audio session
    // or handle permission failures...
});
```

# Microphone Routing







Notes



Reminders



Stocks



Game Center



Newsstand



iTunes Store



App Store



Passbook



Compass



Settings



Phone



Mail



Safari



Music



↑  
Headphone



↑  
↑  
Microphone  
Headphone



↑ Lightning  
↑ Microphone  
↑ Headphone

# Tencent Weibo



# Tencent Weibo



```
ACAccountStore *accountStore = [[ACAccountStore alloc] init];
```

```
ACAccountType *tencentWeiboAccount = [self.accountStore  
accountTypeWithAccountTypeIdentifier:ACAccountTypeIdentifierTencentWeibo];
```

# Tencent Weibo



```
ACAccountStore *accountStore = [[ACAccountStore alloc] init];
```

```
ACAccountType *tencentWeiboAccount = [self.accountStore  
accountTypeWithIdentifier:ACAccountTypeIdentifierTencentWeibo];
```

```
[accountStore requestAccessToAccountsWithType:tencentWeiboAccount options:nil  
completion:^(BOOL granted, NSError *error) {  
    // do something with account access or  
    // handle failure...  
}];  
}
```

# Tencent Weibo



```
ACAccountType *socialAccount = [accountStore
accountTypeWithIdentifier: ACAccountTypeIdentifierTencentWeibo];

