User Privacy on iOS and OS X

Session 715

David Stites
Apple Product Security and Privacy

Katie Skinner
Apple Product Security and Privacy

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

```
[NSUUID UUID]
```

Vendor Identifier

```
[[UIDevice currentDevice] identifierForVendor]
```

Advertising Identifier

```
[[UIDevice currentDevice] identifierForAdvertising]
```

Identifier APIs

Protecting Your User's Privacy

WWDC 2013

Identifier 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	"Reset Advertising ID"	Yes	No

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]
```

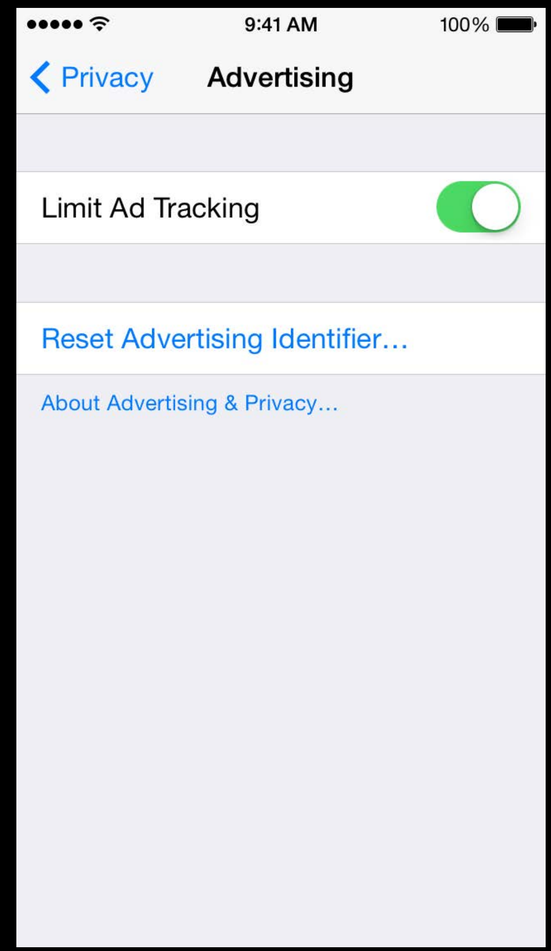
Required to check the value of this property before using Advertising Identifier

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

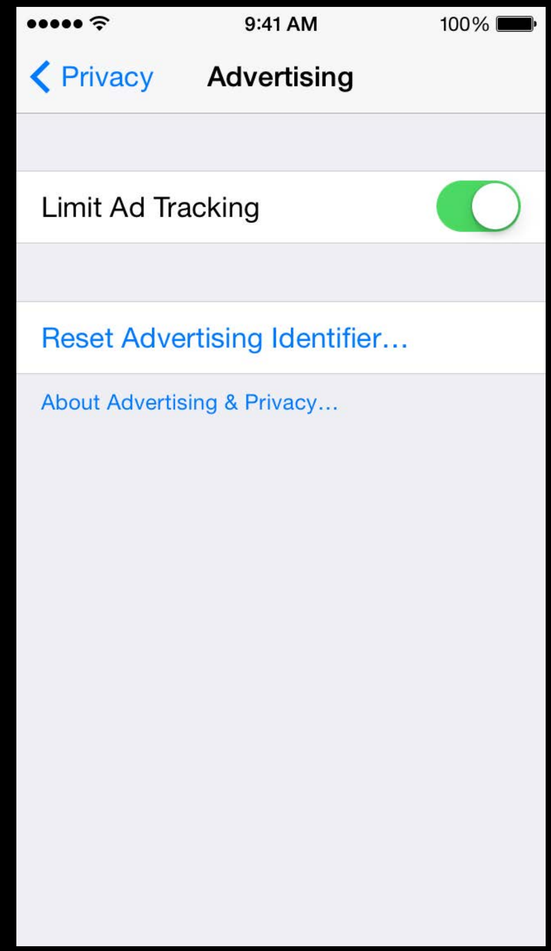


Advertising Identifier

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

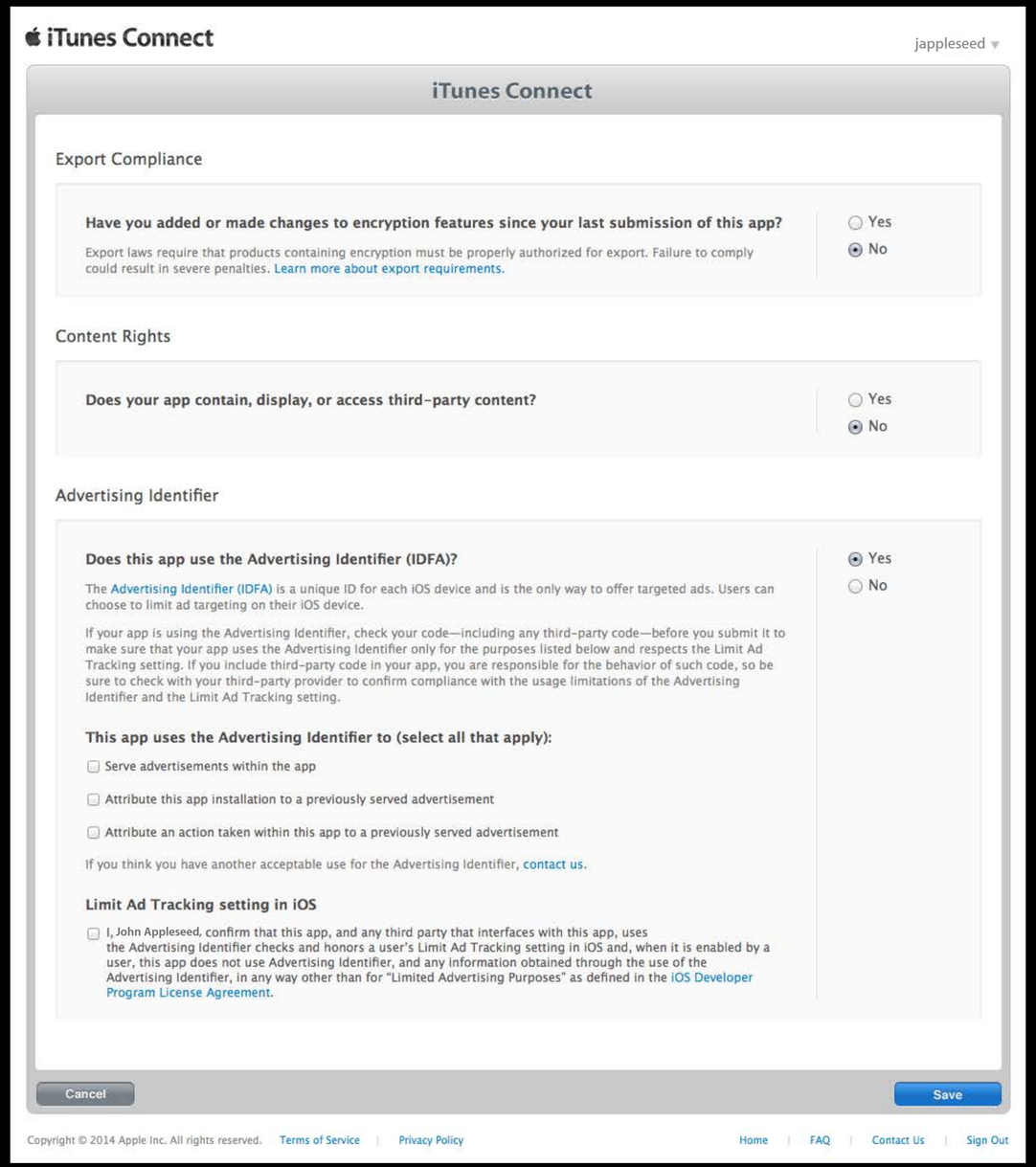


Advertising Identifier

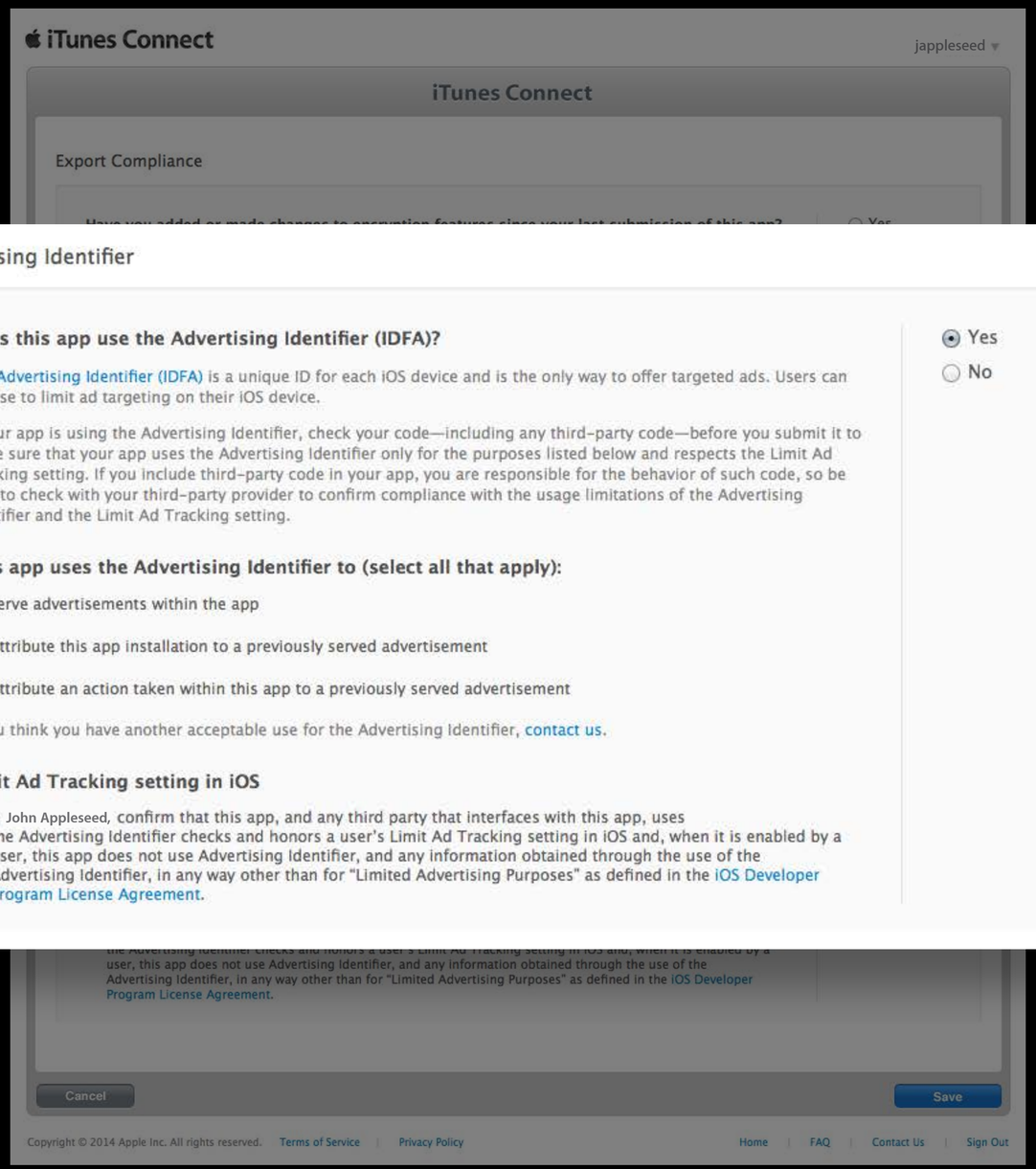
