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

The figure illustrates the changes in iOS 6, focusing on the move from UDID to a new ID system. The table below shows the scope of different identifiers:

<table>
<thead>
<tr>
<th>Identifier</th>
<th>Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application ID</td>
<td>App</td>
</tr>
<tr>
<td>Vendor ID</td>
<td>Developer</td>
</tr>
<tr>
<td>Advertising ID</td>
<td>Device</td>
</tr>
</tbody>
</table>
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—46b74f03b8de6726e5f9c2889e84e32fe938e24c
• In iOS 7—FFFFFFFF<Vendor Identifier without dashes>
• UDID—46b74f03b8de6726e5f9c2889e84e32fe938e24c
• In iOS 7—FFFFFFFF<Vendor Identifier without dashes>
• Vendor ID—BBBBDD211–B69B–4FB4–9CB3–6D7A42FB5A6B
• In iOS 7—FFFFFFFFBBBBDD211B69B4FB49CB36D7A42FB5A6B
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

The future "UDID" would look like FFFFFFFFBBBDD211B69B4FB49CB36D7A42FB5A6B
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

App 1

App 2

53BDBF59-43E3-4B6E-A5C8-52F2102931BA
Vendor Identifier
Vendor Identifier

App 2

02C3EBF3-2951-4D4E-8048-03A5C1FF6C79
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
<table>
<thead>
<tr>
<th>Ridge Replacement APIs</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scope</strong></td>
</tr>
<tr>
<td>Application ID</td>
</tr>
<tr>
<td>Vendor ID</td>
</tr>
<tr>
<td>Advertising ID</td>
</tr>
</tbody>
</table>
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
  ▪ 02:00:00:00:00:00:00
• Applies to existing apps
gethostuuuid()

• 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
"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
“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

<table>
<thead>
<tr>
<th>Data Class</th>
<th>Mountain Lion</th>
<th>Mavericks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contacts</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Location</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Calendars</td>
<td></td>
<td>●</td>
</tr>
<tr>
<td>Reminders</td>
<td></td>
<td>●</td>
</tr>
</tbody>
</table>
# Existing and New Support on OS X

<table>
<thead>
<tr>
<th>Data Class</th>
<th>Mountain Lion</th>
<th>Mavericks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Twitter</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Sina Weibo</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>LinkedIn</td>
<td></td>
<td>●</td>
</tr>
<tr>
<td>Tencent Weibo</td>
<td></td>
<td>●</td>
</tr>
</tbody>
</table>
### Existing and New Support on iOS

<table>
<thead>
<tr>
<th>Data Class</th>
<th>iOS 6</th>
<th>iOS 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contacts</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Location</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Calendars</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Reminders</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Photos</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Bluetooth</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Microphone</td>
<td></td>
<td>●</td>
</tr>
<tr>
<td>Camera (only some regions)</td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>
# Existing and New Support on iOS

<table>
<thead>
<tr>
<th>Data Class</th>
<th>iOS 6</th>
<th>iOS 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facebook</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Twitter</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Sina Weibo</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Tencent Weibo</td>
<td></td>
<td>●</td>
</tr>
</tbody>
</table>
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
### App Sandbox

<table>
<thead>
<tr>
<th>Network</th>
<th>Hardware</th>
<th>App Data</th>
<th>File Access</th>
</tr>
</thead>
</table>
| - [ ] Incoming Connections (Server) | - [ ] Camera     | [ ] Contacts | [ ] User Selected File | Permission & Access: None
| - [ ] Outgoing Connections (Client) | - [ ] Microphone  | [ ] Location  | [ ] Downloads Folder | None
|                              | - [ ] USB        |            | [ ] Pictures Folder | None
|                              | - [ ] Printing   |            | [ ] Music Folder    | None
|                              |                  |            | [ ] Movies Folder   | None

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

Capabilities

App Data: 
- Contacts
- Calendar

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

Hardware: 
- Camera
- Microphone
- USB
Privacy Support in 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

<table>
<thead>
<tr>
<th>Data Type</th>
<th>System Authorization Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td><code>+[CLLocationManager authorizationStatus]</code></td>
</tr>
<tr>
<td></td>
<td><code>-[CLLocationManager startUpdatingLocation]</code></td>
</tr>
<tr>
<td>Photos, videos, and other media</td>
<td><code>-[ALAssetLibrary enumerateGroupsWithTypes:usingBlock:failureBlock:]</code></td>
</tr>
<tr>
<td></td>
<td><code>-[UIImagePickerController alloc] init</code></td>
</tr>
<tr>
<td>Contacts</td>
<td><code>ABAddressBookGetAuthorizationStatus()</code></td>
</tr>
<tr>
<td></td>
<td><code>ABAddressBookRequestAccessWithCompletion(ABAddressBookRef, ABAddressBookRequestAccessCompletionHandler)</code></td>
</tr>
</tbody>
</table>
## APIs in OS X and iOS