if([socialAccount accessGranted]) {
    // do something with the account
}
else {
    // handle denied access request
}
```



# Testing



- Just run your app
- Test on device
  - Data isolation will be supported in the Simulator in a future seed of iOS 7
- Apps can only trigger the prompt once
  - Settings > General > Reset > Reset Location & Privacy on iOS
  - tccutil on OS X
- Test all cases

# Test Cases



Permission being  
sought and denied

Permission being  
sought and granted

Permission  
previously denied

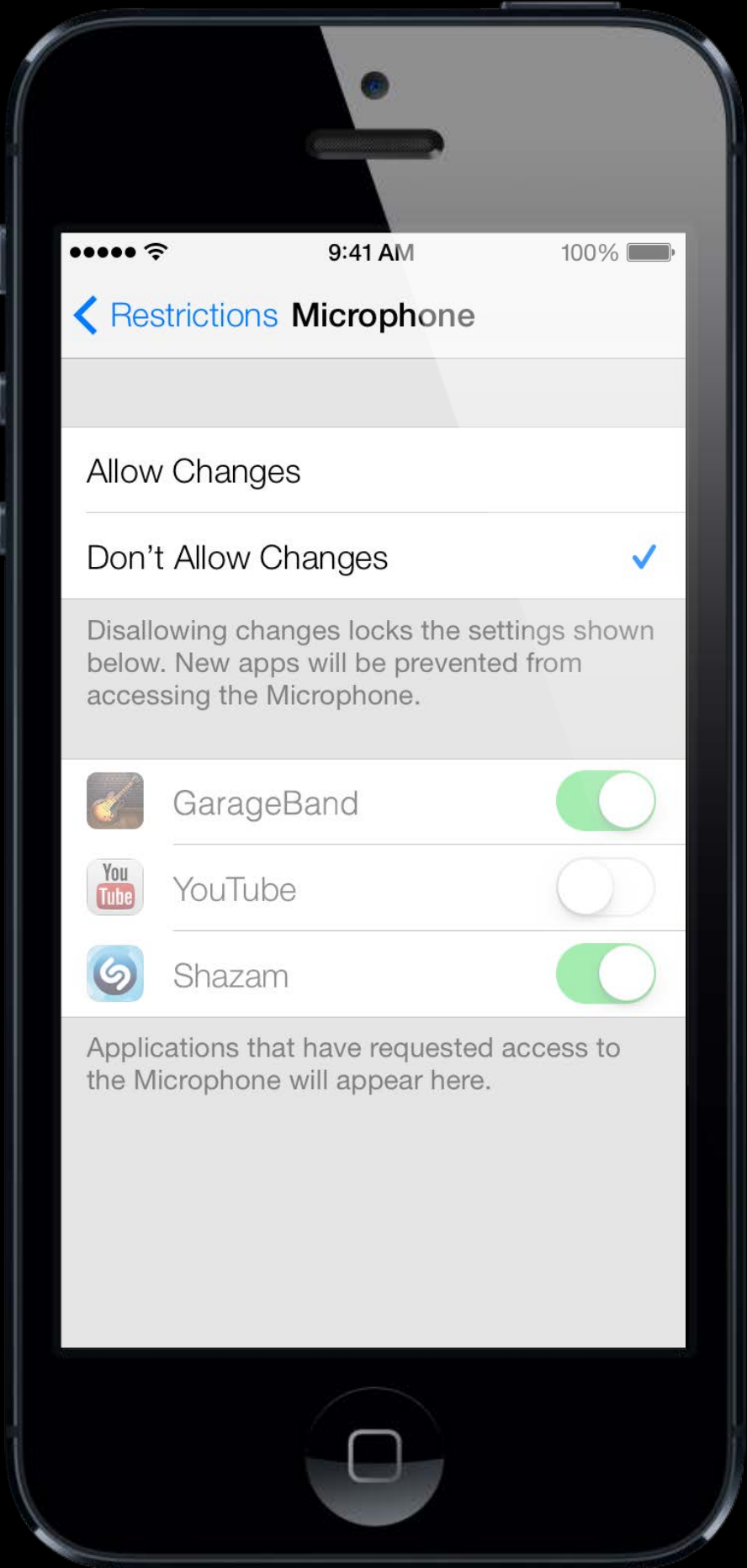
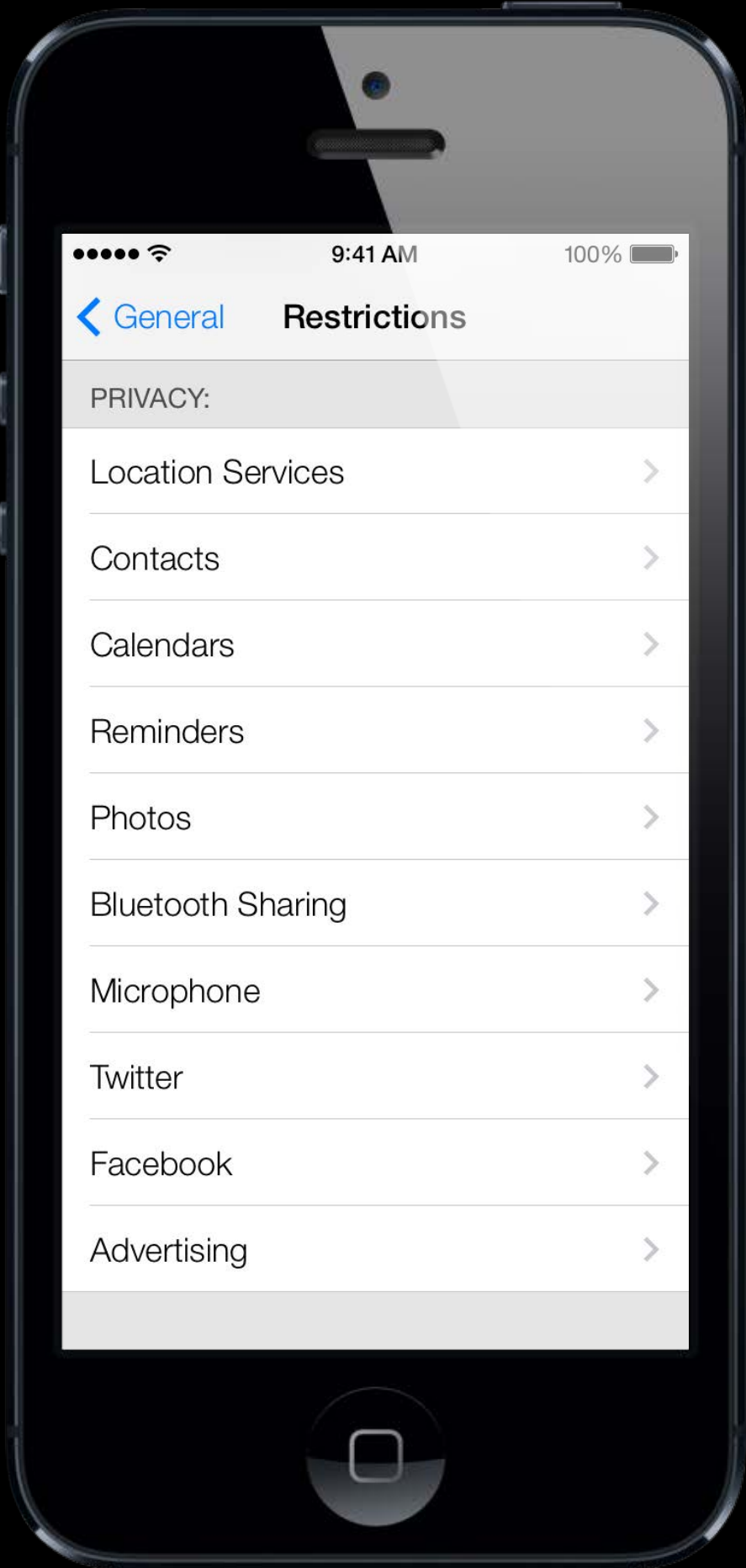
Permission restricted

# Failing Gracefully



- OS can help
  - Fallback behavior when denied
  - Keep the user engaged
- Code should be resilient to lack of data returned
- Restrictions can prevent users from changing privacy settings
  - Enterprise and on-device restrictions

# Restrictions



Conveying Purpose

# Consent Dialogs

**“Camera” Would Like to Use Your Current Location**

Photos and videos will be tagged with the location where they were taken.

[Don't Allow](#) [OK](#)



**“Aperture.app” would like to access your contacts.**

This information will be used to assist you in completing IPTC Contact info, creating slideshows, and using Faces.

[?](#) [Don't Allow](#) [OK](#)

# Purpose Strings

## “Camera” Would Like to Use Your Current Location

Photos and videos will be tagged with the location where they were taken.

Don't Allow

OK



## “Aperture.app” would like to access your contacts.

This information will be used to assist you in completing IPTC Contact info, creating slideshows, and using Faces.



Don't Allow

OK

# Purpose Strings

“Camera” Would Like to Use  
Your Current Location

Photos and videos will be tagged with  
the location where they were taken.

Don't Allow

OK



“Aperture.app” would like to access your  
contacts.

This information will be used to assist you in  
completing IPTC Contact info, creating slideshows,  
and using Faces.



Don't Allow

OK



# Purpose Strings

**“Camera” Would Like to Use  
Your Current Location**

Photos and videos will be tagged with  
the location where they were taken.

Don't Allow

OK



**“Aperture.app” would like to access your  
contacts.**

This information will be used to assist you in  
completing IPTC Contact info, creating slideshows,  
and using Faces.