In iTunes Connect, select how your app is using the Advertising Identifier

- Serve advertisements
- Attribute app installation with previously served advertisement
- Attribute an action taken to a previously served advertisement

iTunes Connect and Advertising Identifier



iTunes Connect and Advertising Identifier



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

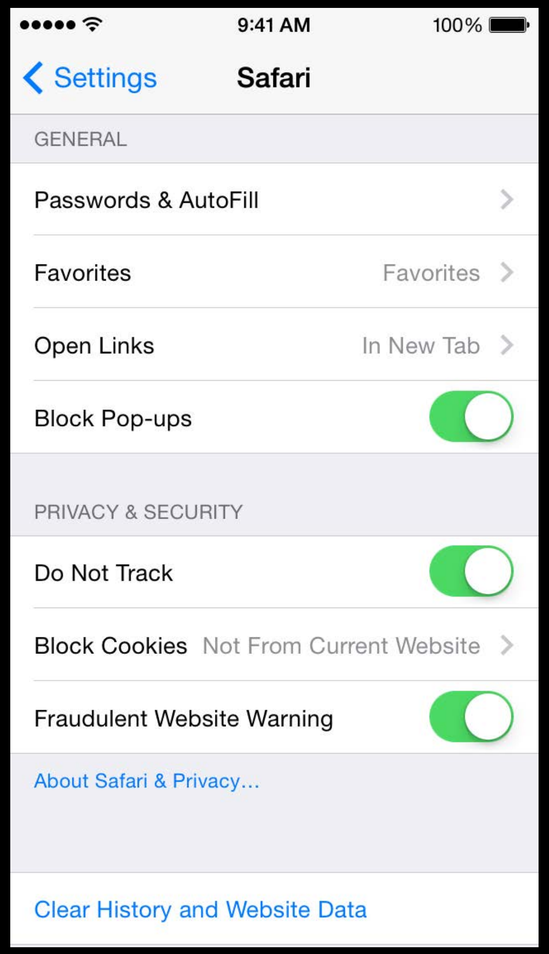
Safari Third Party Cookie Policy

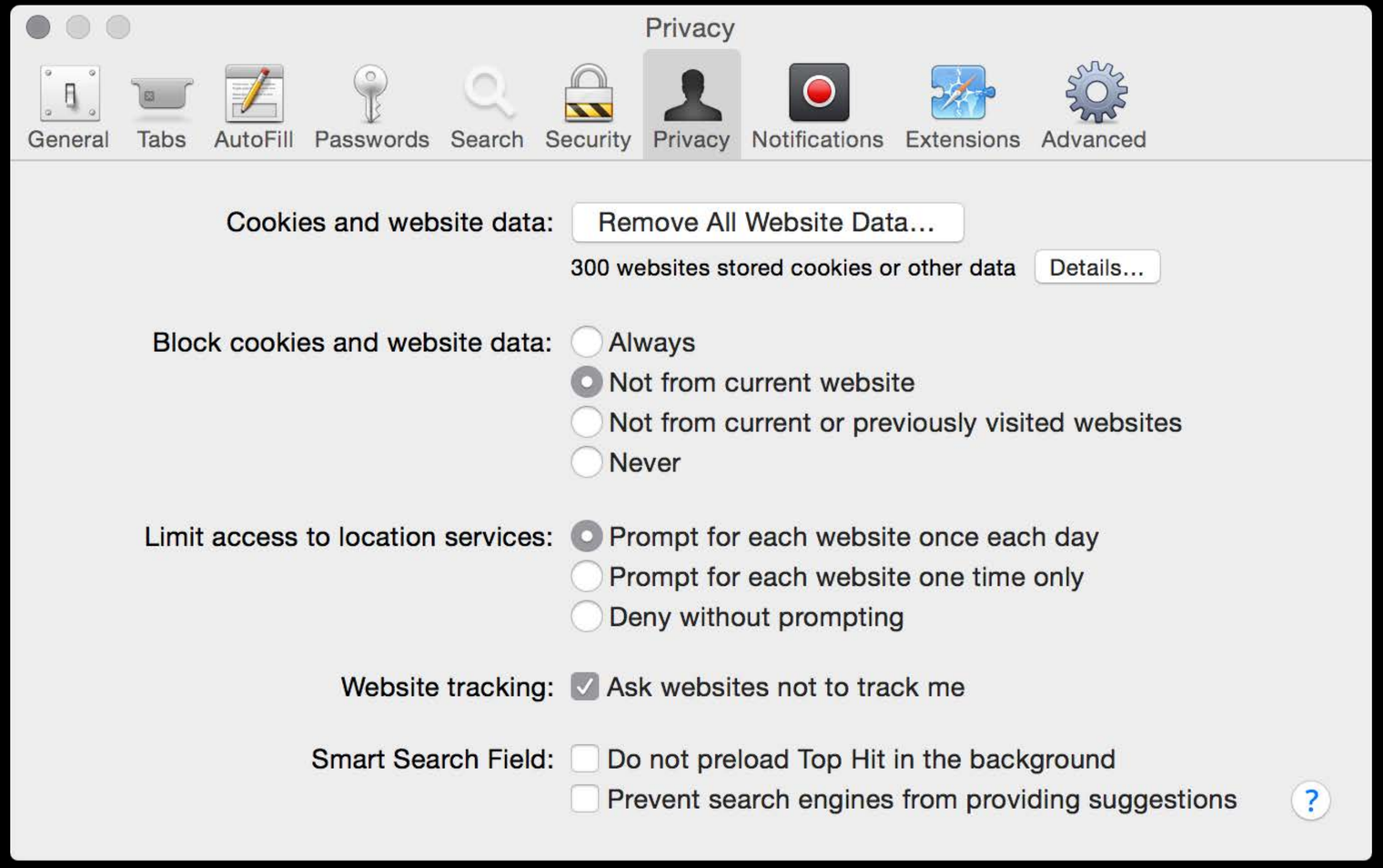
New setting to block all third party cookies, regardless of whether the user has visited a site previously

Example—foo.com iframe on apple.com won't be able to read or write foo.com cookies

Safari Third Party Cookie Policy

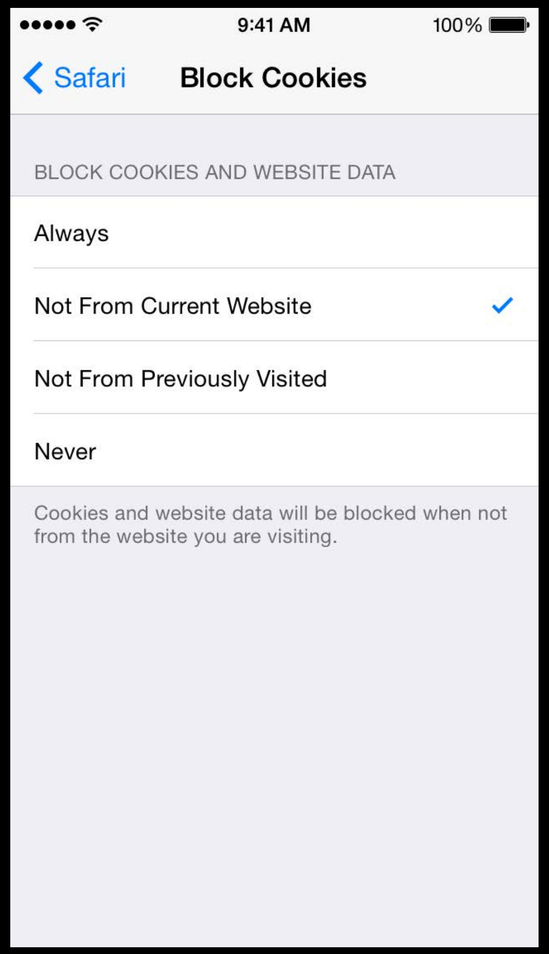
NEW

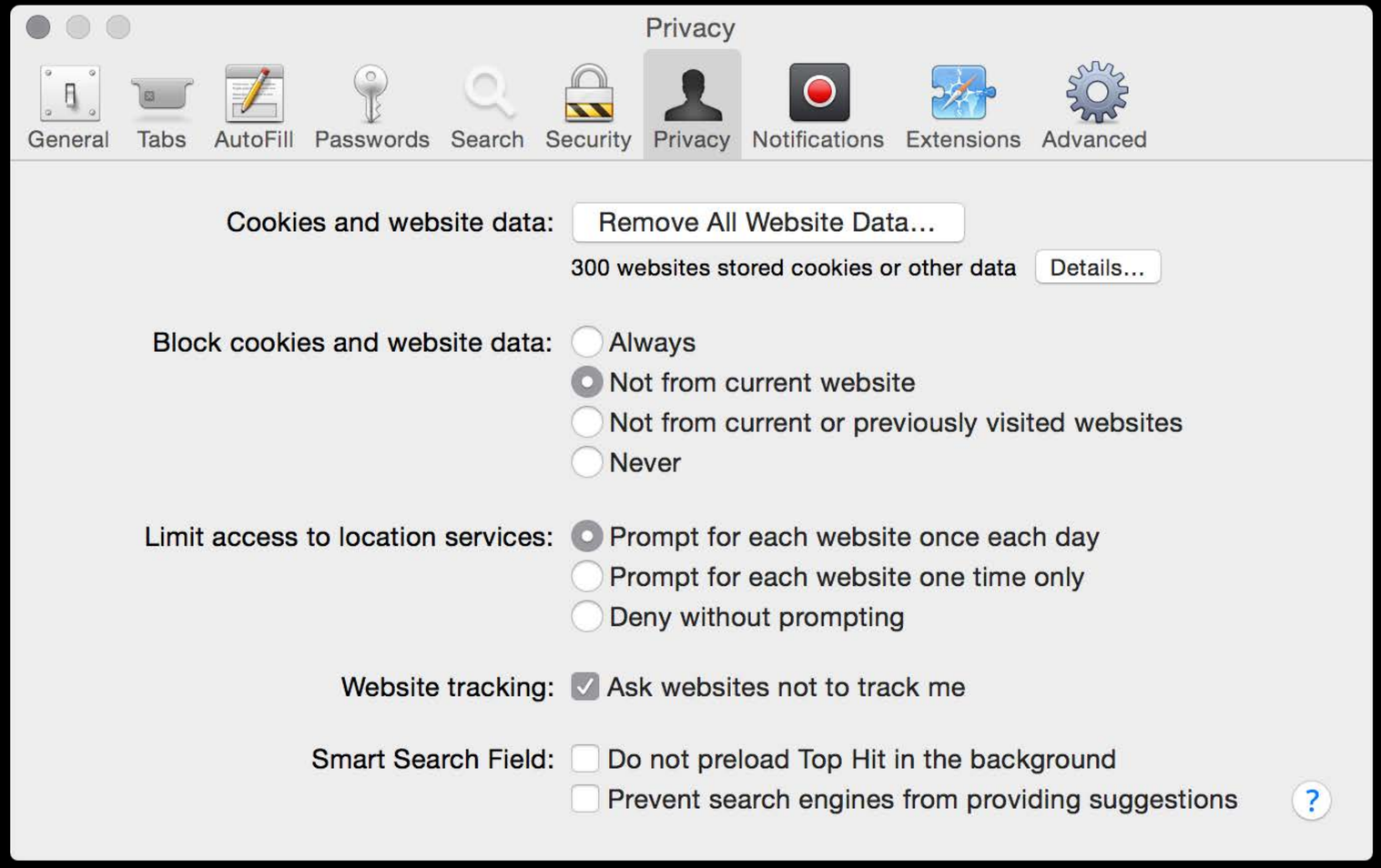




Safari Third Party Cookie Policy

NEW





People Picker

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

https://developer.apple.com/library/ios/people_picker_sample

People Picker

iOS 7 Delegate Methods

