

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

```
[NSUserDefaults standardUserDefaults] objectForKey:@"kApplicationIdentifier"]
```

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]
```

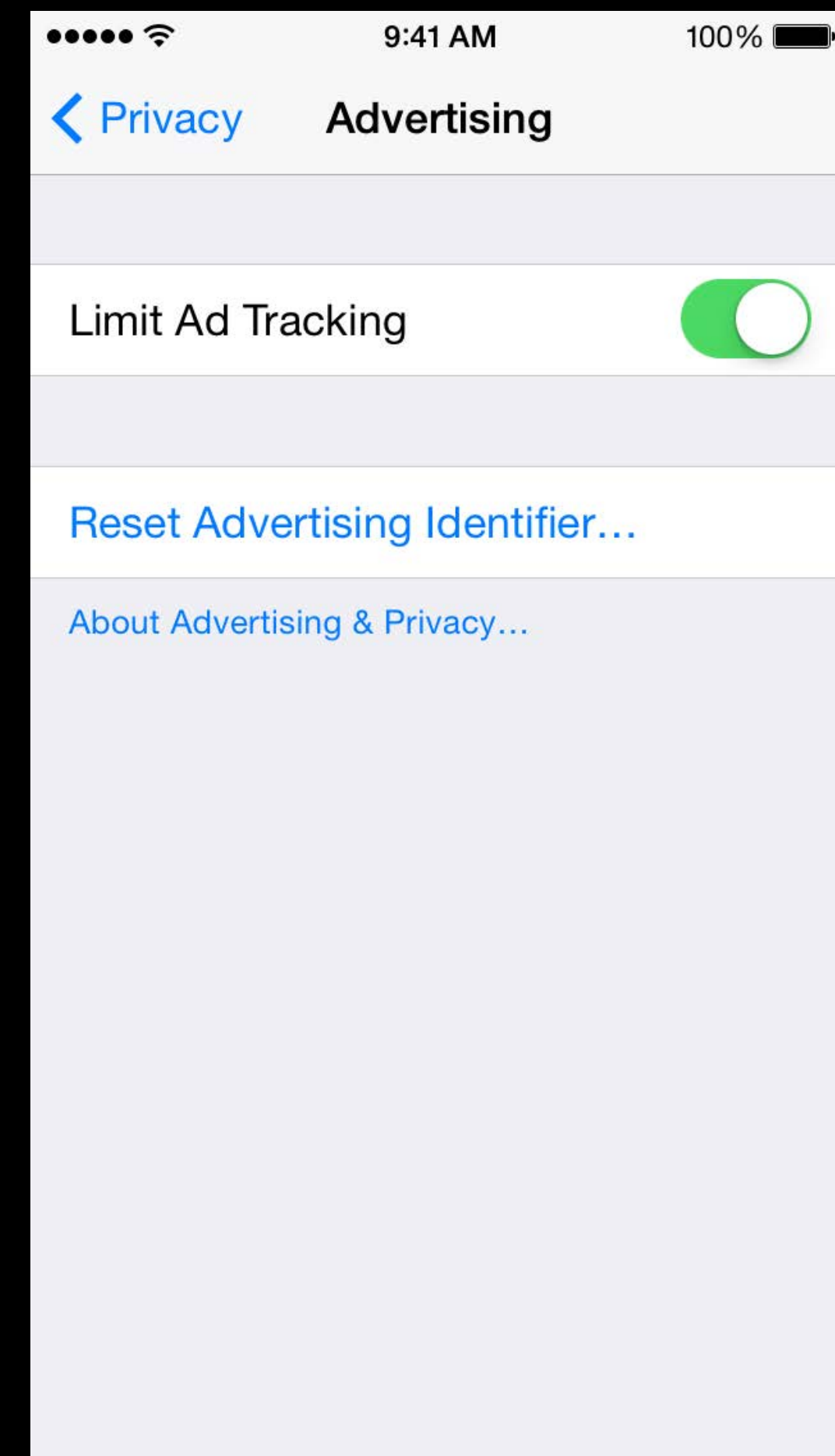
Required to check the value of this property before using Advertising Identifier

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

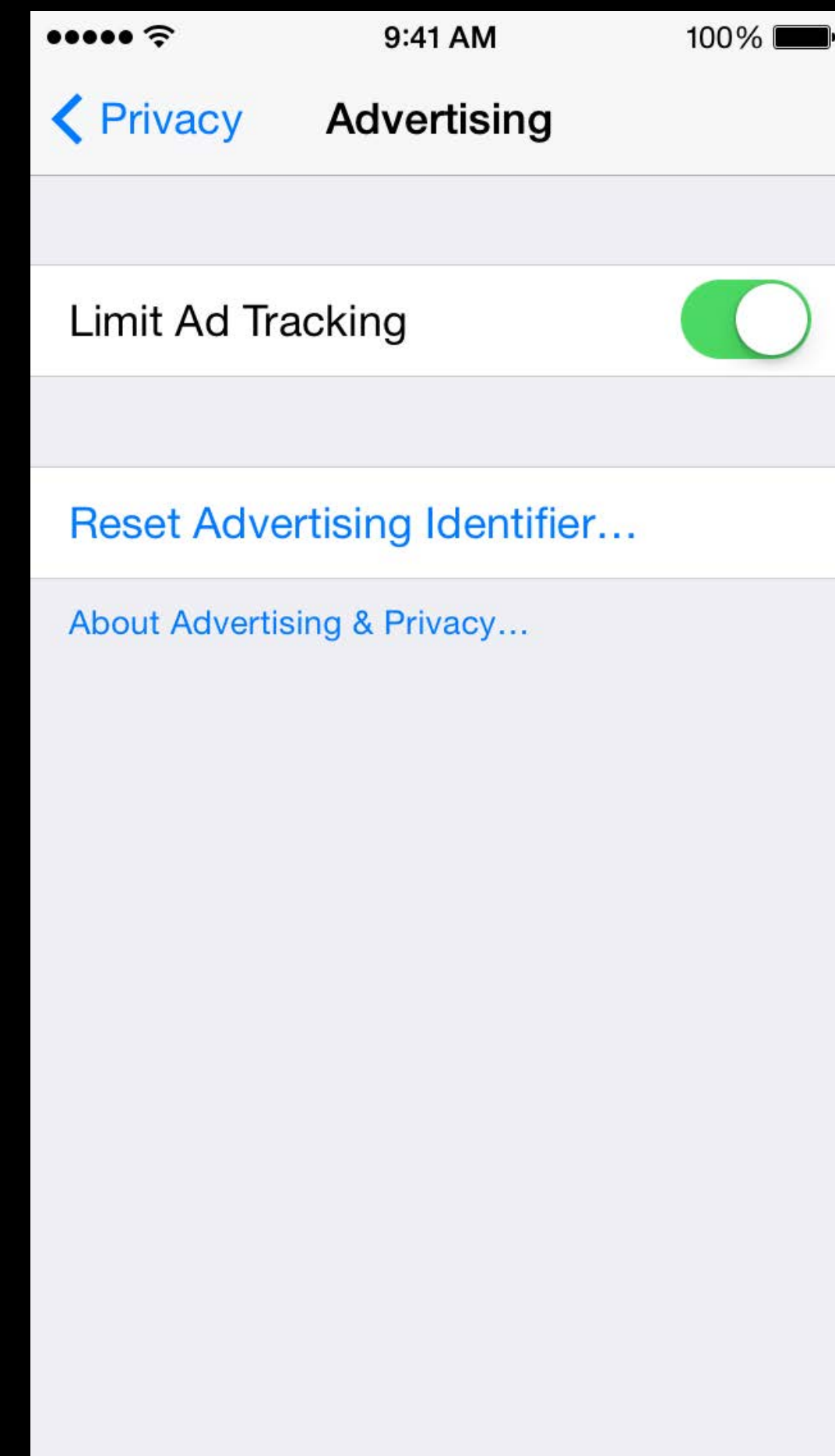


Advertising Identifier

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

Apple iTunes Connect jappleseed ▾

iTunes Connect

Export Compliance

Have you added or made changes to encryption features since your last submission of this app? Yes
 No

Export laws require that products containing encryption must be properly authorized for export. Failure to comply could result in severe penalties. [Learn more about export requirements.](#)

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