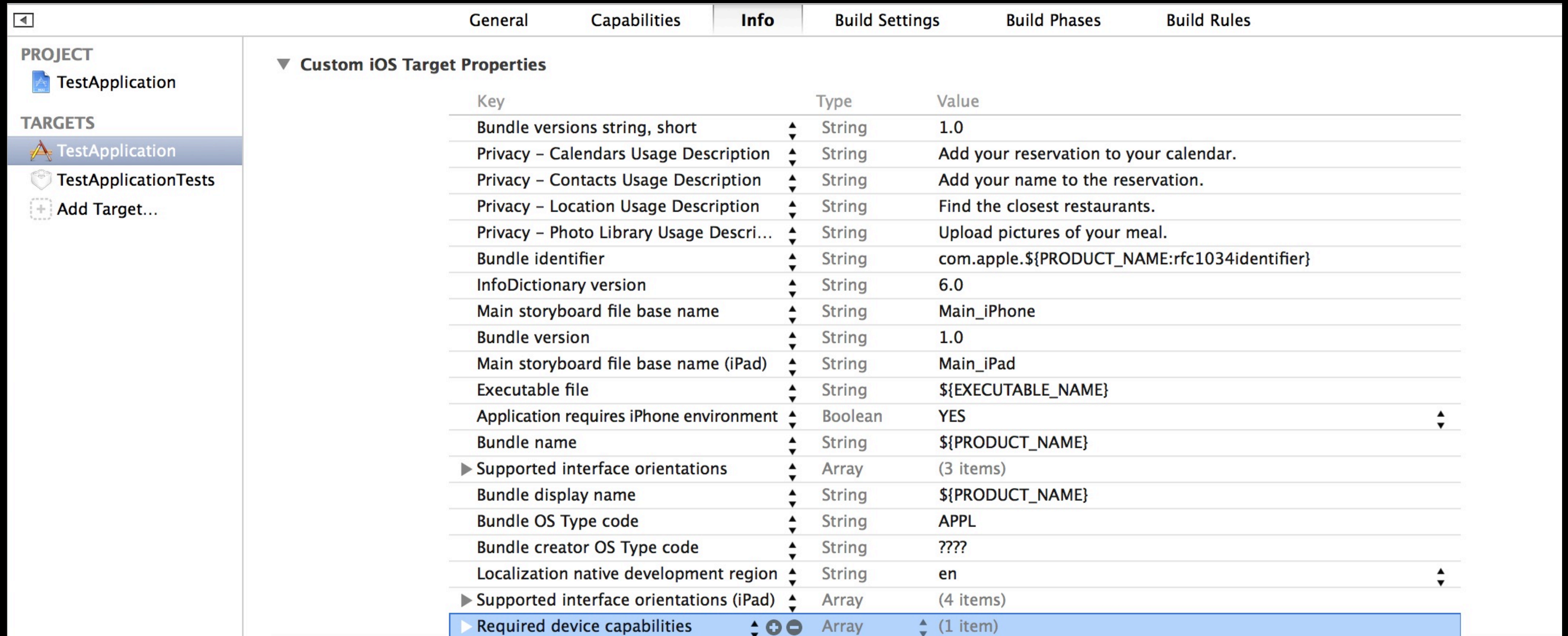
Don't Allow

OK

# Conveying Purpose

- All consent dialogs support developer-specified purpose strings
- Optional, highly encouraged
- One purpose per kind of data
- 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"

# Conveying Purpose



The screenshot shows the Xcode interface with the 'Info' tab selected. The left sidebar shows the project 'TestApplication' and its targets: 'TestApplication', 'TestApplicationTests', and 'Add Target...'. The main area displays a table of 'Custom iOS Target Properties'.

Key	Type	Value
Bundle versions string, short	String	1.0
Privacy - Calendars Usage Description	String	Add your reservation to your calendar.
Privacy - Contacts Usage Description	String	Add your name to the reservation.
Privacy - Location Usage Description	String	Find the closest restaurants.
Privacy - Photo Library Usage Descri...	String	Upload pictures of your meal.
Bundle identifier	String	com.apple.\${PRODUCT_NAME:rfc1034identifier}
InfoDictionary version	String	6.0
Main storyboard file base name	String	Main_iPhone
Bundle version	String	1.0
Main storyboard file base name (iPad)	String	Main_iPad
Executable file	String	\${EXECUTABLE_NAME}
Application requires iPhone environment	Boolean	YES
Bundle name	String	\${PRODUCT_NAME}
▶ Supported interface orientations	Array	(3 items)
Bundle display name	String	\${PRODUCT_NAME}
Bundle OS Type code	String	APPL
Bundle creator OS Type code	String	????
Localization native development region	String	en
▶ Supported interface orientations (iPad)	Array	(4 items)
▶ Required device capabilities	Array	(1 item)

# Conveying Purpose

The screenshot shows the Xcode interface with the 'Info' tab selected. The 'Custom iOS Target Properties' table is visible, listing various keys, their types, and values. A white highlight box is overlaid on the table, covering the rows for 'Privacy - Calendars Usage Description', 'Privacy - Contacts Usage Description', 'Privacy - Location Usage Description', and 'Privacy - Photo Library Usage Description'.