```
-[ABPeoplePickerNavigationControllerDelegate
peoplePickerNavigationController:shouldContinueAfterSelectingPerson:]
-[ABPeoplePickerNavigationControllerDelegate
peoplePickerNavigationController: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

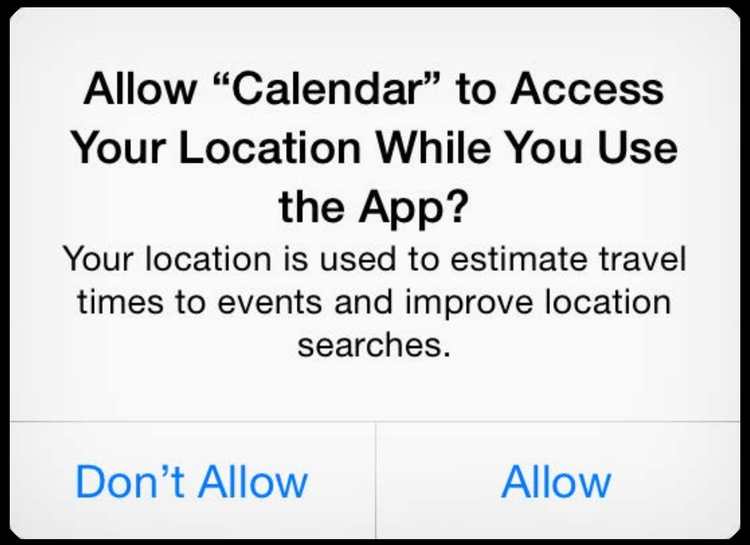
Design the experience

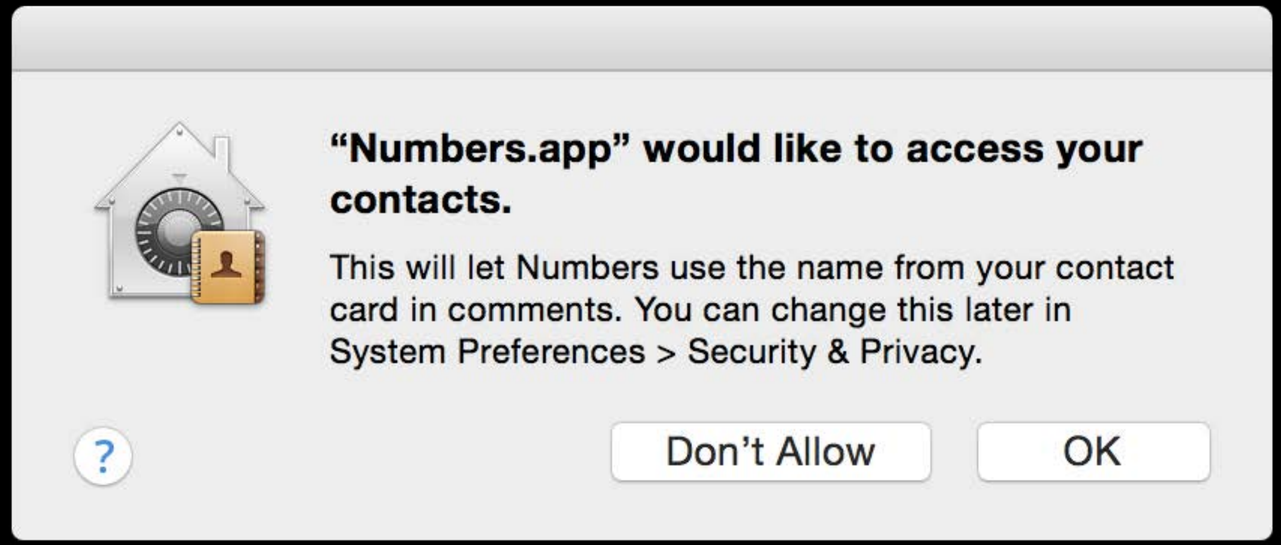
Five core principles for “prompting with purpose”