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](#).

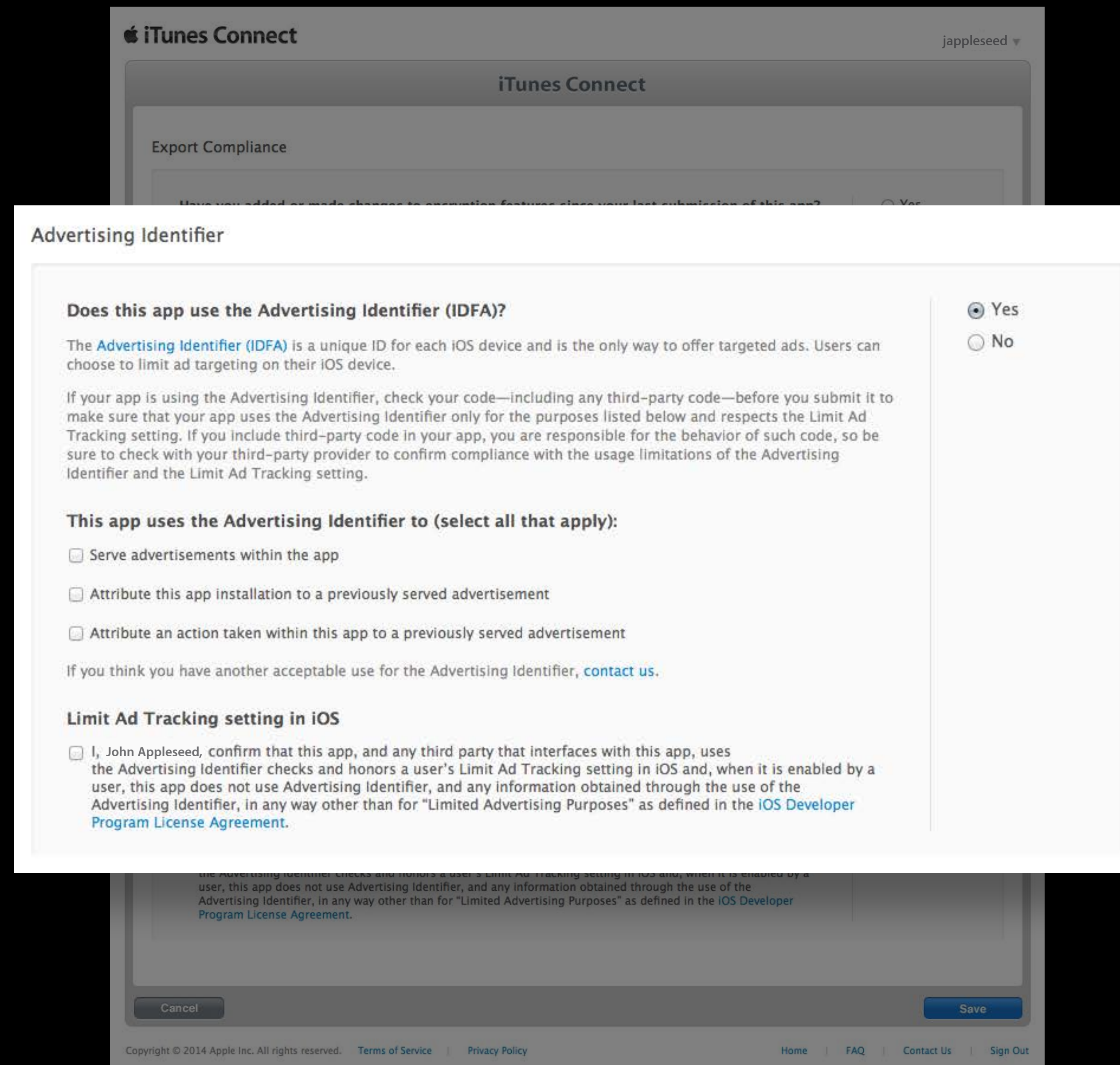
Limit Ad Tracking setting in iOS

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](#).

Cancel Save

Copyright © 2014 Apple Inc. All rights reserved. [Terms of Service](#) | [Privacy Policy](#) [Home](#) | [FAQ](#) | [Contact Us](#) | [Sign Out](#)

iTunes Connect and Advertising Identifier



The image shows a screenshot of the iTunes Connect interface. At the top, the 'iTunes Connect' logo is visible on the left, and the user's name 'jappleseed' is on the right. Below the logo, there's a navigation bar with 'Export Compliance' and a question: 'Have you added or made changes to optional features since your last submission of this app?' with a 'Yes' button. The main content area is titled 'Advertising Identifier' and contains the following sections:

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](#).

On the right side of the form, there are two radio buttons: 'Yes' (which is selected) and 'No'.

At the bottom of the form, there are 'Cancel' and 'Save' buttons. Below the form, the footer contains: 'Copyright © 2014 Apple Inc. All rights reserved. Terms of Service Privacy Policy Home FAQ Contact Us Sign Out'.

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

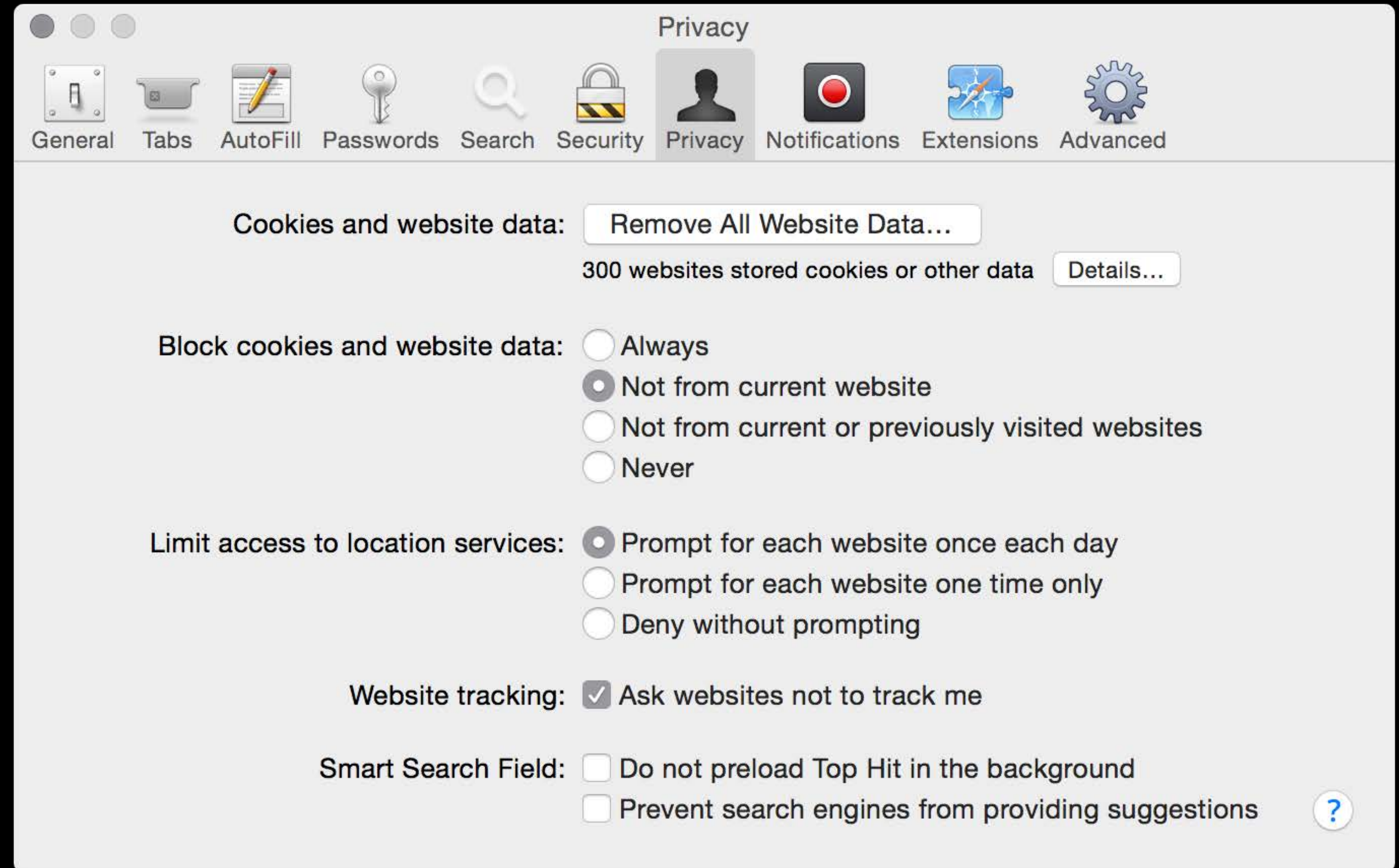
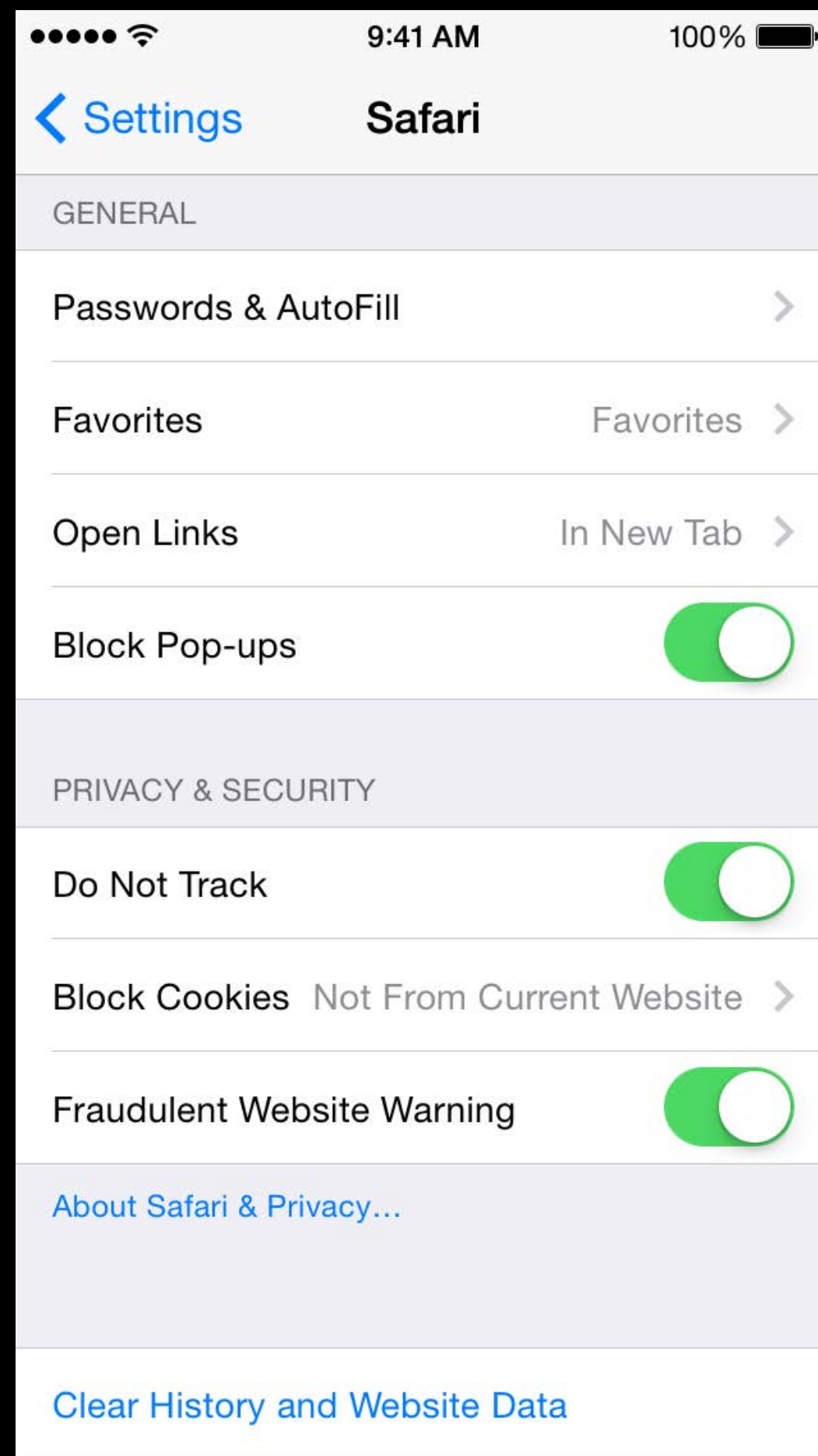


New setting to block all third party cookies, regardless of whether the user has visited a site previously

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

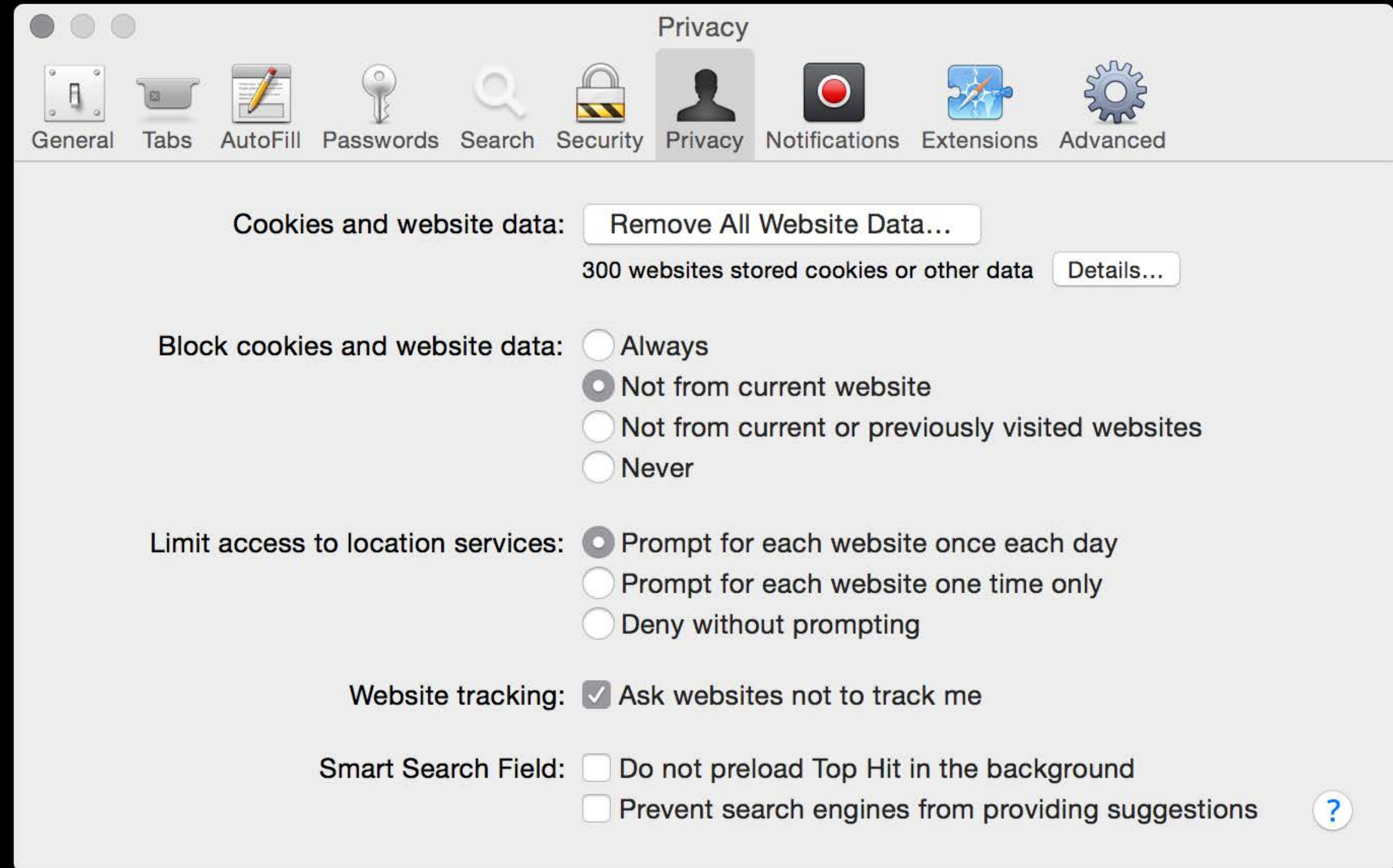
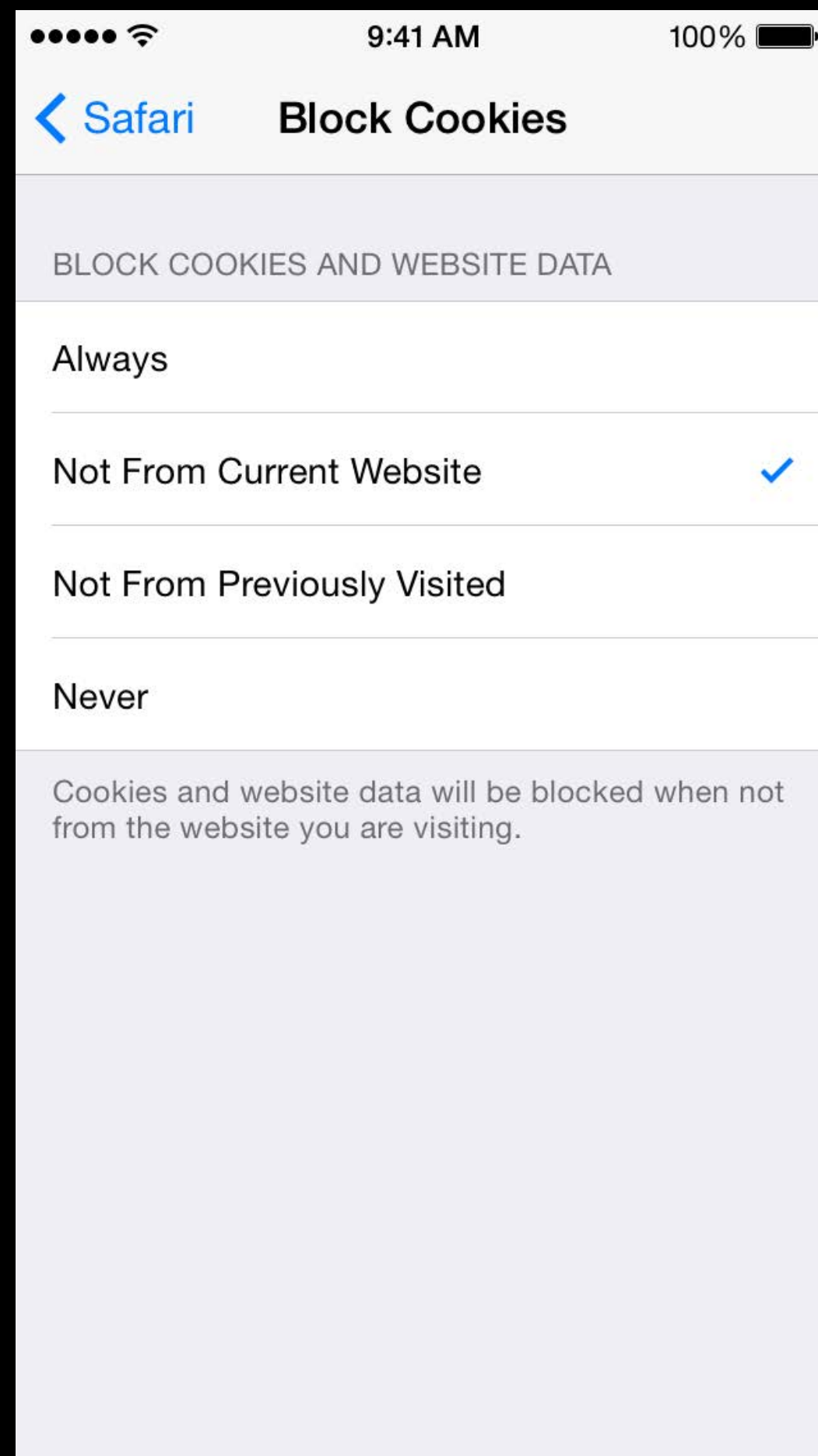
Safari Third Party Cookie Policy

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

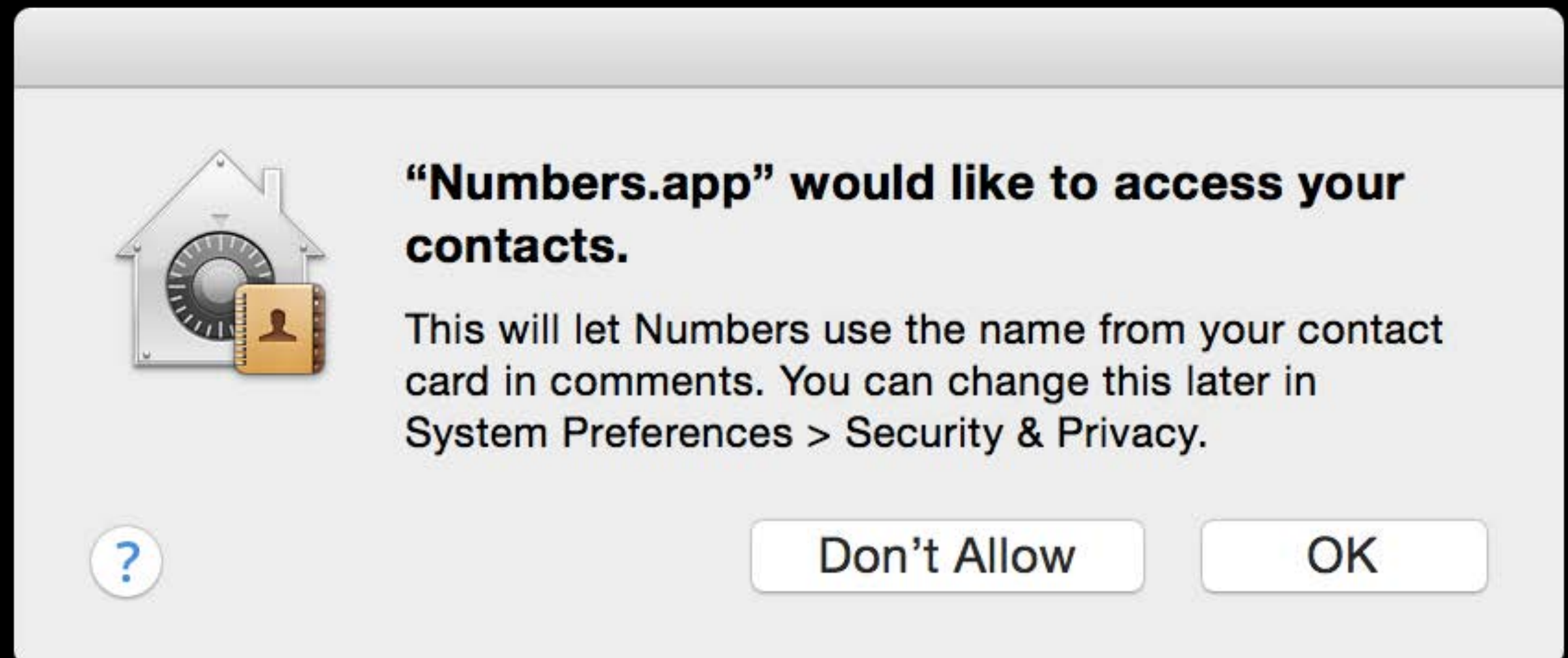
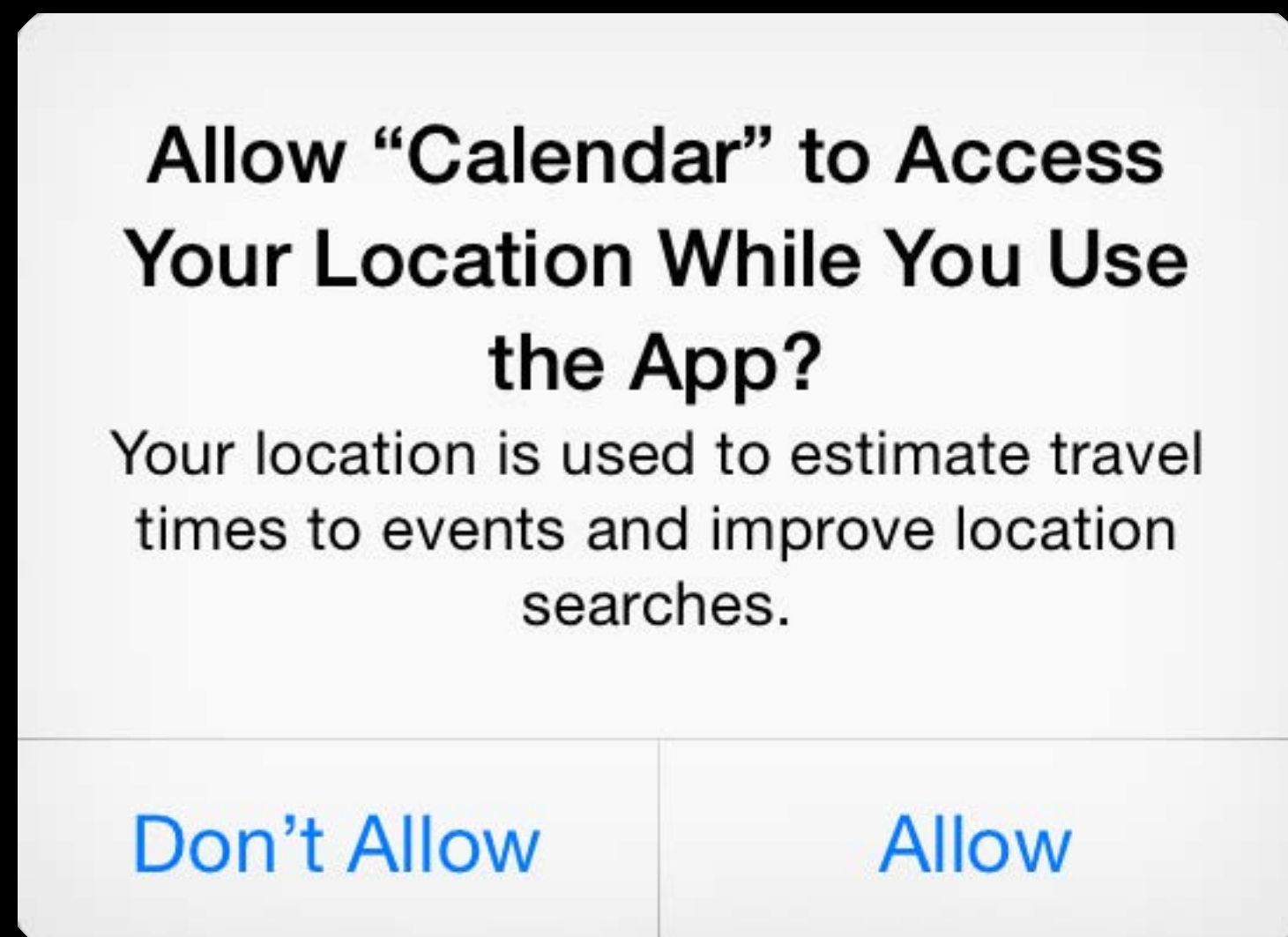