Key	Type	Value
Bundle versions string, short	String	1.0
Privacy - Calendars Usage Description	String	Add your reservation to your calendar.
Privacy - Contacts Usage Description	String	Add your name to the reservation.
Privacy - Location Usage Description	String	Find the closest restaurants.
Privacy - Calendars Usage Description	String	Add your reservation to your calendar.
Privacy - Contacts Usage Description	String	Add your name to the reservation.
Privacy - Location Usage Description	String	Find the closest restaurants.
Privacy - Photo Library Usage Description	String	Upload pictures of your meal.
Bundle version	String	1.0
Main storyboard file base name (iPad)	String	Main_iPad
Executable file	String	\${EXECUTABLE_NAME}
Application requires iPhone environment	Boolean	YES
Bundle name	String	\${PRODUCT_NAME}
Supported interface orientations	Array	(3 items)
Bundle display name	String	\${PRODUCT_NAME}
Bundle OS Type code	String	APPL
Bundle creator OS Type code	String	????
Localization native development region	String	en
Supported interface orientations (iPad)	Array	(4 items)
Required device capabilities	Array	(1 item)

# Purpose Strings

Data Class	Info.plist Key	iOS Only
Location	NSLocationUsageDescription	
Photos	NSPhotoLibraryUsageDescription	●
Calendars	NSCalendarsUsageDescription	
Contacts	NSContactsUsageDescription	
Reminders	NSRemindersUsageDescription	●
Bluetooth	NSBluetoothPeripheralUsageDescription	●
Microphone	NSMicrophoneUsageDescription	●

# iOS Sample Code

- Available on the iOS Developer Center today
- “PrivacyPrompts” project

# Key Points of Data Isolation

- Think about privacy and build it into your applications
- Start today
- New categories: Microphone, Tencent Weibo, camera (only some regions)
- Data isolation applies to both iOS and OS X (OS X has additional work to do)
- Utilize purpose strings
- Test, test, test

# Best Practices



# Best Practices

- Transparency
- Control
- Data collection techniques
- Avoid fingerprinting
- Data protection

# Transparency

- Gives the user opportunities to inspect data
- Privacy policy or statement
  - Important to have one
  - Can submit a link to Apple in iTunes Connect
  - Link visible on the App Store