- Consent
- Transparency
- Context
- Clarity
- Minimization

Prompting with Purpose

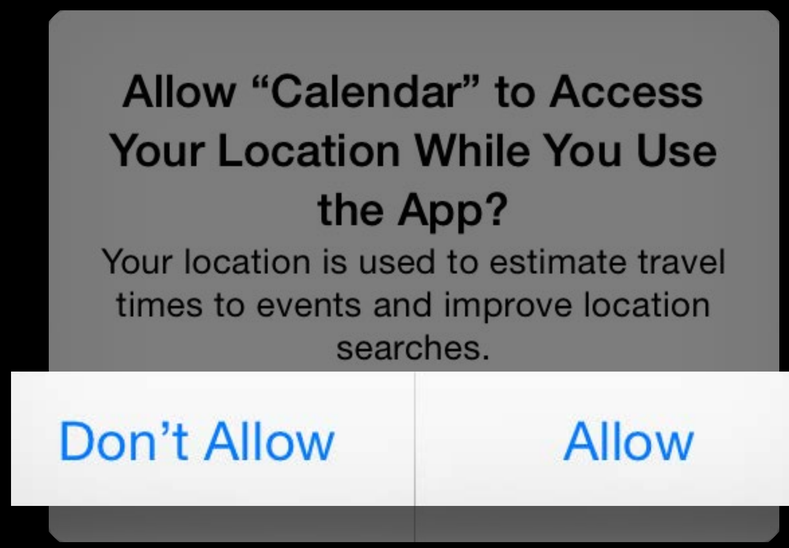
Consent

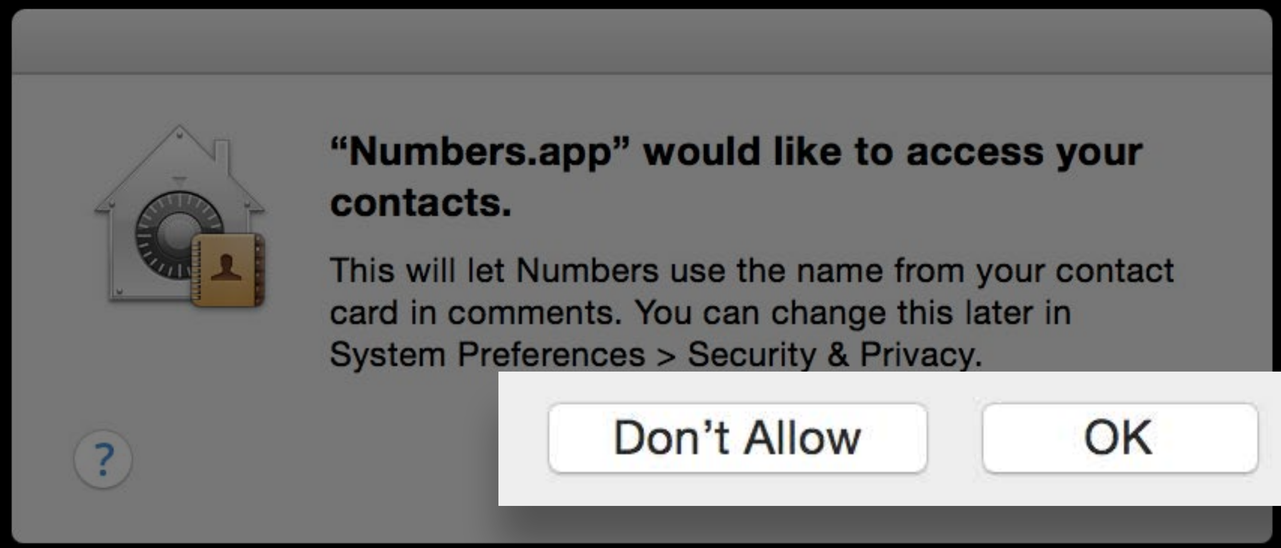




Prompting with Purpose

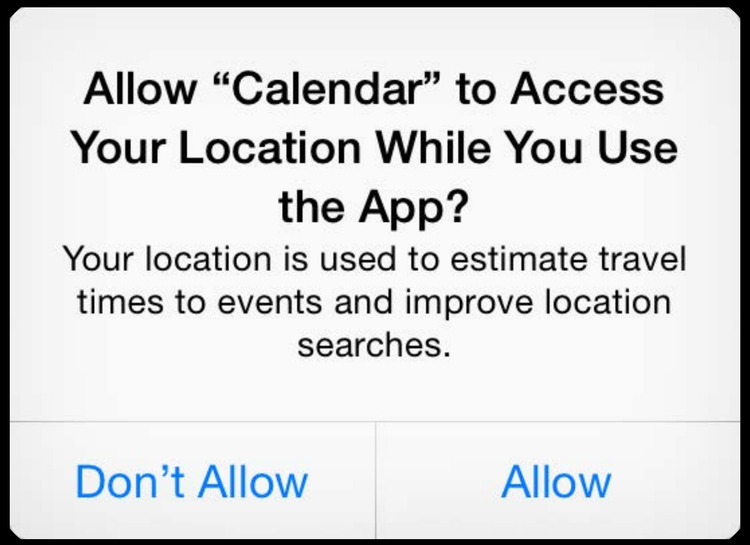
Consent

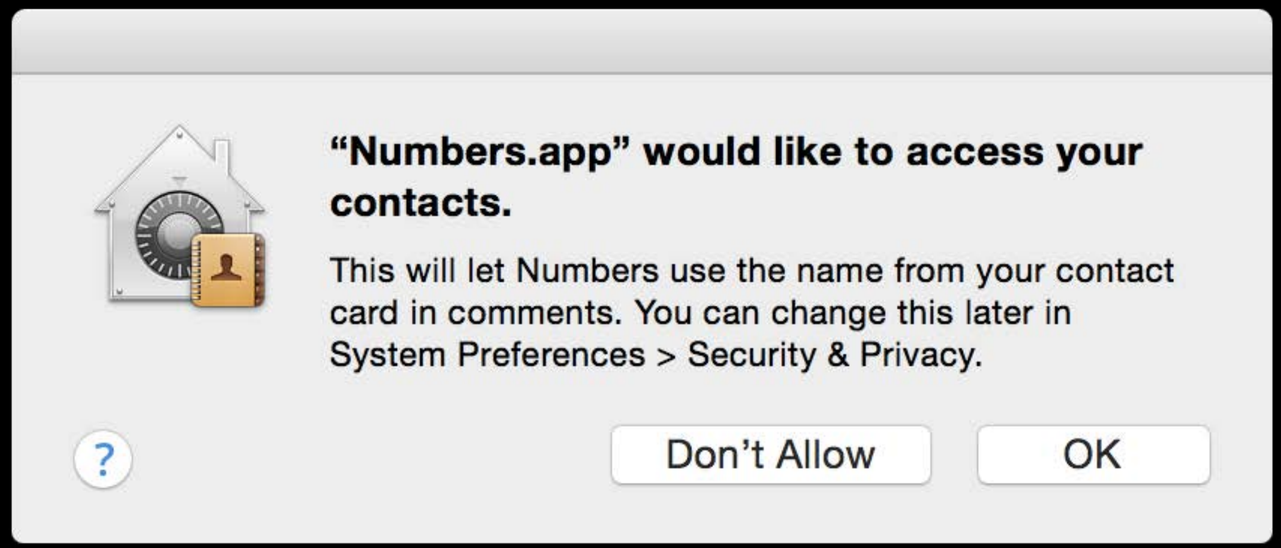




Prompting with Purpose

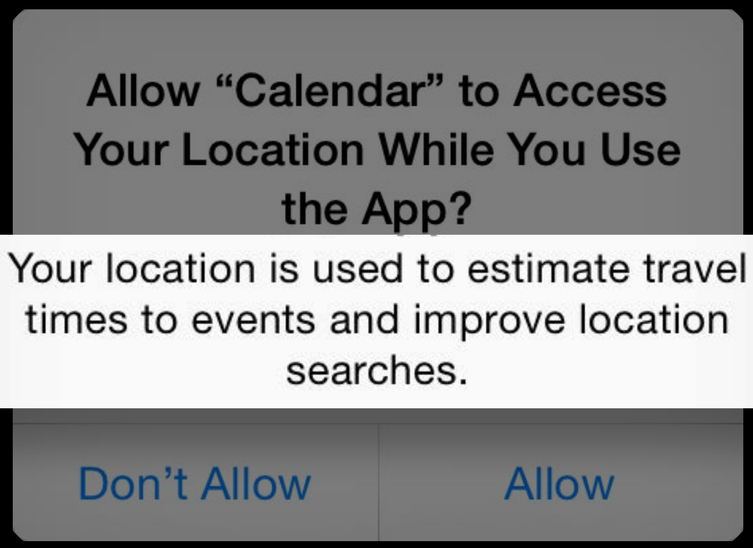
Transparency

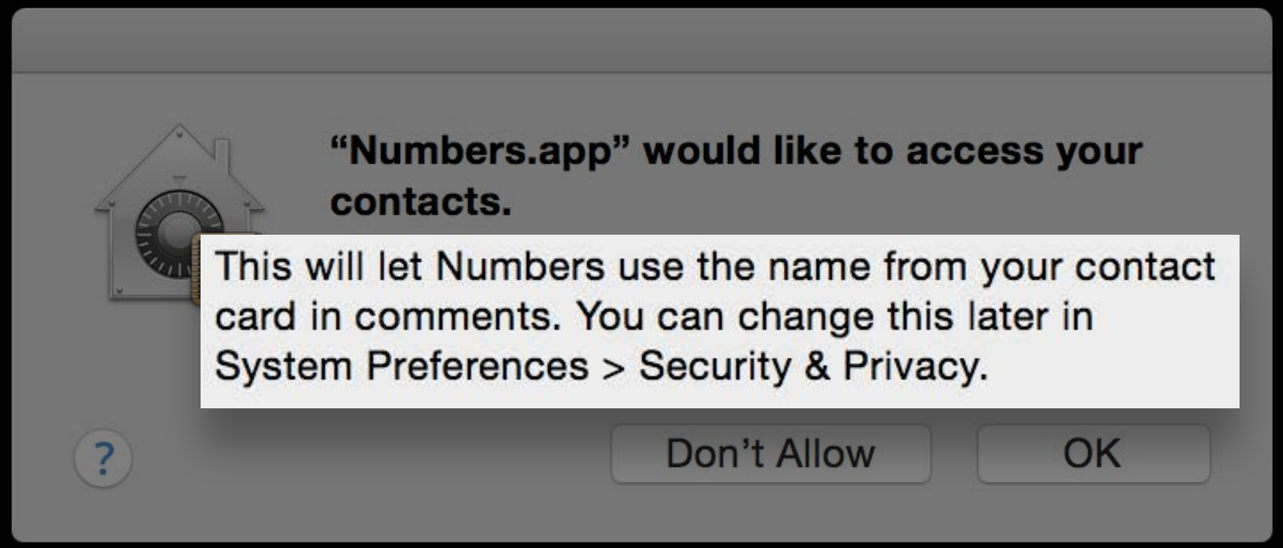




Prompting with Purpose

Transparency

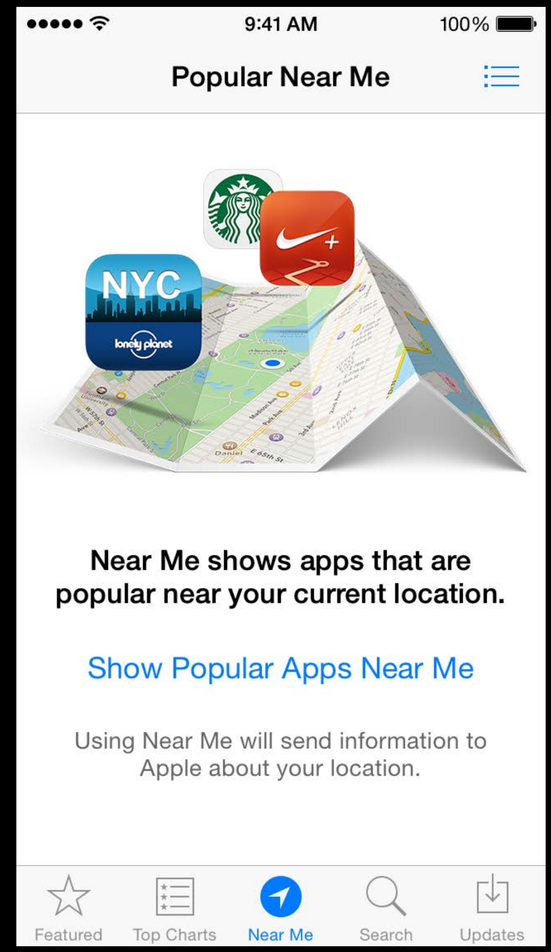




Prompting with Purpose

Context

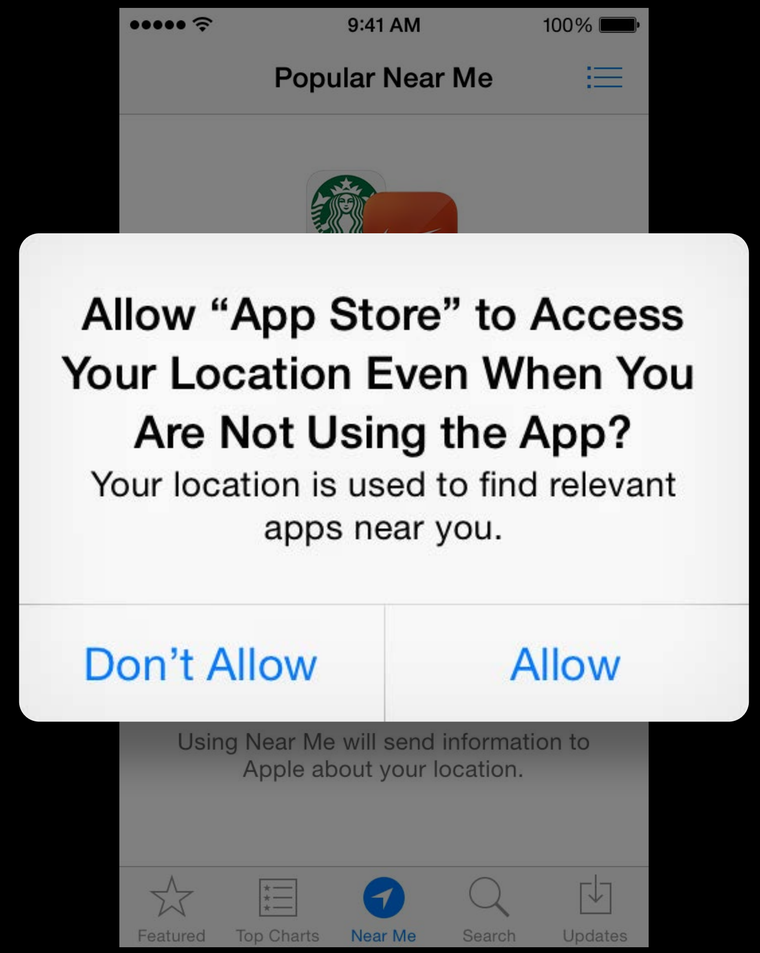
Tie prompting to a user-initiated action



Prompting with Purpose

Context

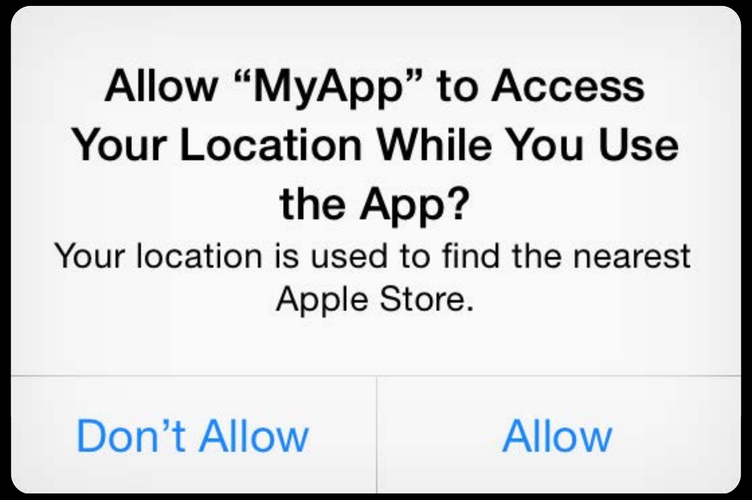
Tie prompting to a user-initiated action



Prompting with Purpose

Context

Tie prompting to a user-initiated action

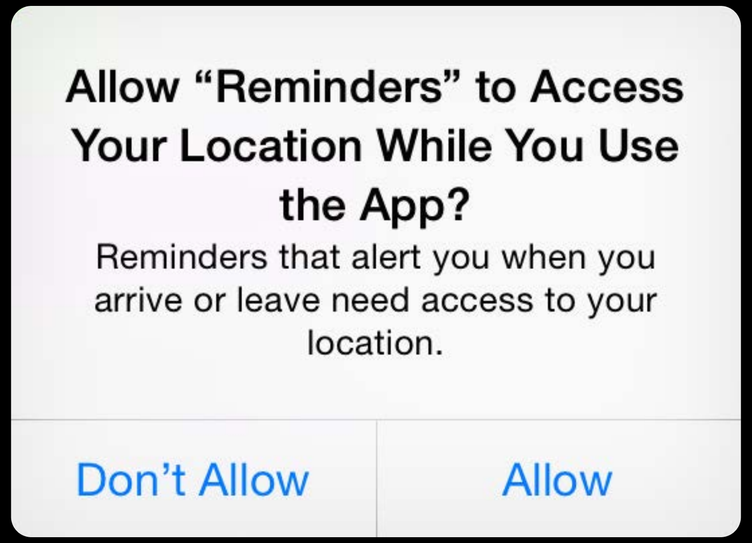


Prompting with Purpose

Clarity

Distill the purpose of your request down to its essence

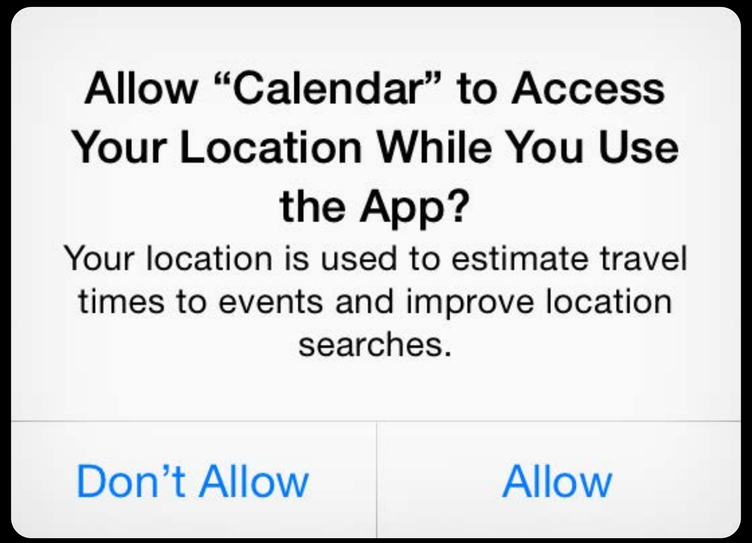
Be concise but include sufficient detail