<table>
<thead>
<tr>
<th>Data Type</th>
<th>System Authorization Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reminders</td>
<td>-[EKEventStore requestAccessToEntityType:completion:]</td>
</tr>
<tr>
<td></td>
<td>+[EKEventStore authorizationStatusForEntityType]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Calendars</td>
<td>-[EKEventStore requestAccessToEntityType:completion:]</td>
</tr>
<tr>
<td></td>
<td>+[EKEventStore authorizationStatusForEntityType]</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Bluetooth</td>
<td>-[CBCentralManager initWithDelegate:queue:]</td>
</tr>
<tr>
<td></td>
<td>-[CBCentralManager scanForPeriperhalsWithService:options:]</td>
</tr>
</tbody>
</table>
# APIs in OS X and iOS

<table>
<thead>
<tr>
<th>Data Type</th>
<th>System Authorization Support</th>
</tr>
</thead>
</table>
| 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];
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
Tencent Weibo
Tencent Weibo

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

ACAccountType *tencentWeiboAccount = [self.accountStore accountTypeWithAccountTypeIdentifier:ACAccountTypeIdentifierTencentWeibo];
ACAccountStore *accountStore = [[ACAccountStore alloc] init];

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

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

ACAccountType *socialAccount = [accountStore
accountTypeWithAccountTypeIdentifier: 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
<table>
<thead>
<tr>
<th>Test Cases</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permission being sought and denied</td>
</tr>
<tr>
<td>Permission being sought and granted</td>
</tr>
<tr>
<td>Permission previously denied</td>
</tr>
<tr>
<td>Permission restricted</td>
</tr>
</tbody>
</table>
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
“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.

“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

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.

“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.
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
### Conveying Purpose

#### Custom iOS Target Properties

<table>
<thead>
<tr>
<th>Key</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bundle versions string, short</td>
<td>String</td>
<td>1.0</td>
</tr>
<tr>
<td>Privacy – Calendars Usage Description</td>
<td>String</td>
<td>Add your reservation to your calendar.</td>
</tr>
<tr>
<td>Privacy – Contacts Usage Description</td>
<td>String</td>
<td>Add your name to the reservation.</td>
</tr>
<tr>
<td>Privacy – Location Usage Description</td>
<td>String</td>
<td>Find the closest restaurants.</td>
</tr>
<tr>
<td>Privacy – Photo Library Usage Description</td>
<td>String</td>
<td>Upload pictures of your meal.</td>
</tr>
</tbody>
</table>

- `Bundle version string, short`: 1.0
- `Privacy – Calendars Usage Description`: Add your reservation to your calendar.
- `Privacy – Contacts Usage Description`: Add your name to the reservation.
- `Privacy – Location Usage Description`: Find the closest restaurants.
- `Privacy – Photo Library Usage Description`: Upload pictures of your meal.
# Purpose Strings

<table>
<thead>
<tr>
<th>Data Class</th>
<th>Info.plist Key</th>
<th>iOS Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>NSLocationUsageDescription</td>
<td></td>
</tr>
<tr>
<td>Photos</td>
<td>NSPhotoLibraryUsageDescription</td>
<td><img src="https://via.placeholder.com/15" alt="iOS Only" /></td>
</tr>
<tr>
<td>Calendars</td>
<td>NSCalendarsUsageDescription</td>
<td></td>
</tr>
<tr>
<td>Contacts</td>
<td>NSContactsUsageDescription</td>
<td></td>
</tr>
<tr>
<td>Reminders</td>
<td>NSRemindersUsageDescription</td>
<td><img src="https://via.placeholder.com/15" alt="iOS Only" /></td>
</tr>
<tr>
<td>Bluetooth</td>
<td>NSBluetoothPeripheralUsageDescription</td>
<td><img src="https://via.placeholder.com/15" alt="iOS Only" /></td>
</tr>
<tr>
<td>Microphone</td>
<td>NSMicrophoneUsageDescription</td>
<td><img src="https://via.placeholder.com/15" alt="iOS Only" /></td>
</tr>
</tbody>
</table>
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
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.

Keywords: iTunes, Connect, Sales, Trends, Apps, Updates, Revenue, Developer, Tools
iTunes Connect Mobile

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.

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

- 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

Aggregate


- 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

<table>
<thead>
<tr>
<th>Session</th>
<th>Location</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protecting Secrets with the Keychain</td>
<td>Marina</td>
<td>Wednesday 11:30AM</td>
</tr>
<tr>
<td>A Practical Guide to the App Sandbox</td>
<td>Russian Hill</td>
<td>Wednesday 2:00PM</td>
</tr>
</tbody>
</table>
| Privacy and Security Lab | Core OS Lab A  
|------------------------|------------------  
|                        | Friday 10:15AM   |
More Information

Paul Danbold
Core OS Evangelist
danbold@apple.com

Sample Code
PrivacyPrompts

Documentation
Best Practices for Maintaining User Privacy

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