# Transparency

Edit English

App Name **iTunes Connect Mobile**

Description  ?

What's New in this Version  ?

Keywords **iTunes,Connect,Sales,Trends,Apps,Updates,Revenue,Developer,Tools**

Support URL  ?

Marketing URL (Optional)  ?

Privacy Policy URL (Optional)  ?

# Transparency

Edit English

App Name **iTunes Connect Mobile**

Description  ?

What's New in this Version  ?

Keywords **iTunes,Connect,Sales,Trends,Apps,Updates,Revenue,Developer,Tools**

Support URL  ?

Marketing URL (Optional)  ?

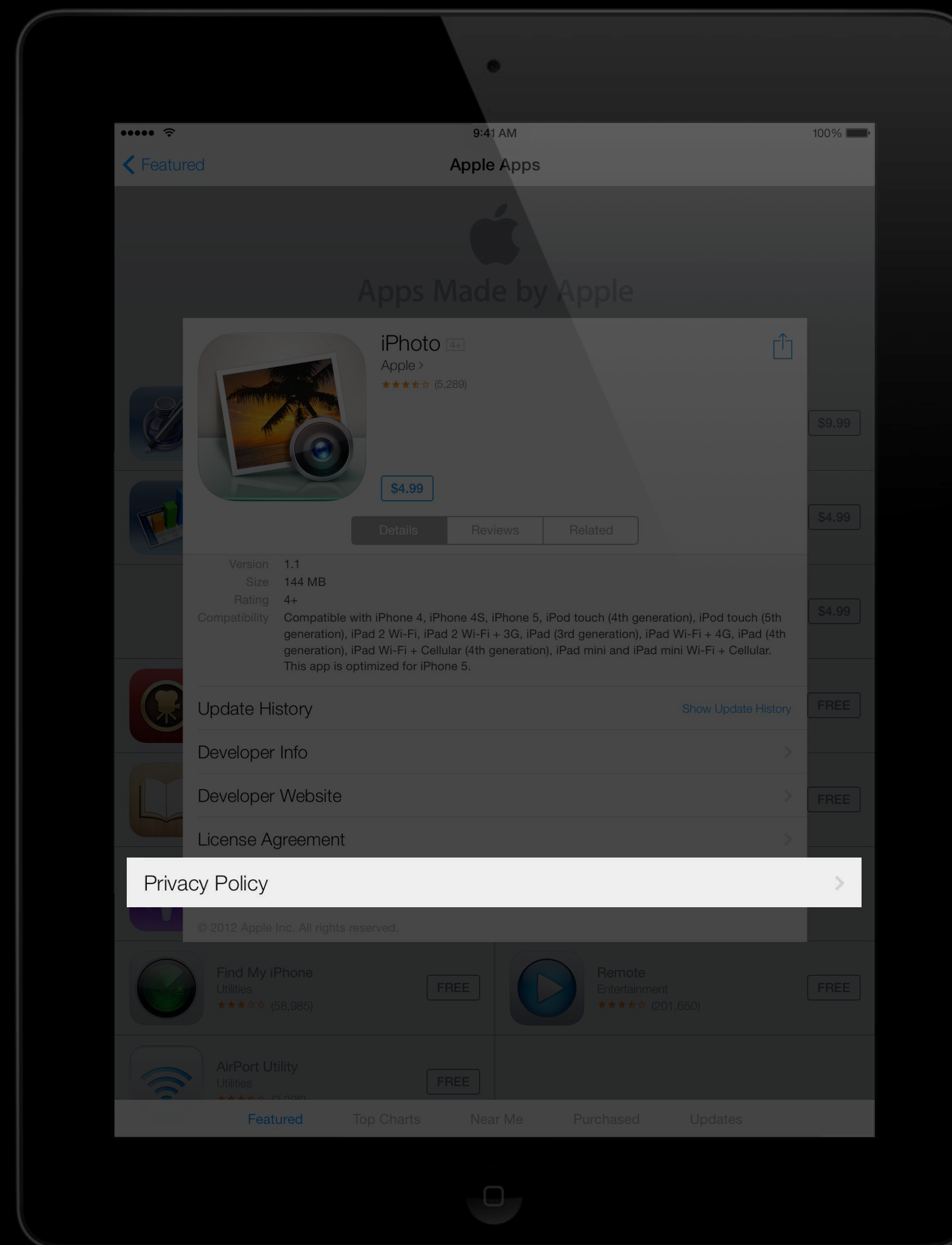
Privacy Policy URL (Optional)  ?

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.

# Transparency



# Transparency



# Control

- Ask for permission with context
- Ask at the time you need it
  - Bad idea—everything right at launch time
- Allow post-hoc changes
- Fail gracefully

# 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

**Anonymize**

# Anonymize

- Initial log—<Error>: Illegal token in "/Users/JohnAppleseed/Documents/ProjectZanzibar/FY2013.keynote"

# Anonymize

- Initial log—<Error>: Illegal token in "/Users/JohnAppleseed/Documents/ProjectZanzibar/FY2013.keynote"
- Better—<Error>: Illegal token in "FY2013.keynote"

# Anonymize

- Initial log—<Error>: Illegal token in `"/Users/JohnAppleseed/Documents/ProjectZanzibar/FY2013.keynote"`
- Better—<Error>: Illegal token in `"FY2013.keynote"`
- Even better—<Error>: Illegal token in `com.apple.keynote file`

# Aggregate

# Aggregate

- Initial log—<Error>: Illegal token in "/Users/JohnAppleseed/Documents/ProjectZanzibar/FY2013.keynote"

# Aggregate

- Initial log—<Error>: Illegal token in "/Users/JohnAppleseed/Documents/ProjectZanzibar/FY2013.keynote"
- Better—<Error>: Illegal tokens {com.apple.keynote: 21; com.foo.doc: 3}



Sample

# Sample

- Initial log—<Error>: Illegal token in com.apple.keynote file

# Sample

- Initial log—<Error>: Illegal token in com.apple.keynote file
- Better—Collect data from only 1 computer in 10 (or 100, or more)

# Sample

- Initial log—<Error>: Illegal token in com.apple.keynote file
- Better—Collect data from only 1 computer in 10 (or 100, or more)
- Even better—Collect data from only 1 operation in 10 (or 100...)