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

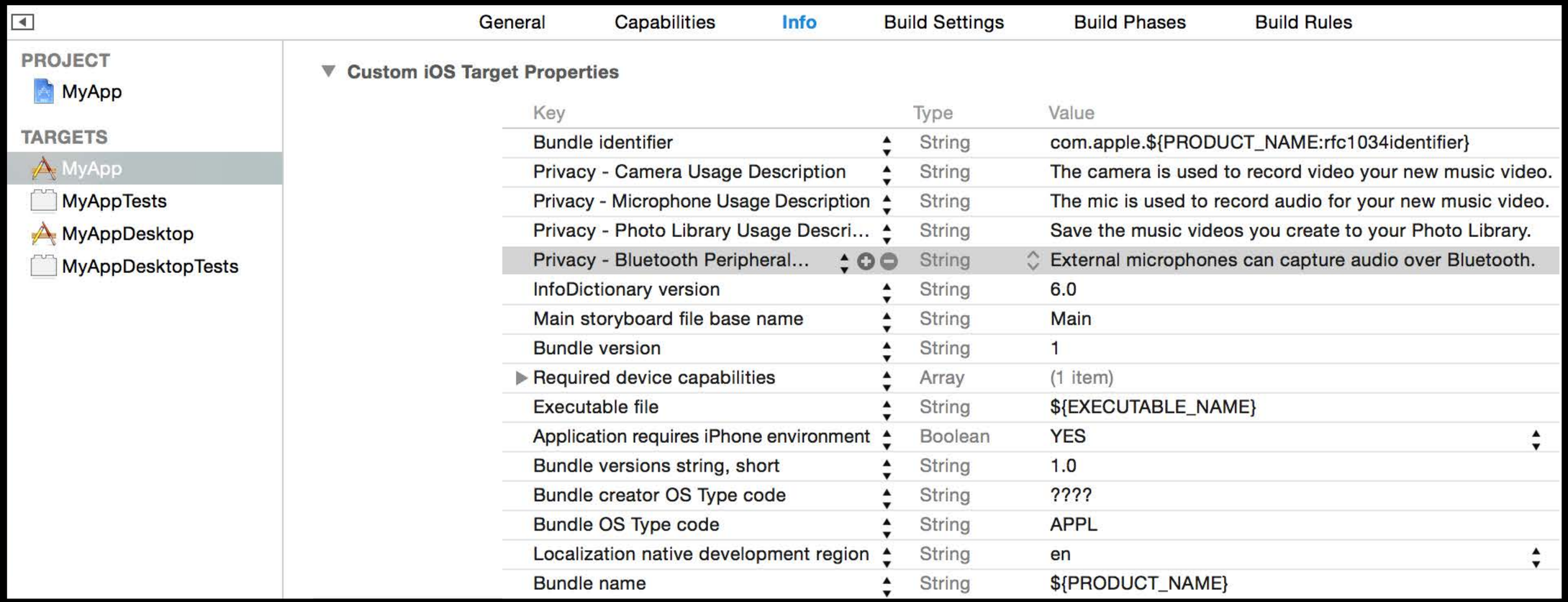
- Add localized versions in Localizable.strings

Look for "Privacy—" keys and provide a value

- e.g. "Privacy—Contacts Usage Description"

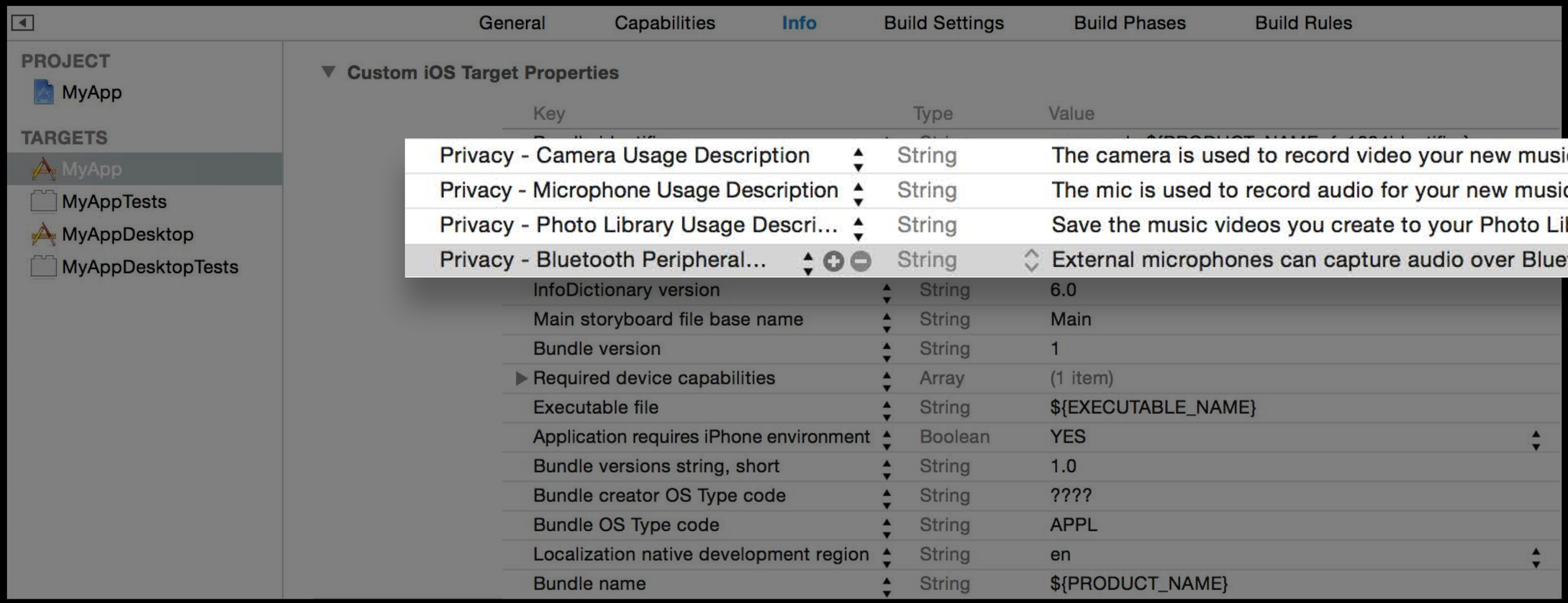
Conveying Purpose

Xcode



Conveying Purpose

Xcode

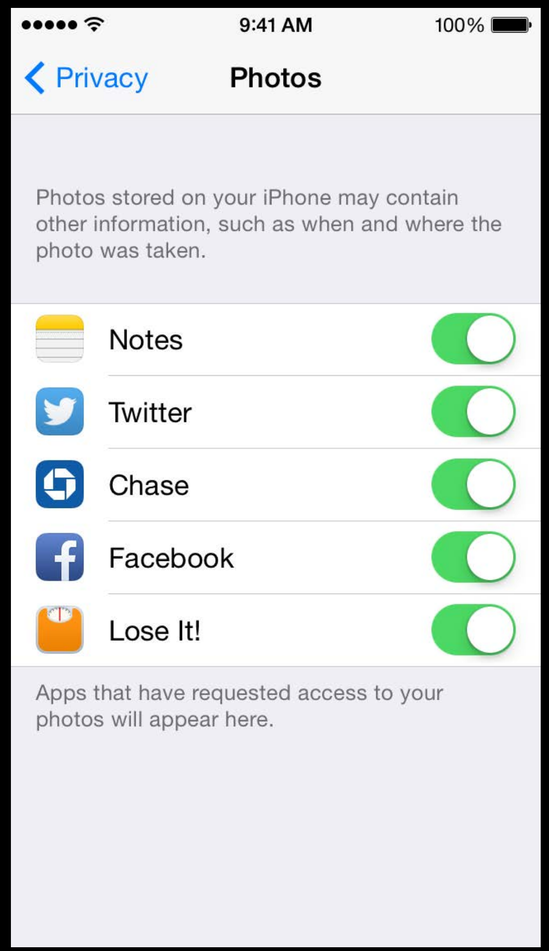


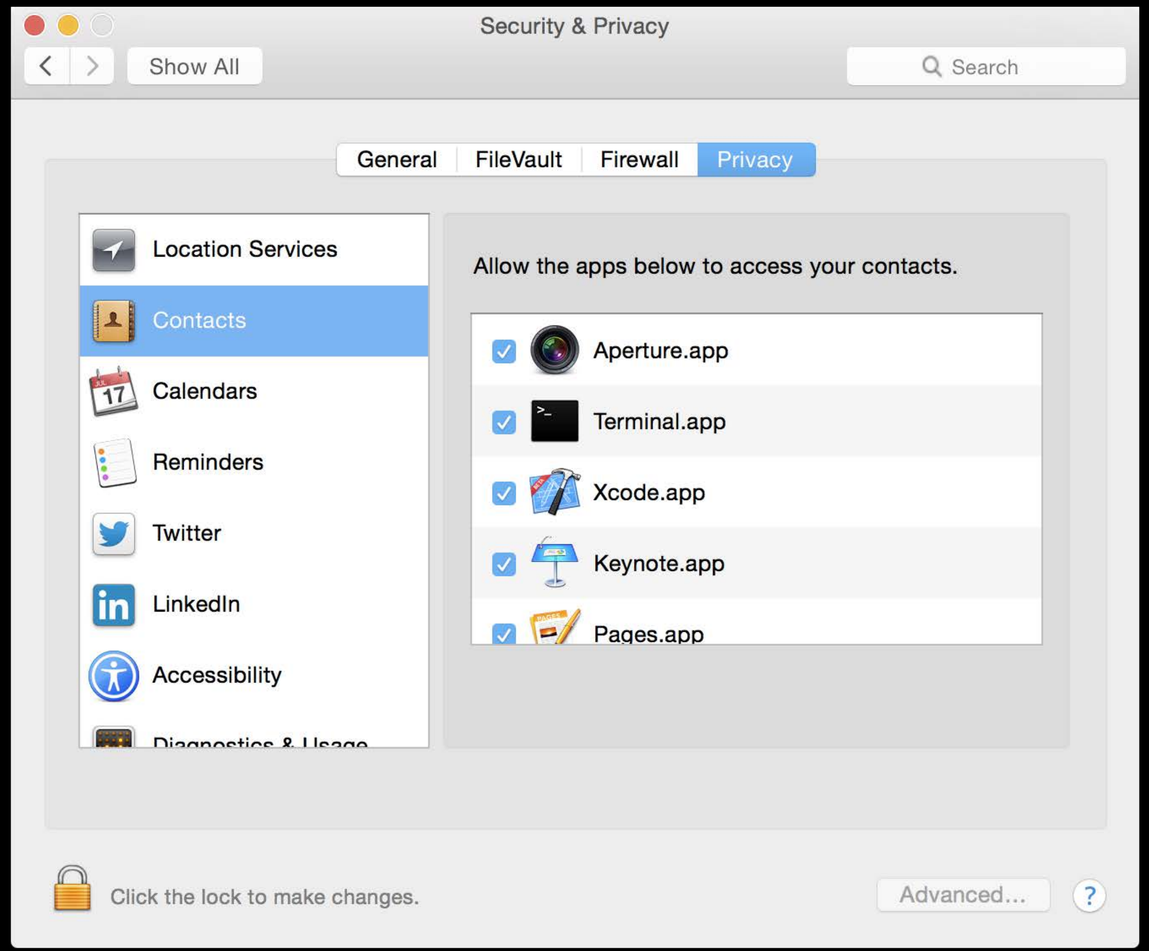
New Purpose String Keys

Data Class	Info.plist Key
Location (iOS)	`NSLocationAlwaysUsageDescription` `NSLocationWhenInUseUsageDescription`
Camera	`NSCameraUsageDescription`
Health Kit	`NSHealthKitUsageDescription`
Motion Activity (available in iOS 7)	`NSMotionActivityUsageDescription`