Design the experience

Five core principles for “prompting with purpose”

- Consent
- Transparency
- Context
- Clarity
- Minimization

Prompting with Purpose

Consent



Prompting with Purpose

Consent

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.

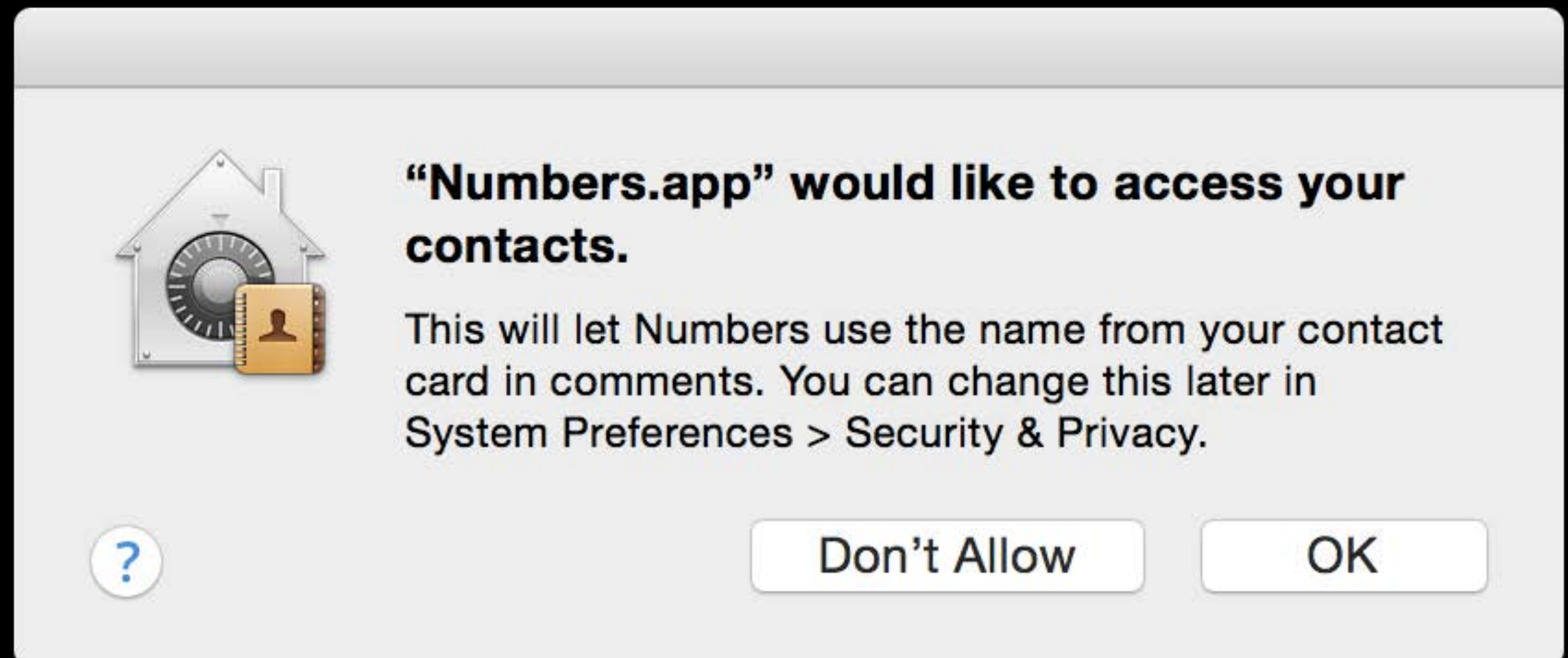
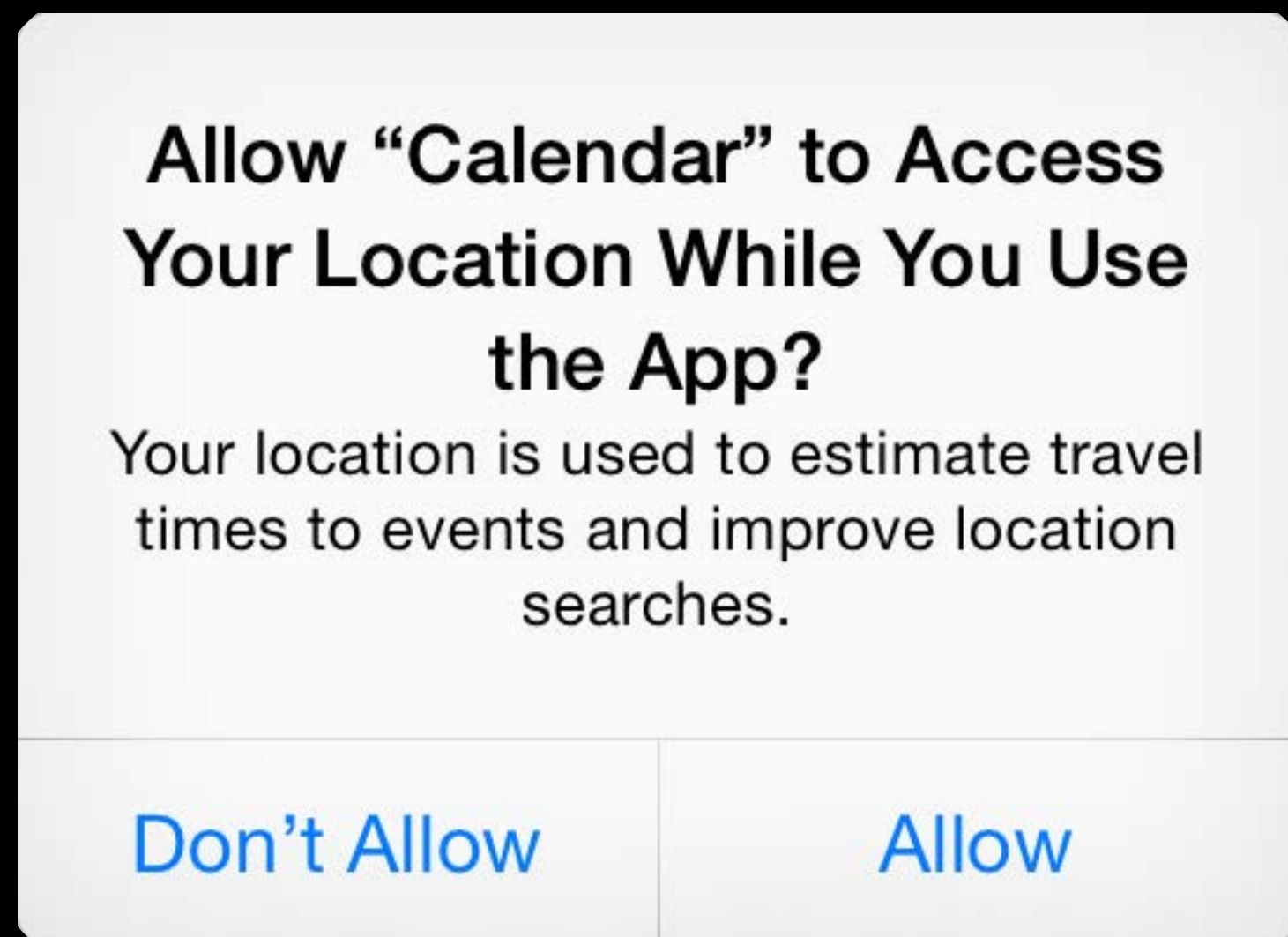


Don't Allow

OK

Prompting with Purpose

Transparency



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.



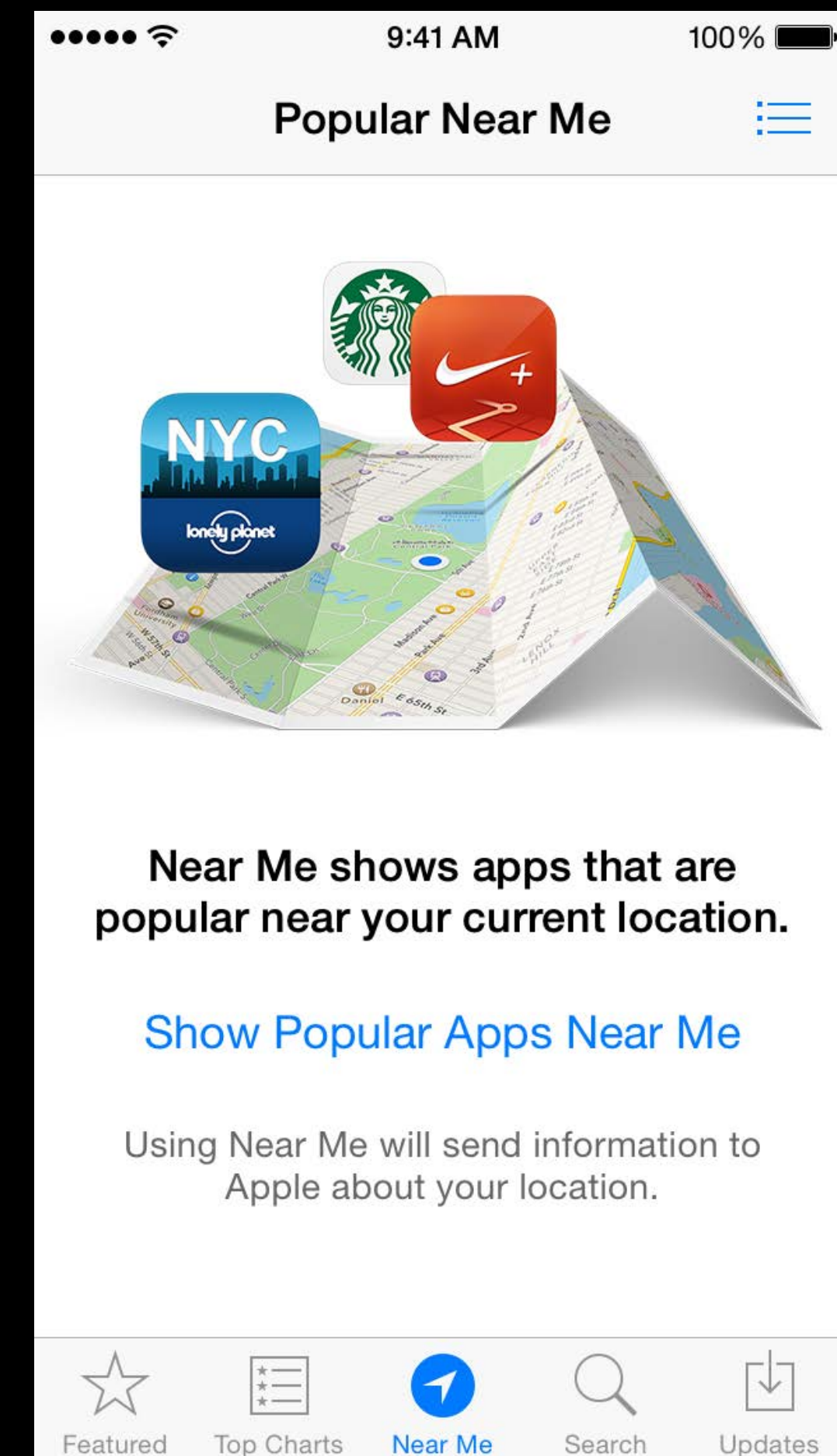
Don't Allow

OK

Prompting with Purpose

Context

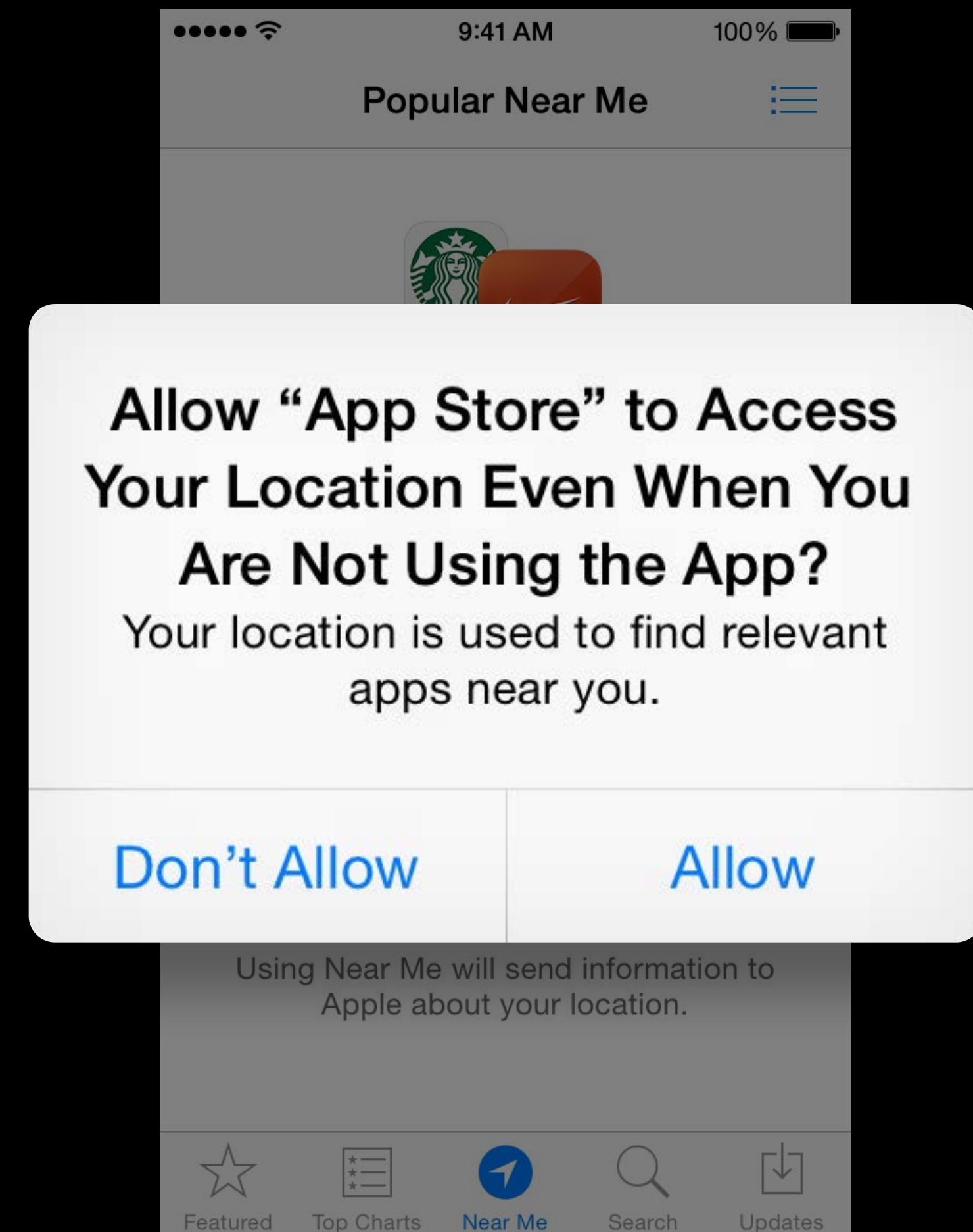
Tie prompting to a user-initiated action



Prompting with Purpose

Context

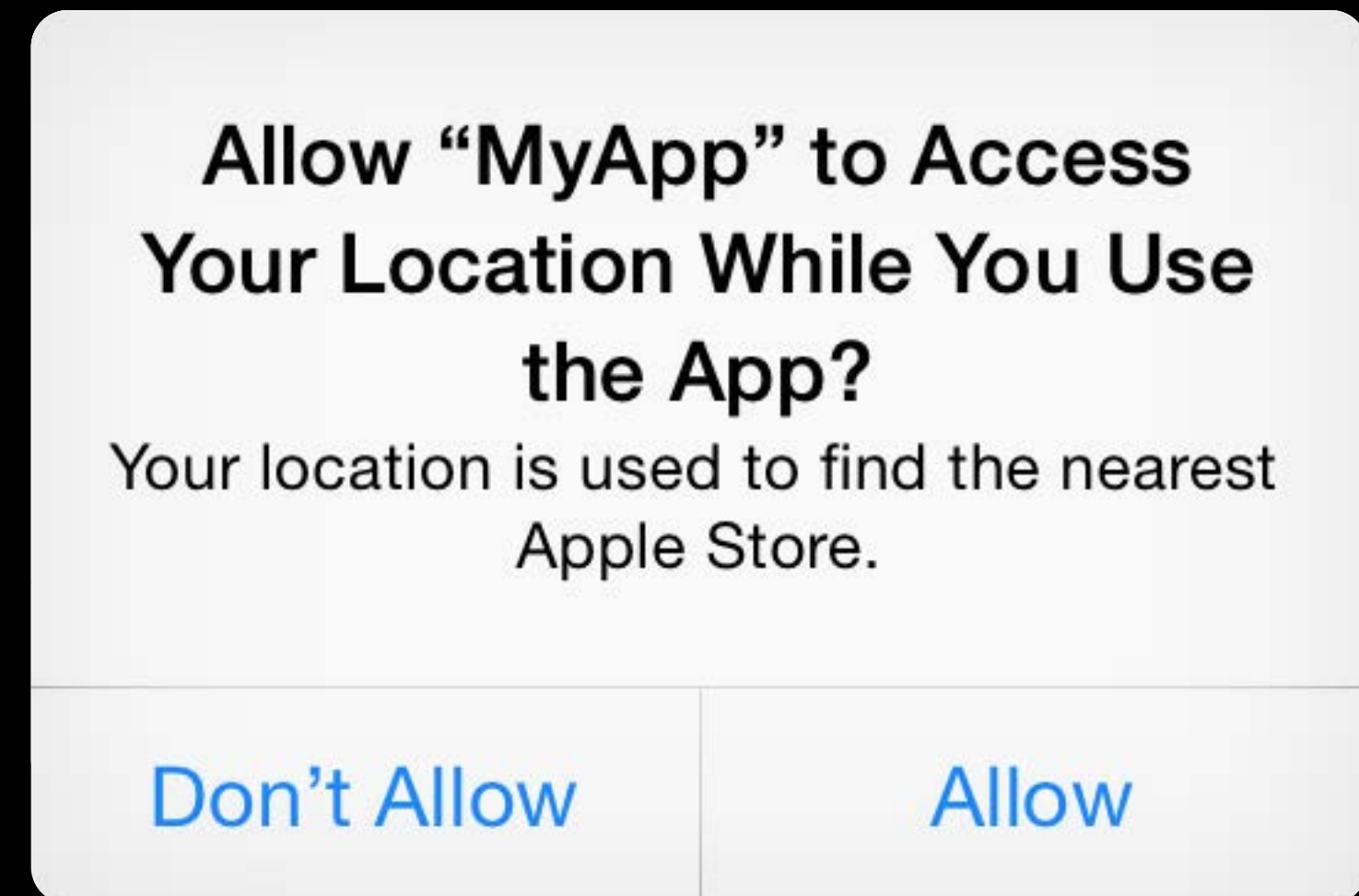
Tie prompting to a user-initiated action



Prompting with Purpose

Context

Tie prompting to a user-initiated action

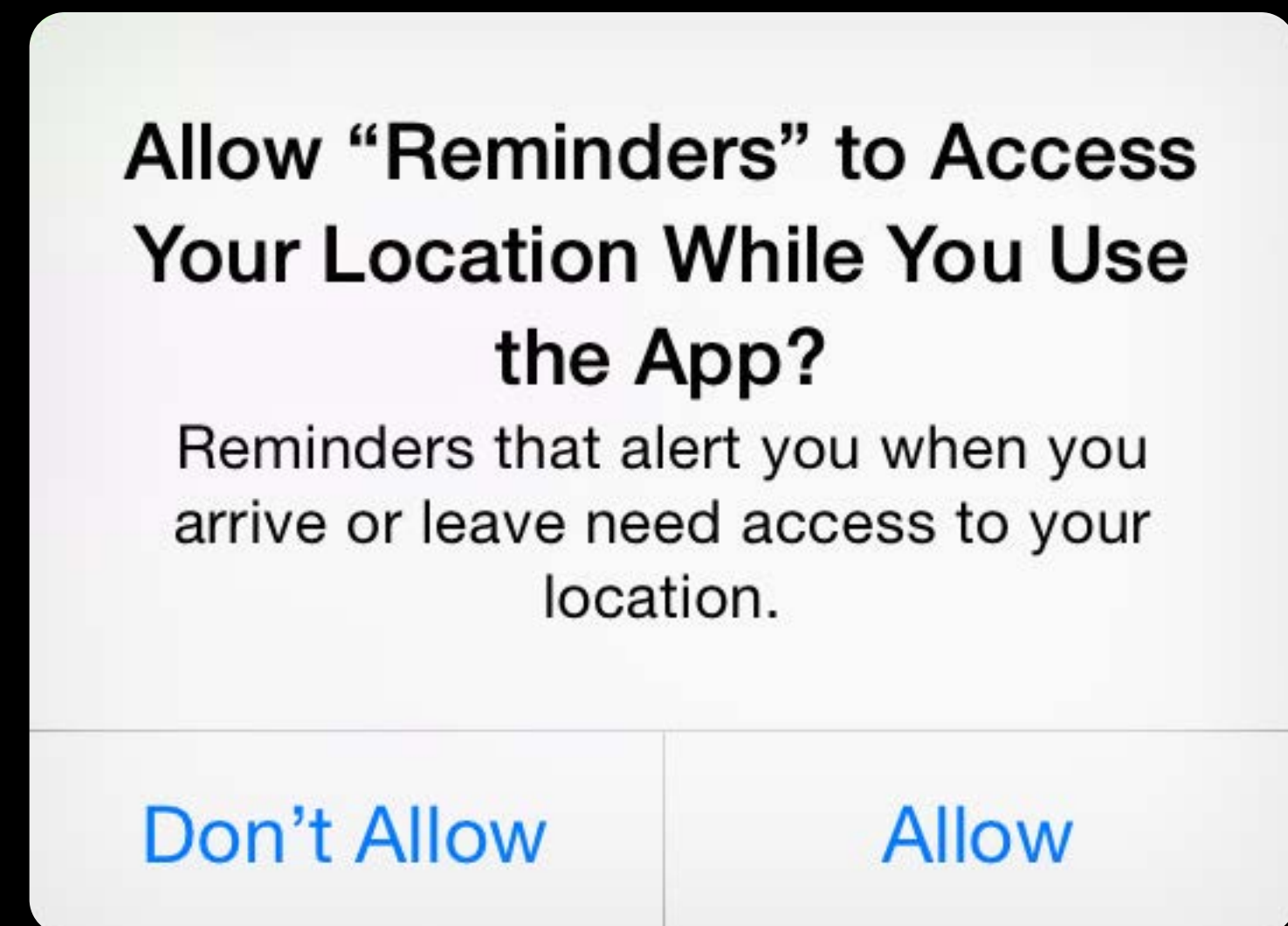


Prompting with Purpose

Clarity