De-Resolve

# De-Resolve

- Initial log—<Info>: May 4 15:03:19: Action succeeded,  
processed 22341 bytes

# De-Resolve

- Initial log—<Info>: May 4 15:03:19: Action succeeded, processed 22341 bytes
- Better—<Info>: May 4 15:00: Action succeeded, processed 22 kB

# De-Resolve

- Initial log—<Info>: May 4 15:03:19: Action succeeded, processed 22341 bytes
- Better—<Info>: May 4 15:00: Action succeeded, processed 22 kB
- Even better—<Info>: Friday 15:00: Action succeeded, processed 20 kB



Decay

# Decay

- Initial log—<Info>: May 4 15:03:19: Action succeeded,  
processed 22341 bytes

# Decay

- Initial log—<Info>: May 4 15:03:19: Action succeeded, processed 22341 bytes
- After 7 days—<Info>: May 4: Action succeeded, processed 22341 bytes

# Decay

- Initial log—<Info>: May 4 15:03:19: Action succeeded, processed 22341 bytes
- After 7 days—<Info>: May 4: Action succeeded, processed 22341 bytes
- After 30 days—<Info>: [Redacted]: Action succeeded, processed 22 kB

**Minimize**

# Minimize

- Initial log—<Info>: May 4 15:03:19: Action succeeded,  
processed 22341 bytes

# Minimize

- Initial log—<Info>: May 4 15:03:19: Action succeeded, processed 22341 bytes
- Better—no collection

# Collection Techniques

- Anonymize
- Aggregate
- Sample
- De-resolve
- Decay
- Minimize



# Avoid Fingerprinting

- A collection of many static metrics form a unique, persistent “fingerprint” for a specific device
- Does not need personal information
- Easy to do accidentally

# Data Protection

- Store important application credentials in the keychain
  - Make a conscious decision if the data will be synchronized among devices
- Encrypt client-server communication using SSL/TLS
- Use Data Protection for data your application stores to disk
  - `NSFileProtectionComplete`, `NSFileProtectionCompleteUnlessOpen`,  
`NSFileProtectionCompleteUntilFirstAuthentication`
- WWDC 2012 Session 706, Protecting User's Data

# Best Practices

- Transparency
- Control
- Data collection techniques
- Avoid fingerprinting
- Data protection

# Related Sessions

Protecting Secrets with the Keychain

Marina  
Wednesday 11:30AM

A Practical Guide to the App Sandbox

Russian Hill  
Wednesday 2:00PM

# Labs

Privacy and Security Lab

Core OS Lab A  
Friday 10:15AM



# More Information

## Paul Danbold

Core OS Evangelist  
[danbold@apple.com](mailto:danbold@apple.com)

## Sample Code

PrivacyPrompts

<http://developer.apple.com/library/prerelease/ios/samplecode/PrivacyPrompts/index.html>

## Documentation

Best Practices for Maintaining User Privacy

[https://developer.apple.com/library/ios/#documentation/iPhone/Conceptual/iPhoneOSProgrammingGuide/AppDesignBasics/AppDesignBasics.html#//apple\\_ref/doc/uid/TP40007072-CH2-SW7](https://developer.apple.com/library/ios/#documentation/iPhone/Conceptual/iPhoneOSProgrammingGuide/AppDesignBasics/AppDesignBasics.html#//apple_ref/doc/uid/TP40007072-CH2-SW7)

## Apple Developer Forums

<http://devforums.apple.com>

# Summary

- Ensure identifier changes do not have user impact
- Test all cases of data isolation access
- Add purpose strings
- Submit a privacy statement link to the App Store
- Collect only data needed to drive specific decisions
- Maintain your reputation by thinking through privacy implications in your design

 WWDC2013