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

Privacy Settings





Directing Users to Settings

Users may want to update their privacy settings

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

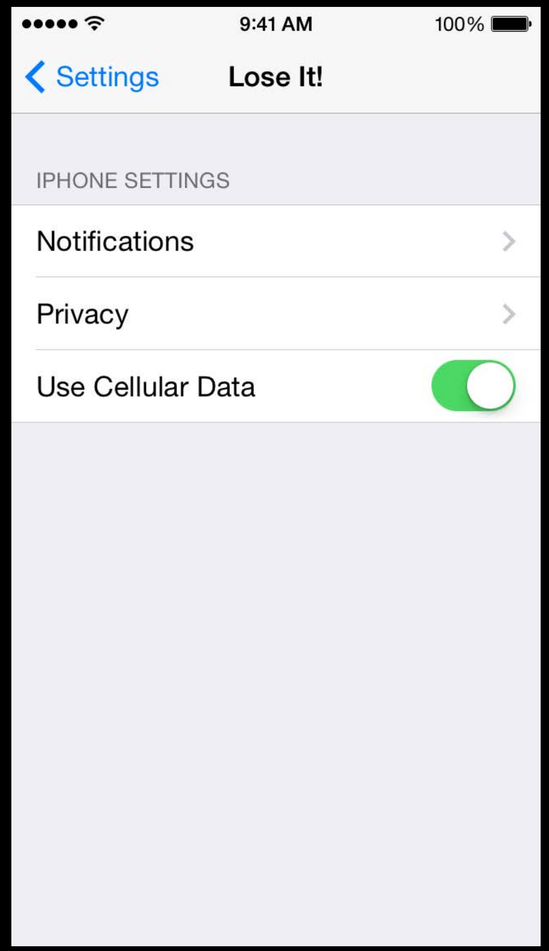
Directing Users to Settings

Users may want to update their privacy settings

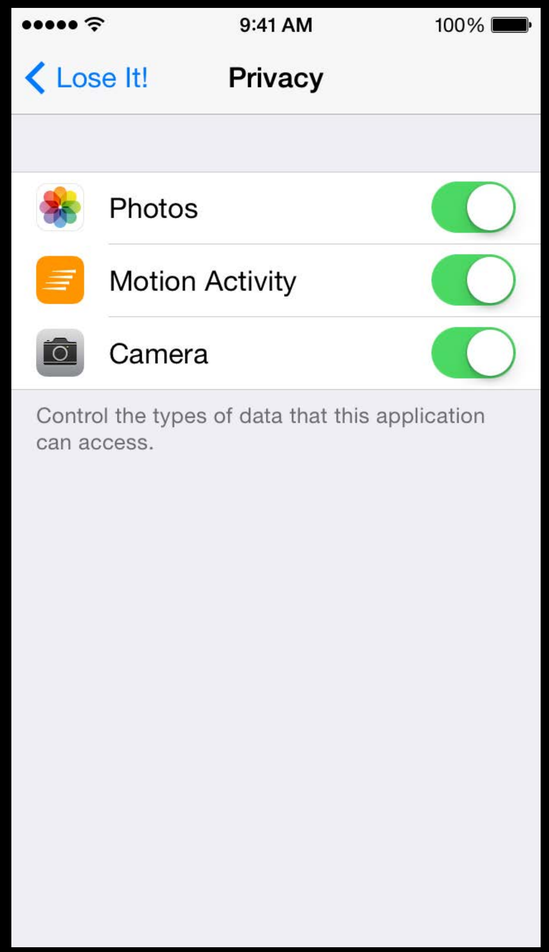
New in iOS 8, your app can direct users directly to settings

```
[[UIApplication sharedApplication] openURL:[NSURL
URLWithString:UIApplicationOpenSettingsURLString]];
```

Your App's Privacy Settings



Your App's Privacy Settings



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

Category	Category
Location	Updated
Contacts	Updated
Calendars	
Reminders	
Photos	
Bluetooth	
Microphone	
Camera (worldwide)	Updated
Motion Activity	Updated
Health Kit	New
Social (Facebook, Twitter, etc.)	

Current Support on OS X

Data Class	Status
Location	
Contacts	
Calendars	
Reminders	
Social (Facebook, Twitter, etc.)	

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

OS X

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

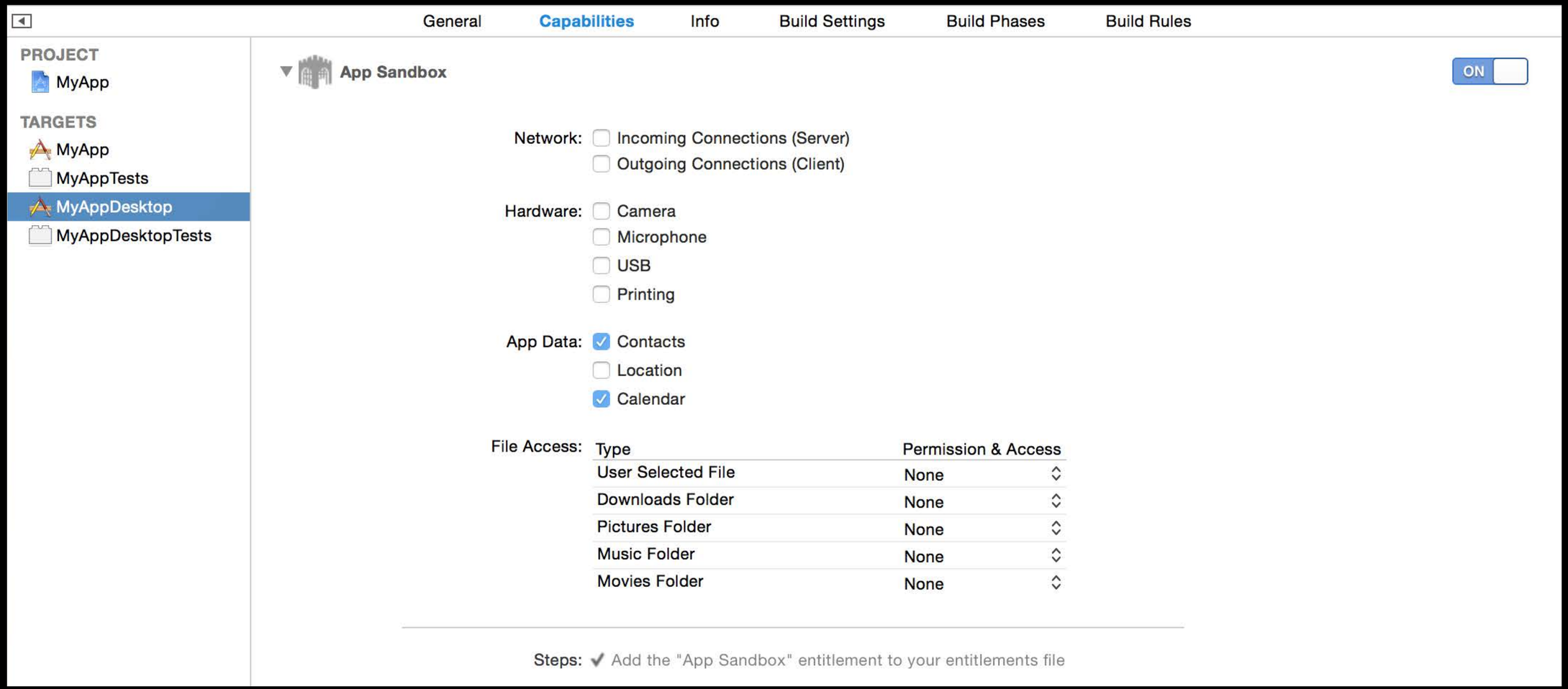
Build with only the entitlements your app needs