Distill the purpose of your request down to its essence

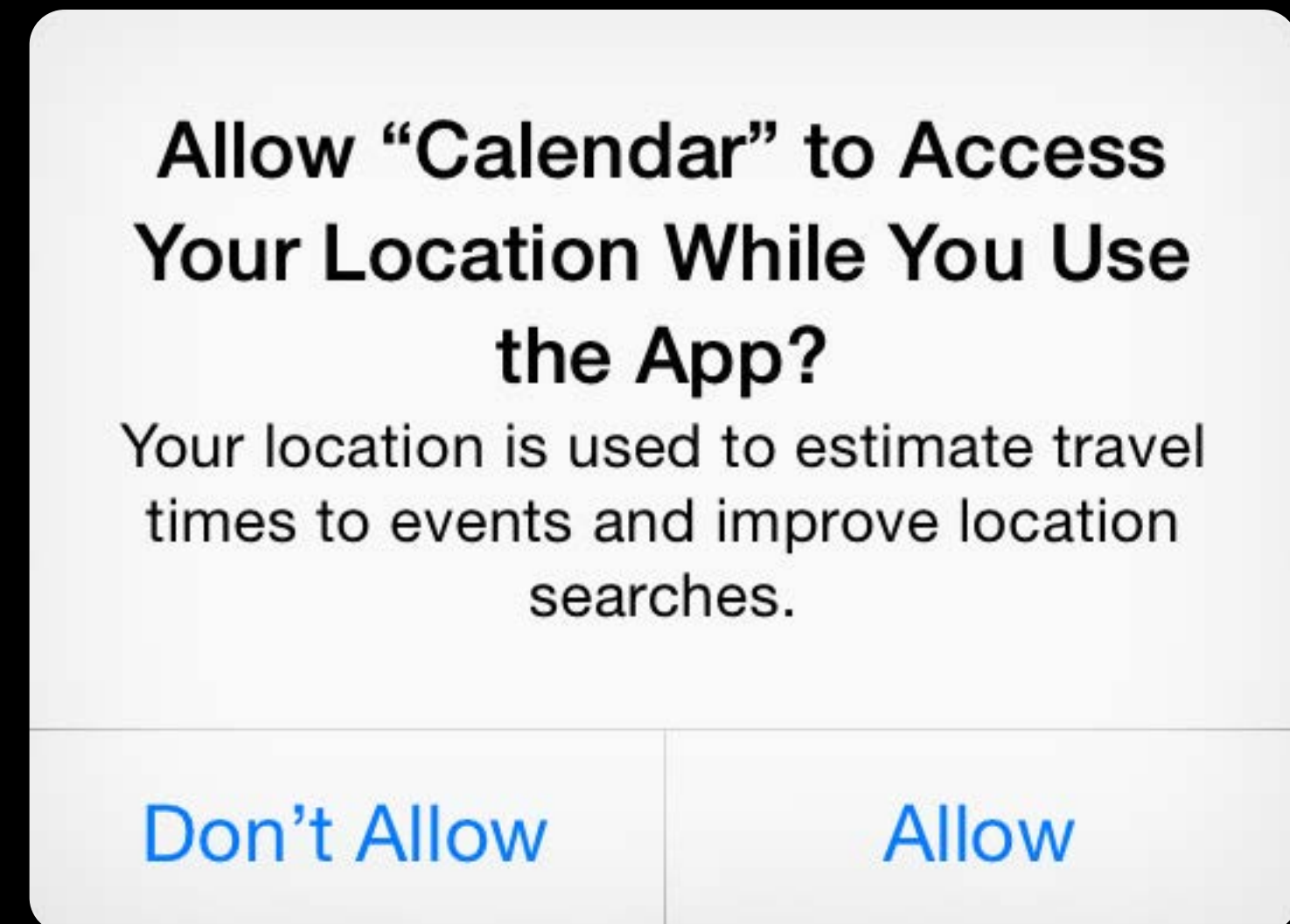
Be concise but include sufficient detail



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

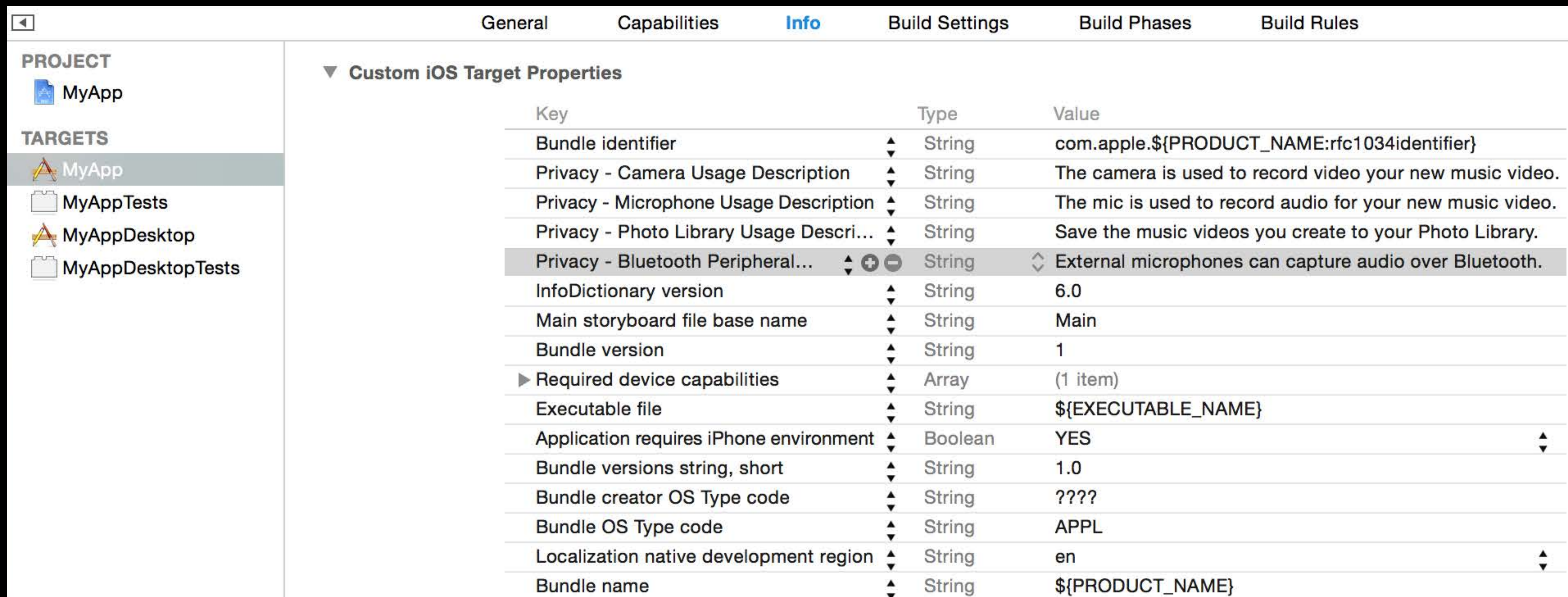
- Add localized versions in Localizable.strings

Look for "Privacy—" keys and provide a value

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

Conveying Purpose

Xcode

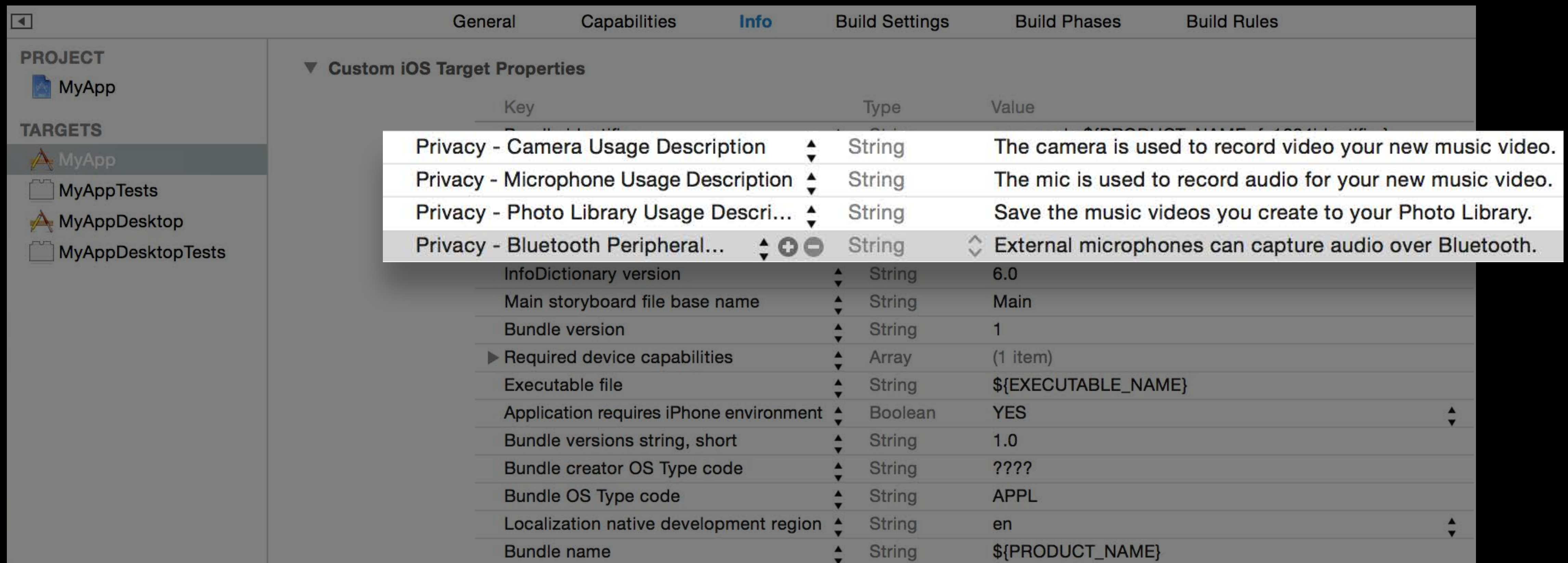


The screenshot shows the Xcode interface with the 'Info' tab selected. The left sidebar shows the project 'MyApp' and its targets: 'MyApp', 'MyAppTests', 'MyAppDesktop', and 'MyAppDesktopTests'. The main area displays 'Custom iOS Target Properties' as a table with columns for Key, Type, and Value.

Key	Type	Value
Bundle identifier	String	com.apple.\${PRODUCT_NAME:rfc1034identifier}
Privacy - Camera Usage Description	String	The camera is used to record video your new music video.