Related Session

A Practical Guide to the App Sandbox	WWDC 2012

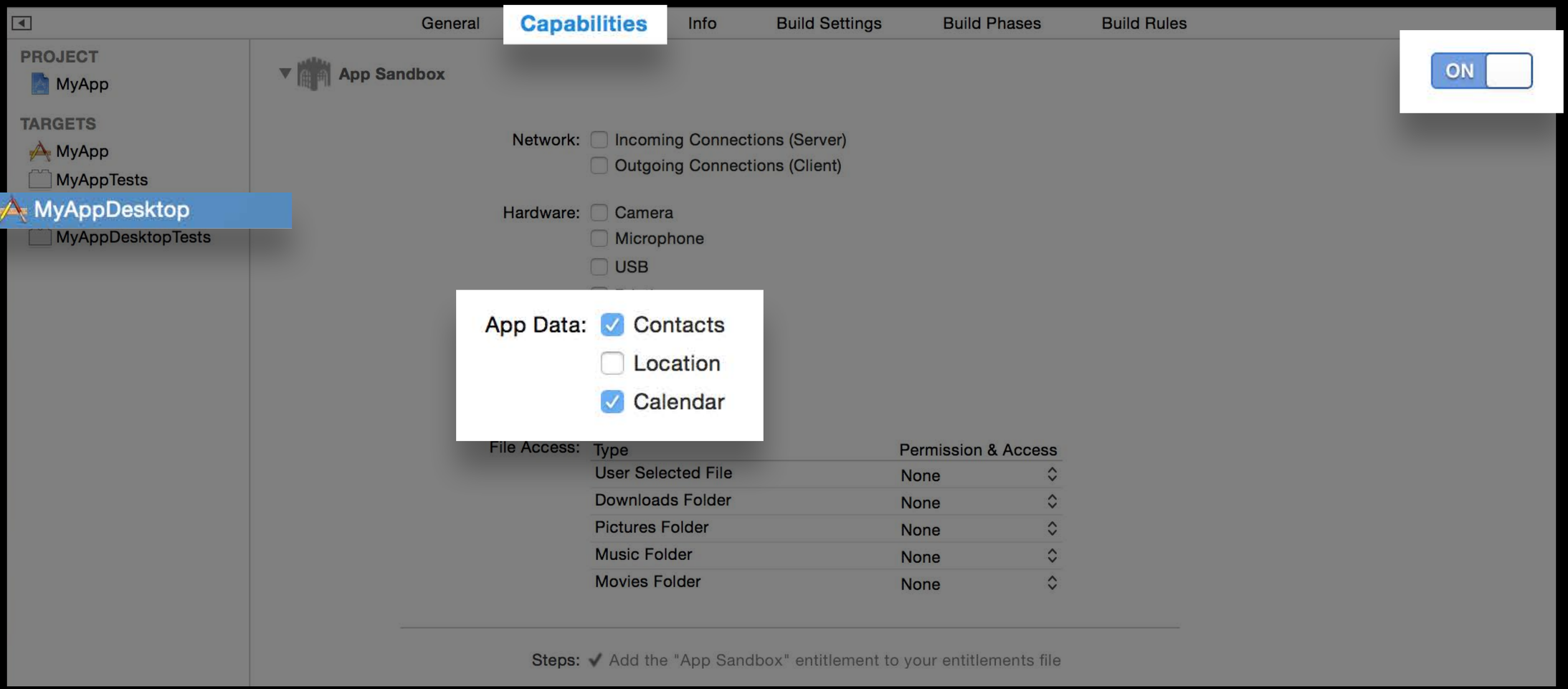
OS X

App Sandbox in Xcode



OS X

App Sandbox in Xcode



Data Isolation on iOS

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

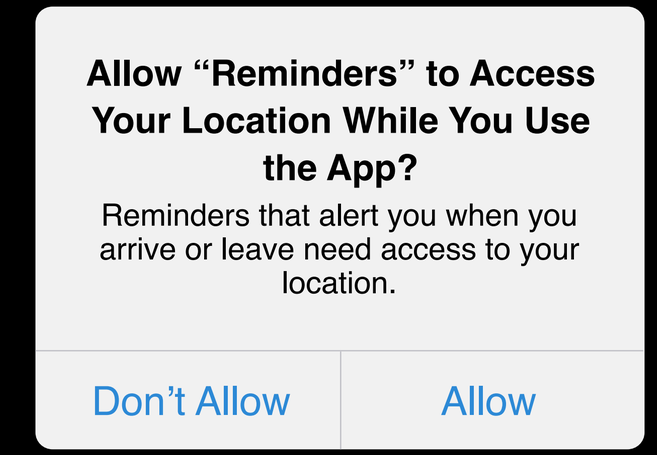
Data Type	System Authorization Support
Location	`-[CLLocationManager requestAlwaysAuthorization]` `-[CLLocationManager requestWhenInUseAuthorization]`
Photos	`-[[PhotoKit alloc] init]`
Camera	`-[AVCaptureDeviceInput deviceInputWithDevice:error:]`
Health Kit	`-[HKHealthStore authorizationStatusForDataType:]` `-[HKHealthStore requestAuthorizationToShareTypes:readTypes:completion:]`

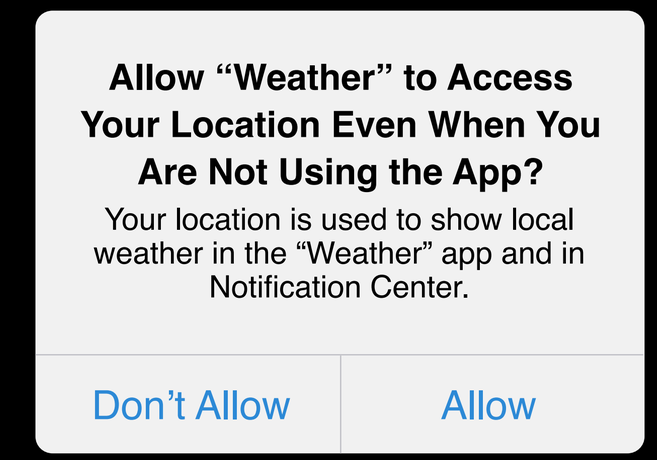
Location Services in iOS 8

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





Location Services in iOS 8

“When In Use” Authorization

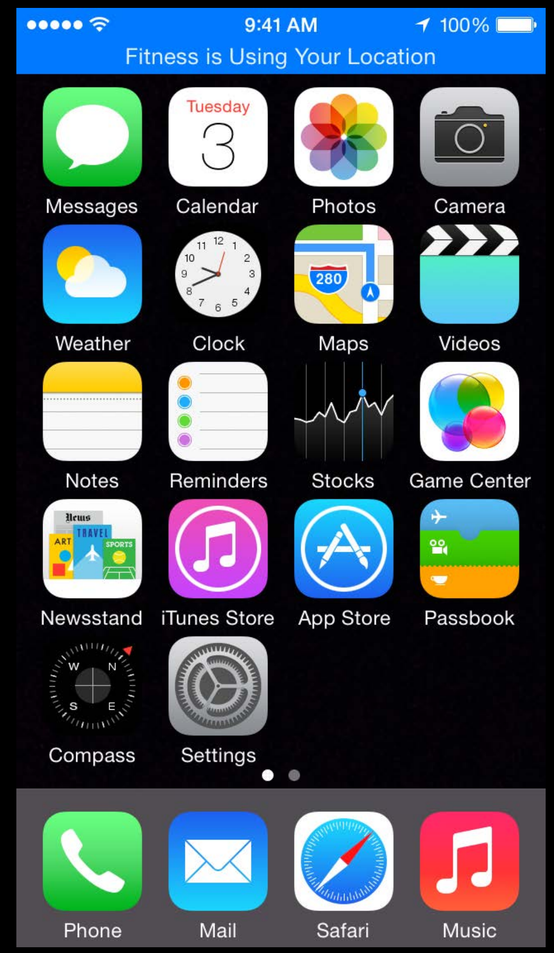
```
-[CLLocationManager
 requestWhenInUseAuthorization]
NSLocationWhenInUseUsageDescription
```

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

```
-[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
```

Location Services in iOS 8

```
CLLocationManager *manager = [CLLocationManager sharedManager];
[manager startUpdatingLocation];
```

Location Services in iOS 8

```
CLLocationManager *manager = [CLLocationManager sharedManager];
if ([manager respondsToSelector:@selector(requestWhenInUseAuthorization)]) {
    [manager startUpdatingLocation];
} else {
    [manager requestWhenInUseAuthorization];
}
```

Location Services in iOS 8

```
CLLocationManager *manager = [CLLocationManager sharedManager];
if ([manager respondsToSelector:@selector(requestWhenInUseAuthorization)]) {
    [manager startUpdatingLocation];
} else {
    [manager requestAlwaysAuthorization];
}
```

Location Services in iOS 8

	iOS 7	When In Use	Always
Triggers user consent dialog	●	●	●
Access to region monitoring, SLC & Visits API	●		●
Can start accessing device location in the background	●		●
iOS presents double height status bar		●	
App receives authorization status callbacks	●	●	●

Related Session

• What’s New in Core Location	Marina	Tuesday 2:00PM

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
}
```

Health Kit

Reading data

```
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

```
[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

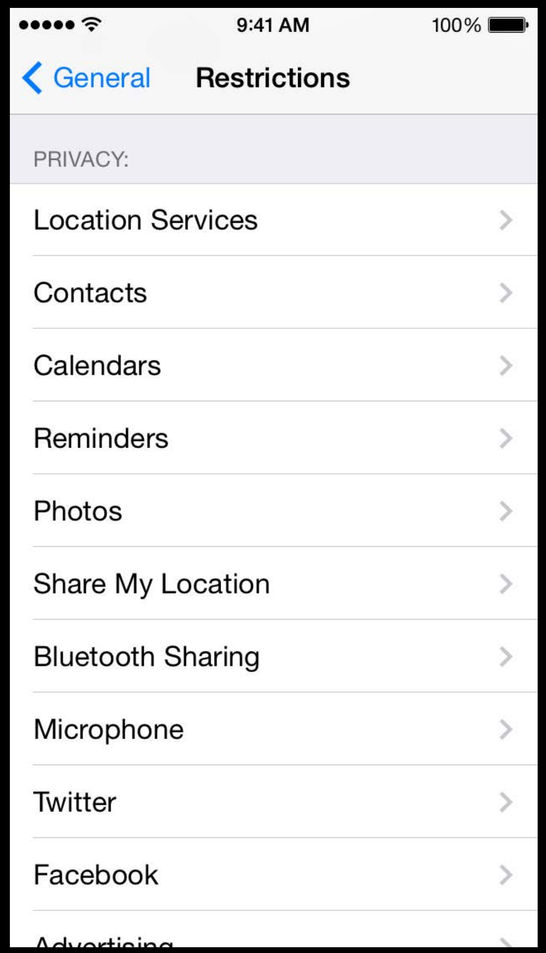
Code should be resilient to lack of data returned

Send users to Settings

Restrictions can prevent users from changing privacy settings

- Enterprise and on-device restrictions

Restrictions



Restrictions

iOS Sample Code

Available on the iOS Developer Library today

“Checking and Requesting Access to Data Classes in Privacy Settings” project

https://developer.apple.com/library/ios/samplecode/PrivacyPrompts/

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

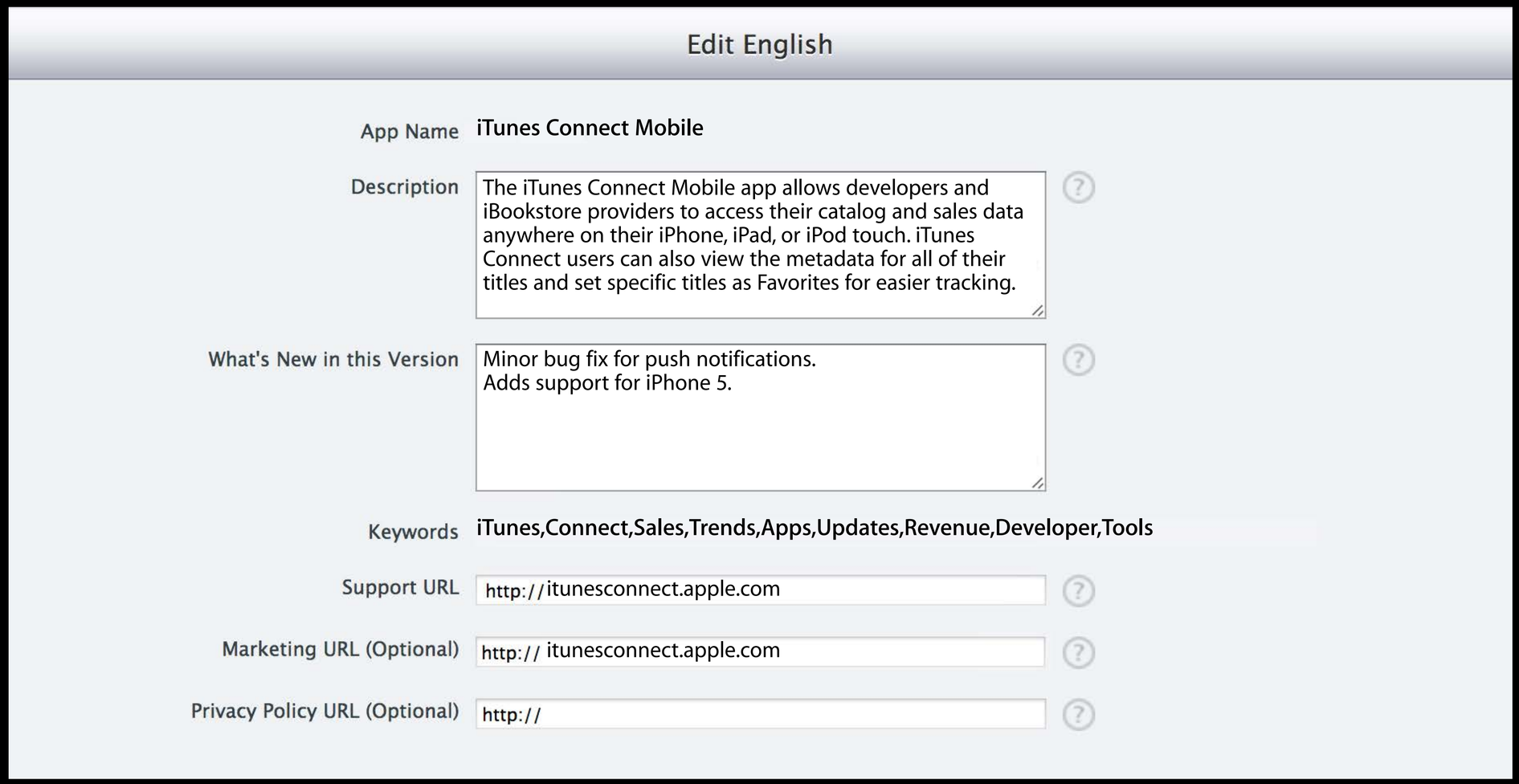
- Apps that link against HealthKit
- Apps that link against HomeKit
- Third party keyboards
- Kids

Can submit a link to Apple in iTunes Connect

Link visible on the App Store

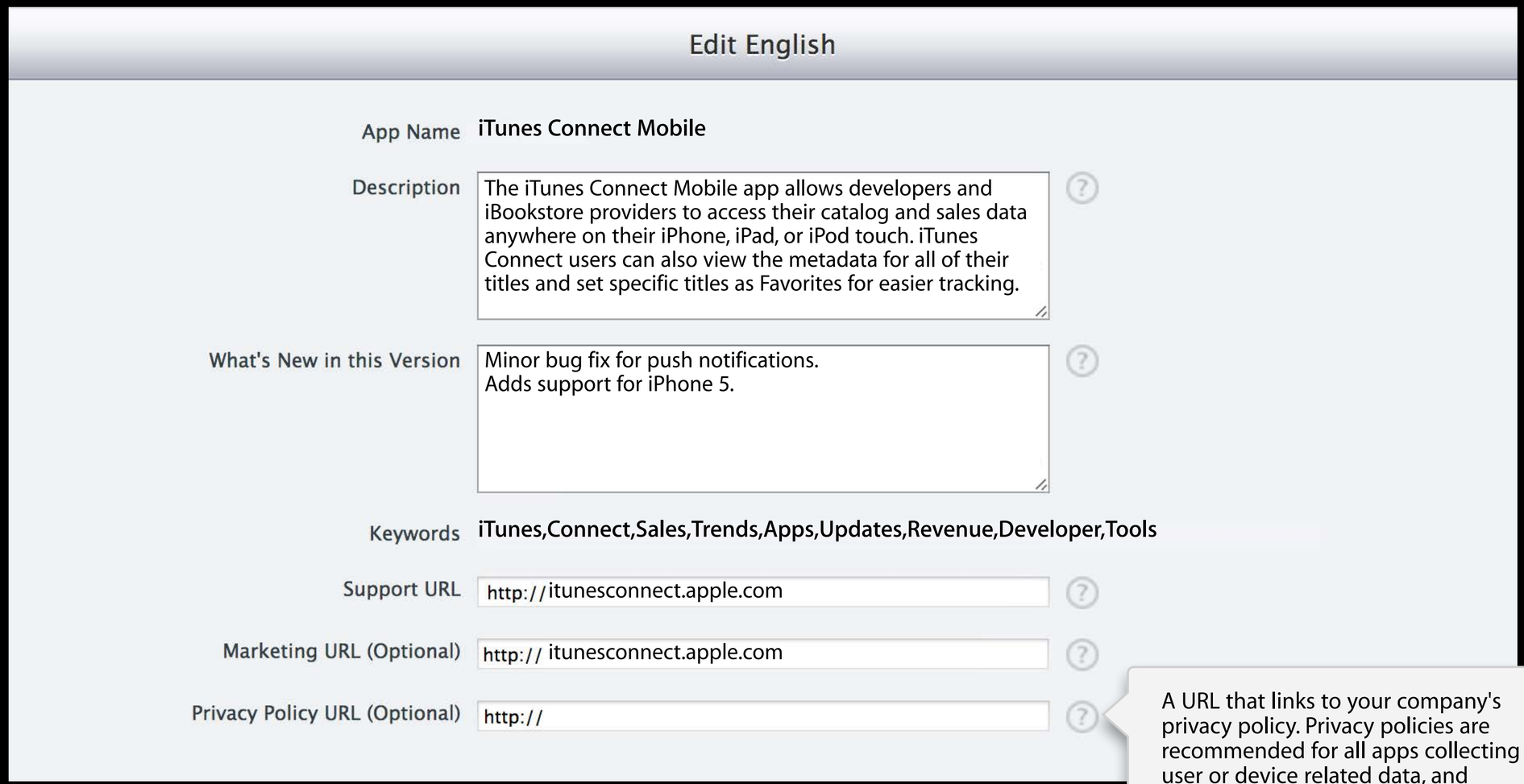
Privacy Policy

iTunes Connect



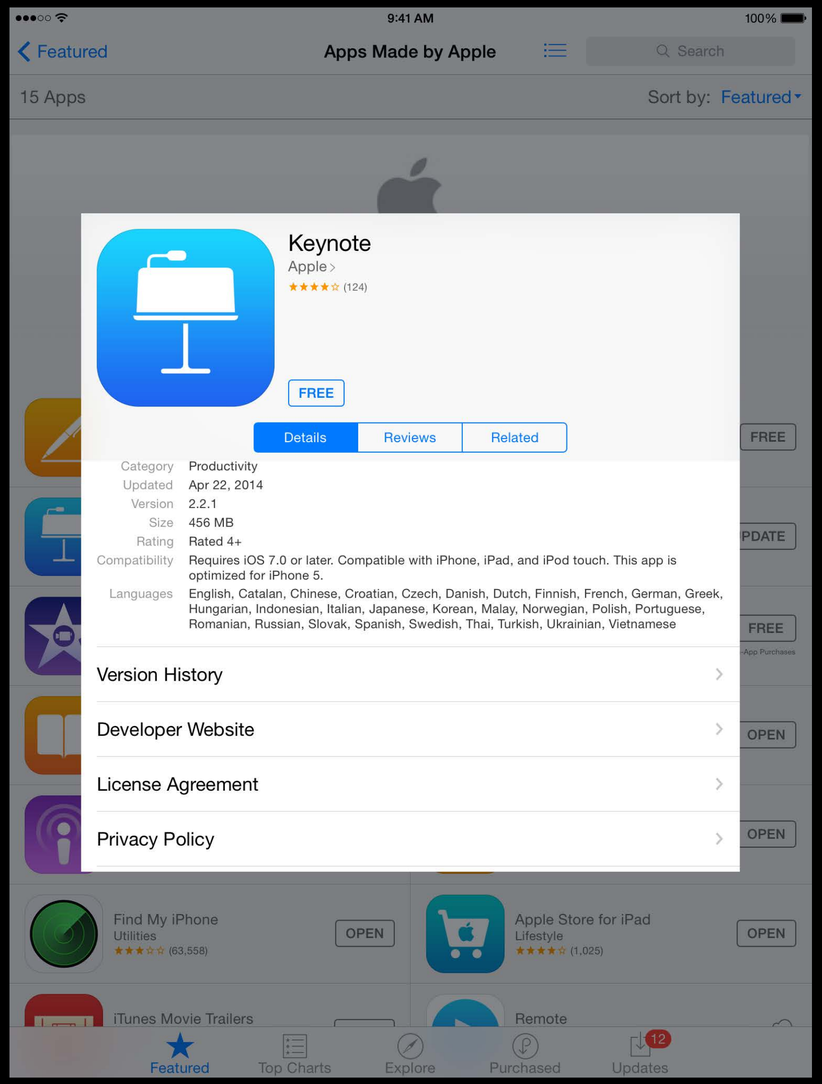
Privacy Policy

iTunes Connect



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

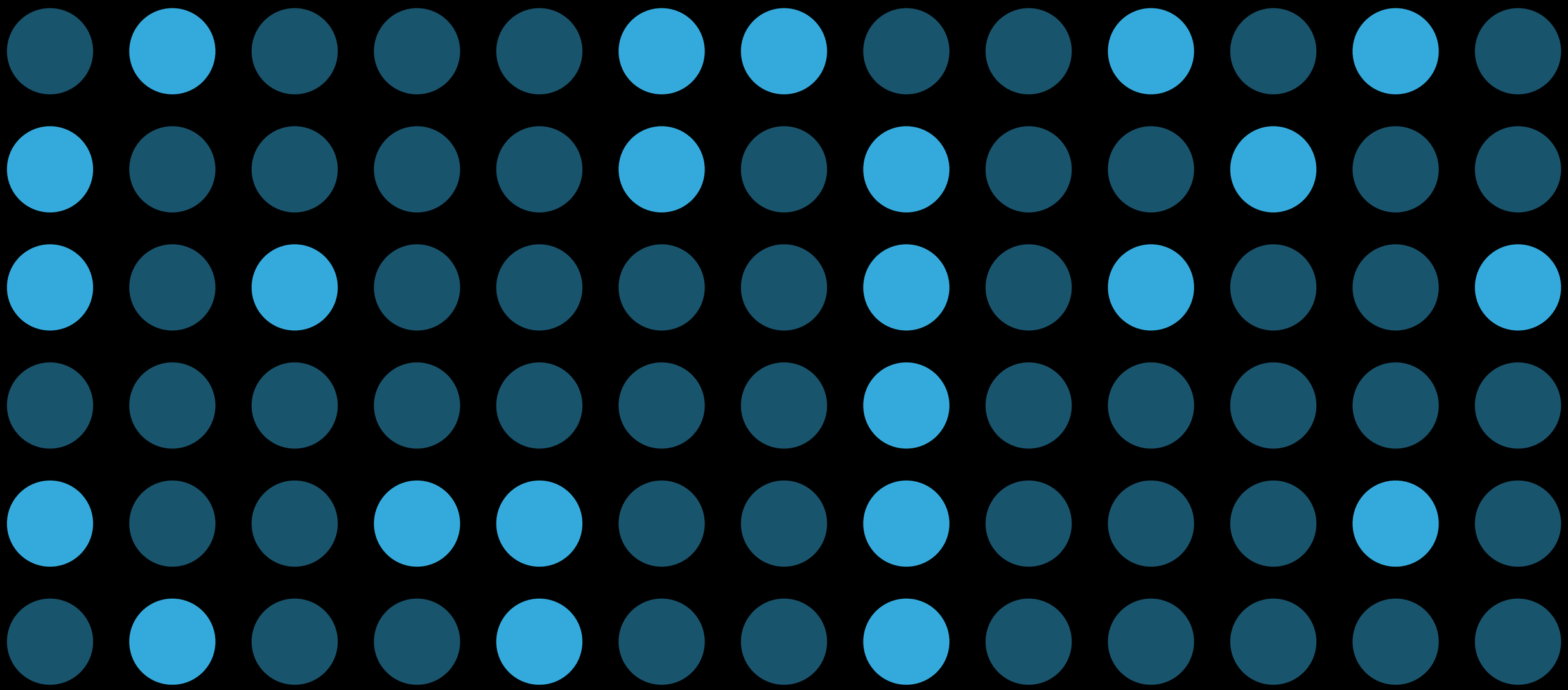
Initial user population

OS X Yosemite installed

Screen resolution 1920x1280

PST timezone

Java installed



Cookies enabled

Flash 11.8.800.128

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
https://developer.apple.com/library/ios/samplecode/PrivacyPrompts/

People Picker
https://developer.apple.com/library/ios/people_picker_sample

More Information

Documentation
Best Practices for Maintaining User Privacy
https://developer.apple.com/library/ios/documentation/iphone/conceptual/iphoneosprogrammingguide/AppDesignBasics/AppDesignBasics.html

Apple Developer Forums
http://devforums.apple.com

Related Sessions

• Kids and Apps	Nob Hill	Thursday 3:15PM
• What's New in Core Location	Marina	Tuesday 2:00PM
• Keychain and Authentication with Touch ID	Nob Hill	Wednesday 10:15AM
Protecting Your User's Privacy		WWDC 2013
Protecting User's Data		WWDC 2013
A Practical Guide to the App Sandbox		WWDC 2012

Labs

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

WWDC14