Privacy - Microphone Usage Description	String	The mic is used to record audio for your new music video.
Privacy - Photo Library Usage Descri...	String	Save the music videos you create to your Photo Library.
Privacy - Bluetooth Peripheral...	String	External microphones can capture audio over Bluetooth.
InfoDictionary version	String	6.0
Main storyboard file base name	String	Main
Bundle version	String	1
▶ Required device capabilities	Array	(1 item)
Executable file	String	\${EXECUTABLE_NAME}
Application requires iPhone environment	Boolean	YES
Bundle versions string, short	String	1.0
Bundle creator OS Type code	String	????
Bundle OS Type code	String	APPL
Localization native development region	String	en
Bundle name	String	\${PRODUCT_NAME}

Conveying Purpose

Xcode



The screenshot shows the Xcode interface with the 'Info' tab selected. The 'Custom iOS Target Properties' section is expanded, displaying a table of properties. The table has three columns: 'Key', 'Type', and 'Value'. The 'Privacy - Bluetooth Peripheral Usage Description' property is highlighted, showing its value as 'External microphones can capture audio over Bluetooth.' Other privacy-related properties include 'Camera Usage Description', 'Microphone Usage Description', and 'Photo Library Usage Description', each with a corresponding descriptive value.

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

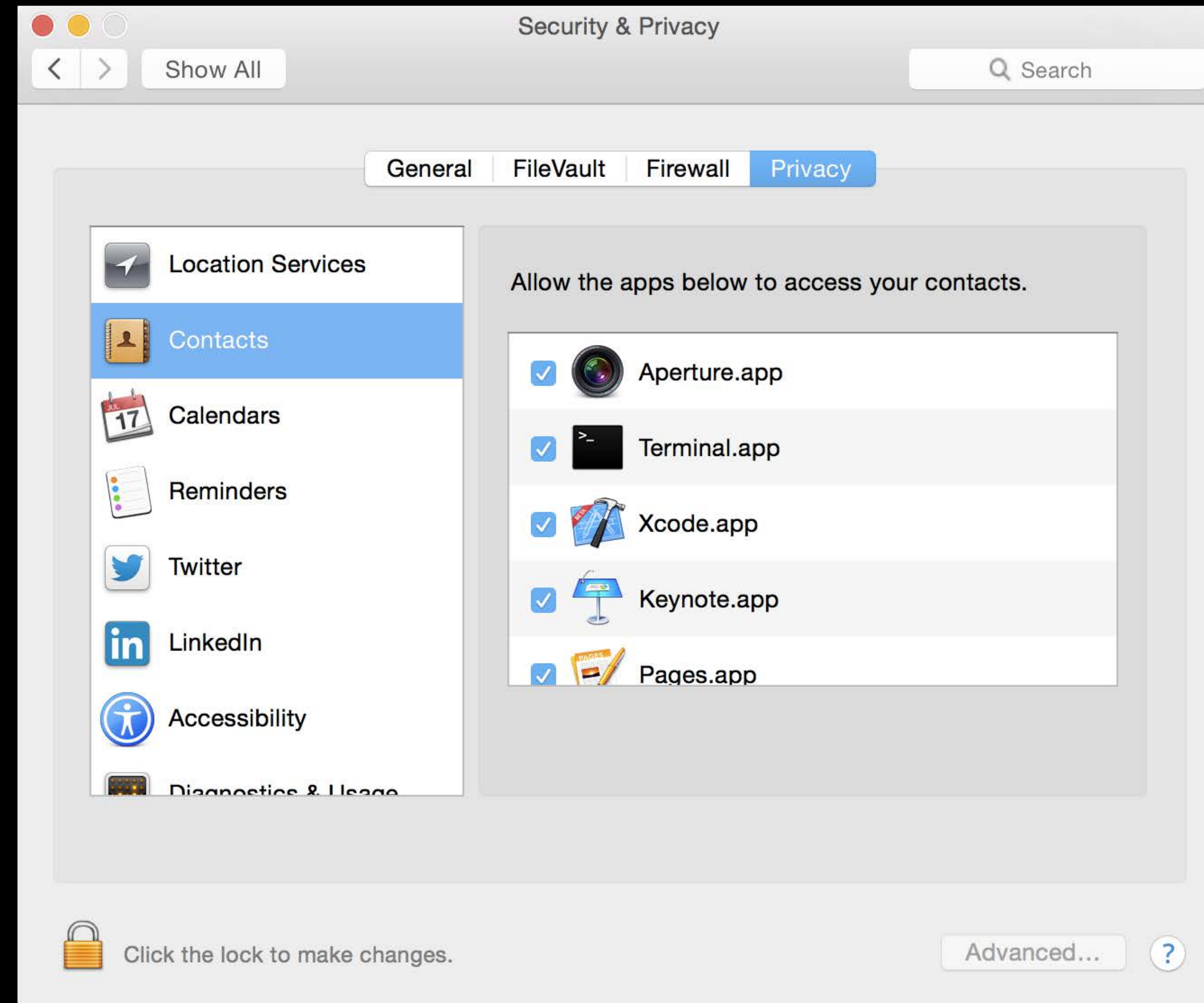
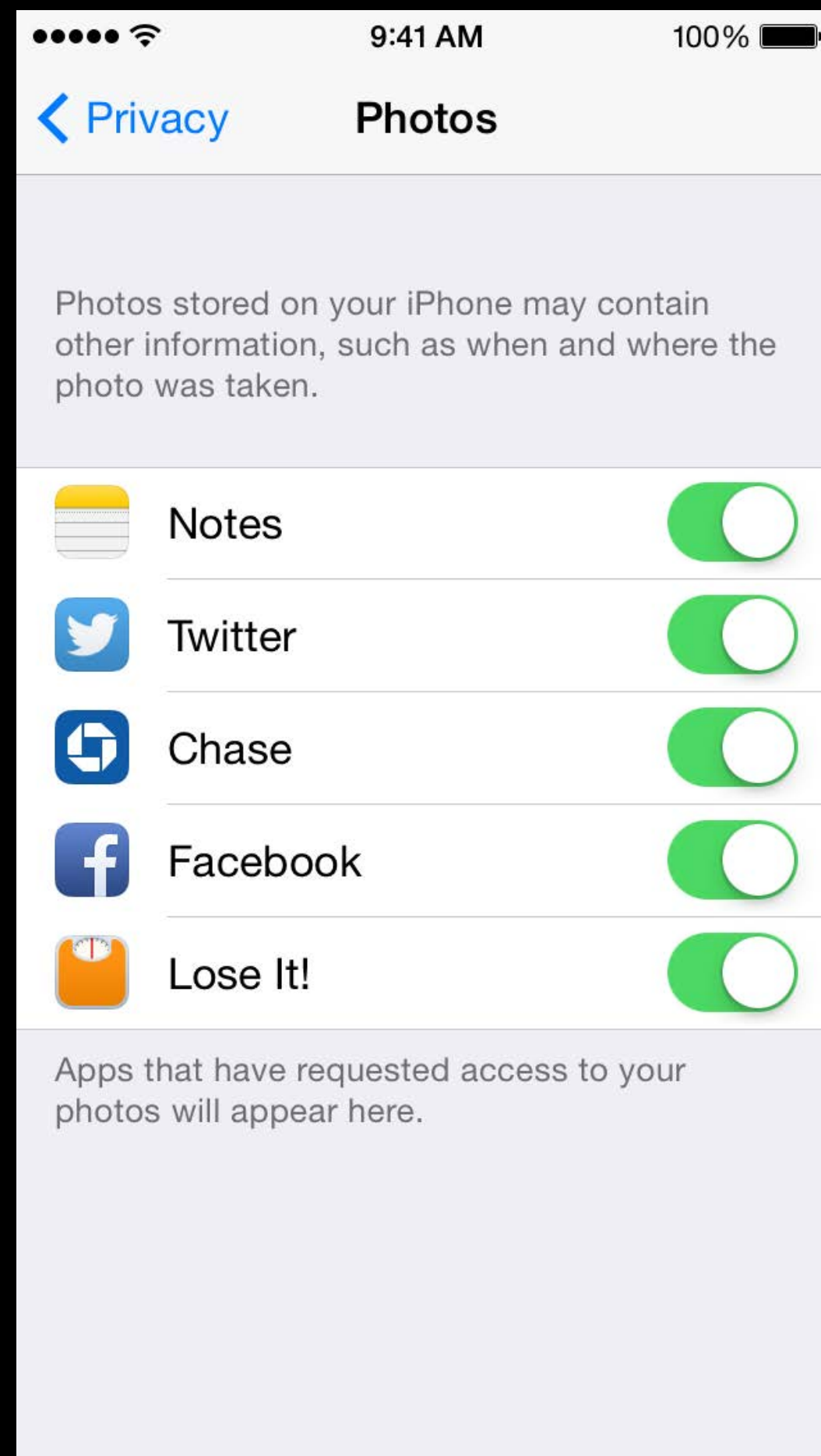
New Purpose String Keys



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

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

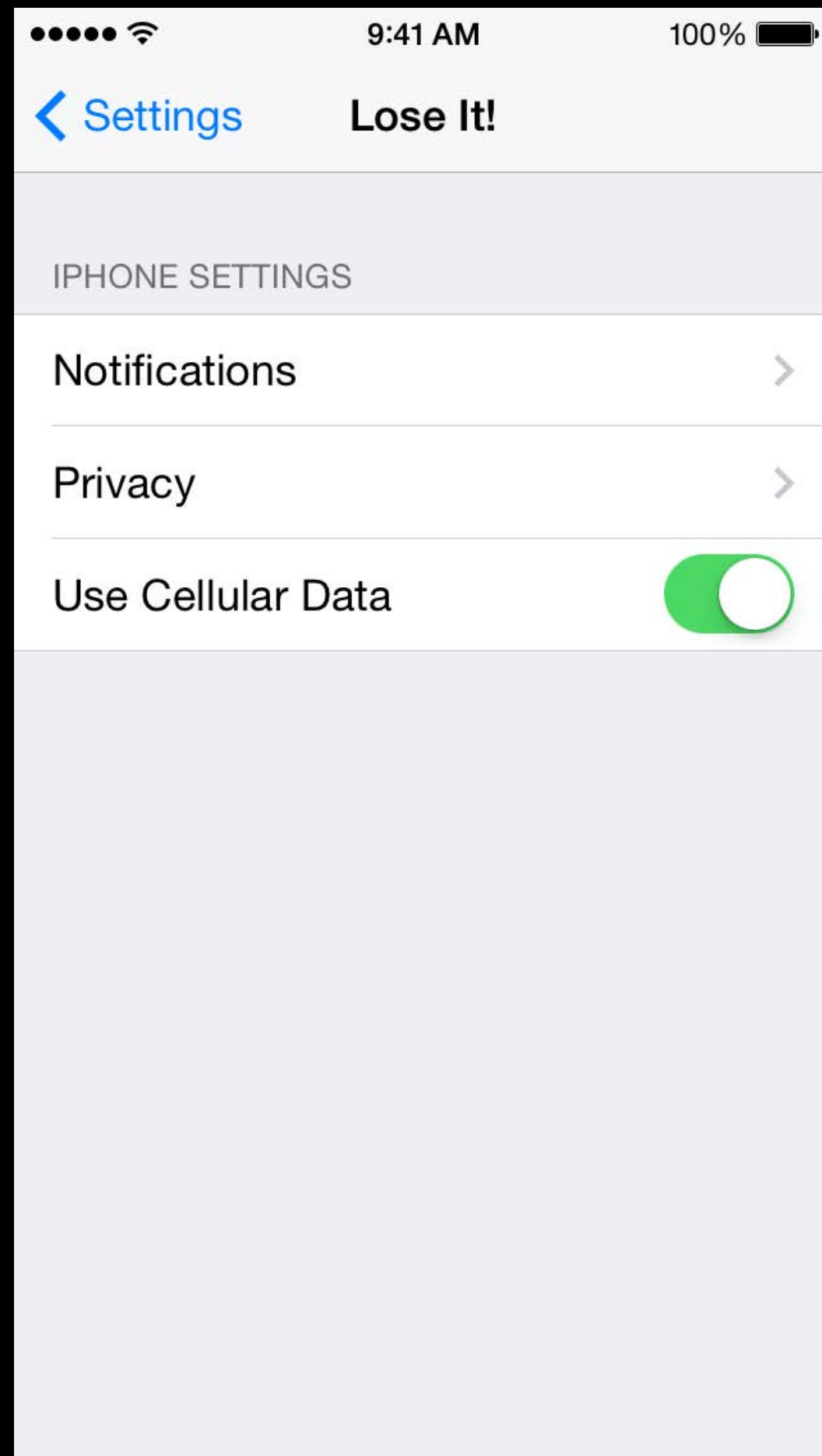


Users may want to update their privacy settings

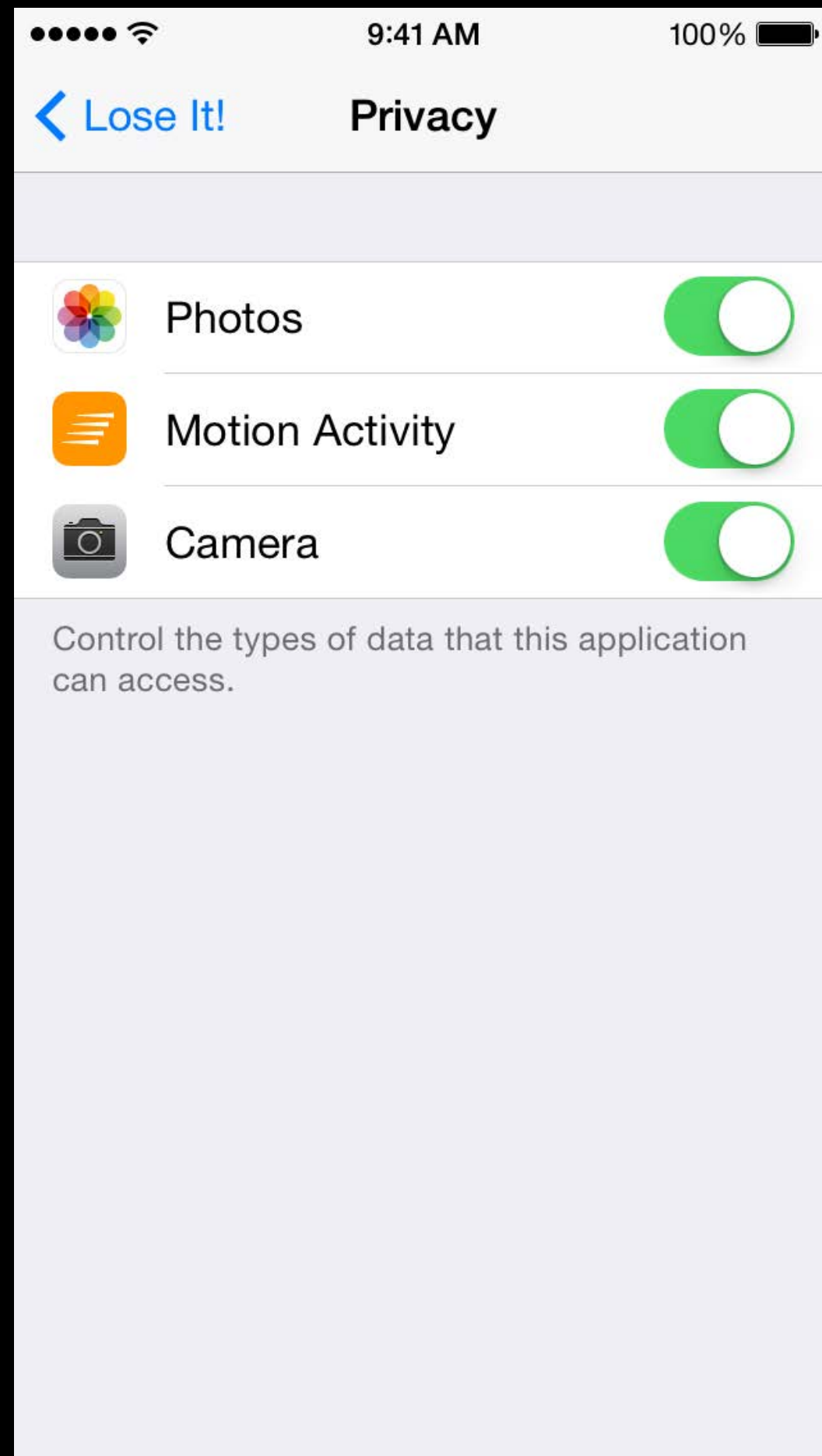
New in iOS 8, your app can direct users directly to settings

```
[[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

The screenshot shows the Xcode interface with the 'Capabilities' tab selected. The 'App Sandbox' capability is turned on. The 'App Data' section has 'Contacts' and 'Calendar' checked. The 'File Access' section shows a table of file types with 'None' permission for all.

General **Capabilities** Info Build Settings Build Phases Build Rules

PROJECT
MyApp

TARGETS
MyApp
MyAppTests
MyAppDesktop
MyAppDesktopTests

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

App Sandbox in Xcode

The screenshot shows the Xcode interface with the 'Capabilities' tab selected. The 'App Sandbox' section is expanded, and the 'App Data' section is highlighted. A table lists file access permissions for various folders, and a 'Steps' section at the bottom provides instructions.

PROJECT

- MyApp

TARGETS

- MyApp
- MyAppTests
- MyAppDesktop**
- MyAppDesktopTests

App Sandbox

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

Hardware: Camera
 Microphone
 USB

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

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

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

– [CLLocationManager
requestAlwaysAuthorization]

CLLocationAlwaysUsageDescription

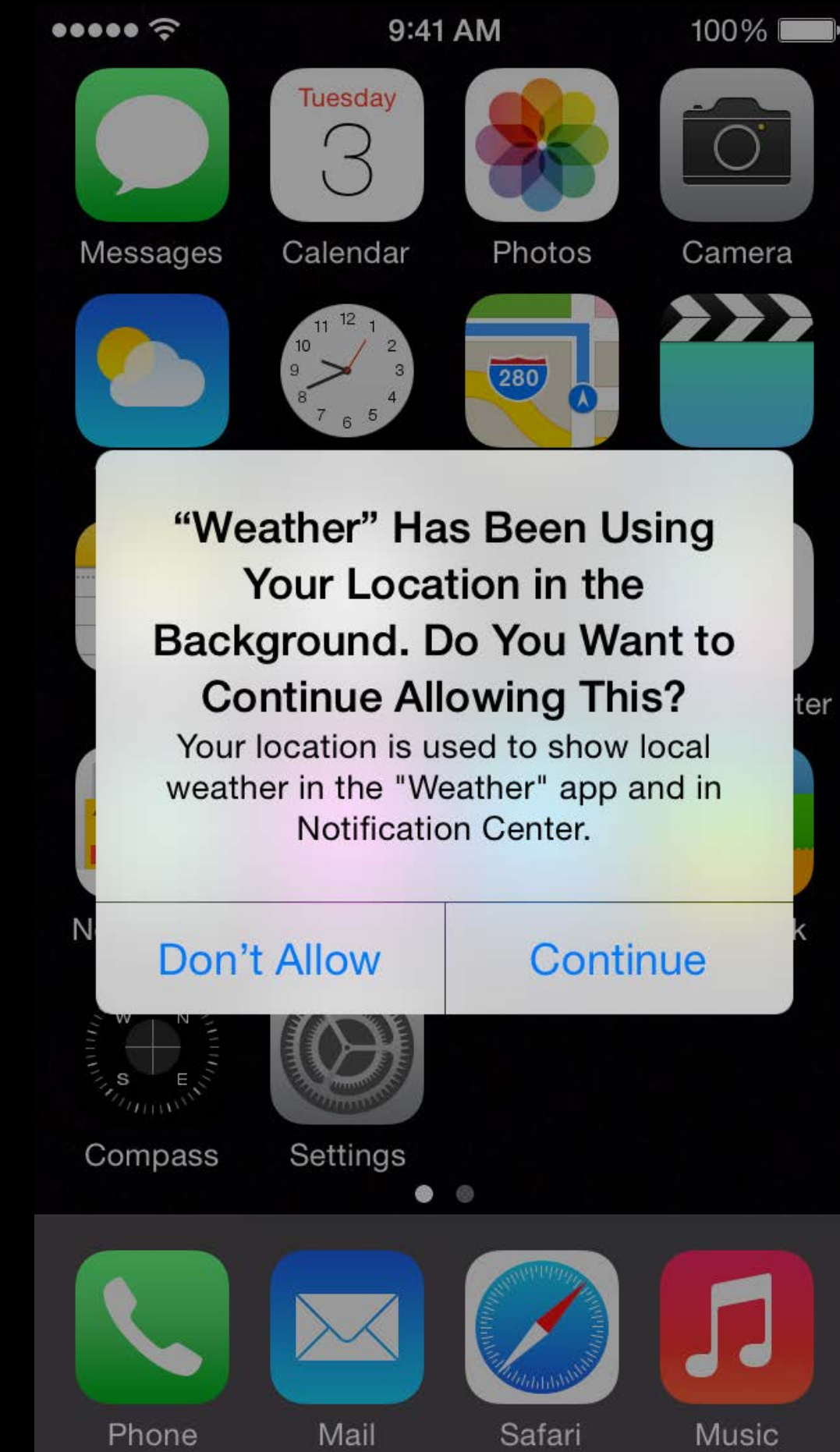
Increased privacy impact for the user

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



`CLLocationUsageDescription` ← 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

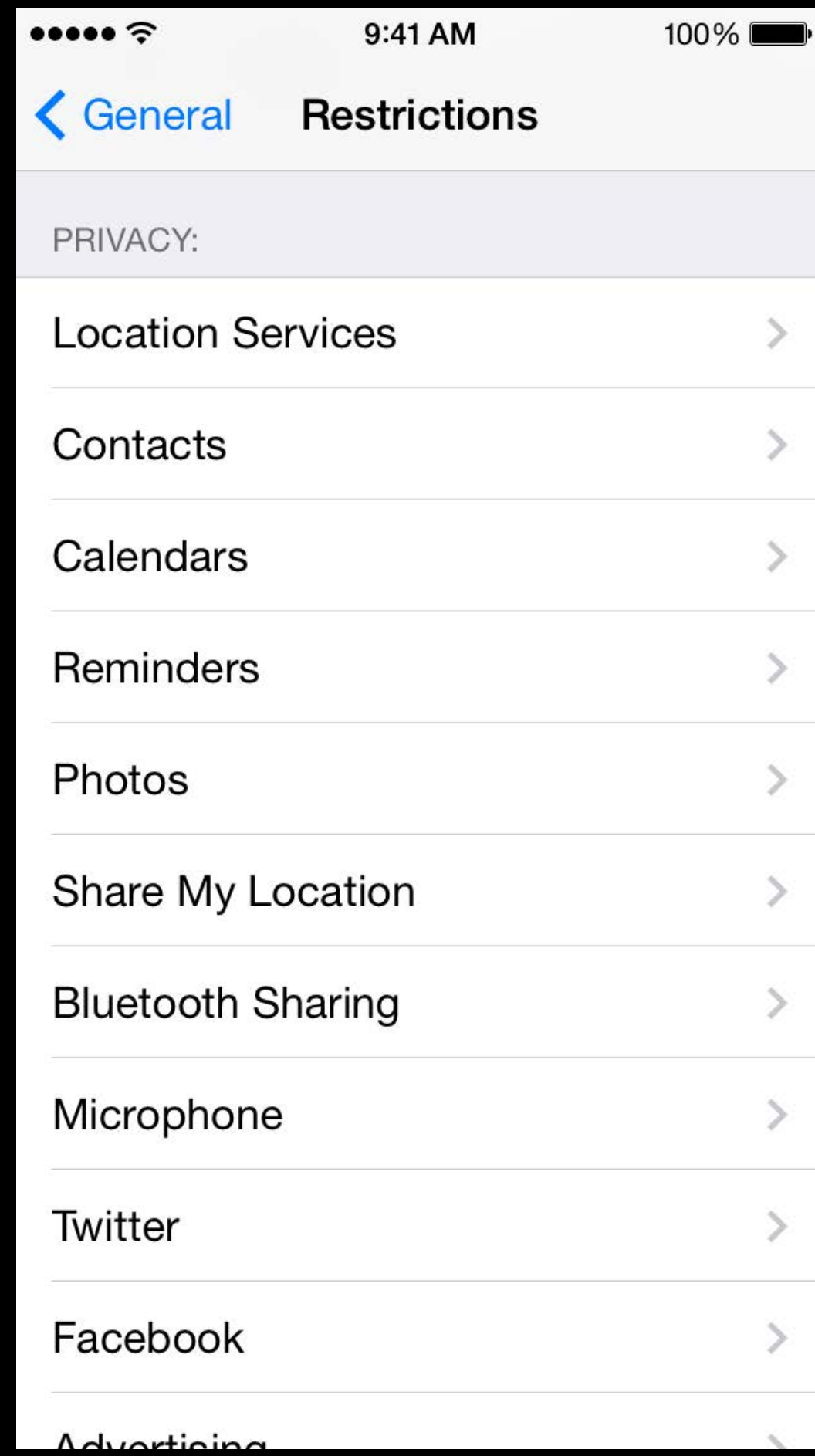
Code should be resilient to lack of data returned

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

Edit English

App Name	iTunes Connect Mobile	
Description	<p>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.</p>	
What's New in this Version	<p>Minor bug fix for push notifications. Adds support for iPhone 5.</p>	
Keywords	iTunes,Connect,Sales,Trends,Apps,Updates,Revenue,Developer,Tools	
Support URL	<input type="text" value="http://itunesconnect.apple.com"/>	
Marketing URL (Optional)	<input type="text" value="http:// itunesconnect.apple.com"/>	
Privacy Policy URL (Optional)	<input type="text" value="http://"/>	

Privacy Policy

iTunes Connect

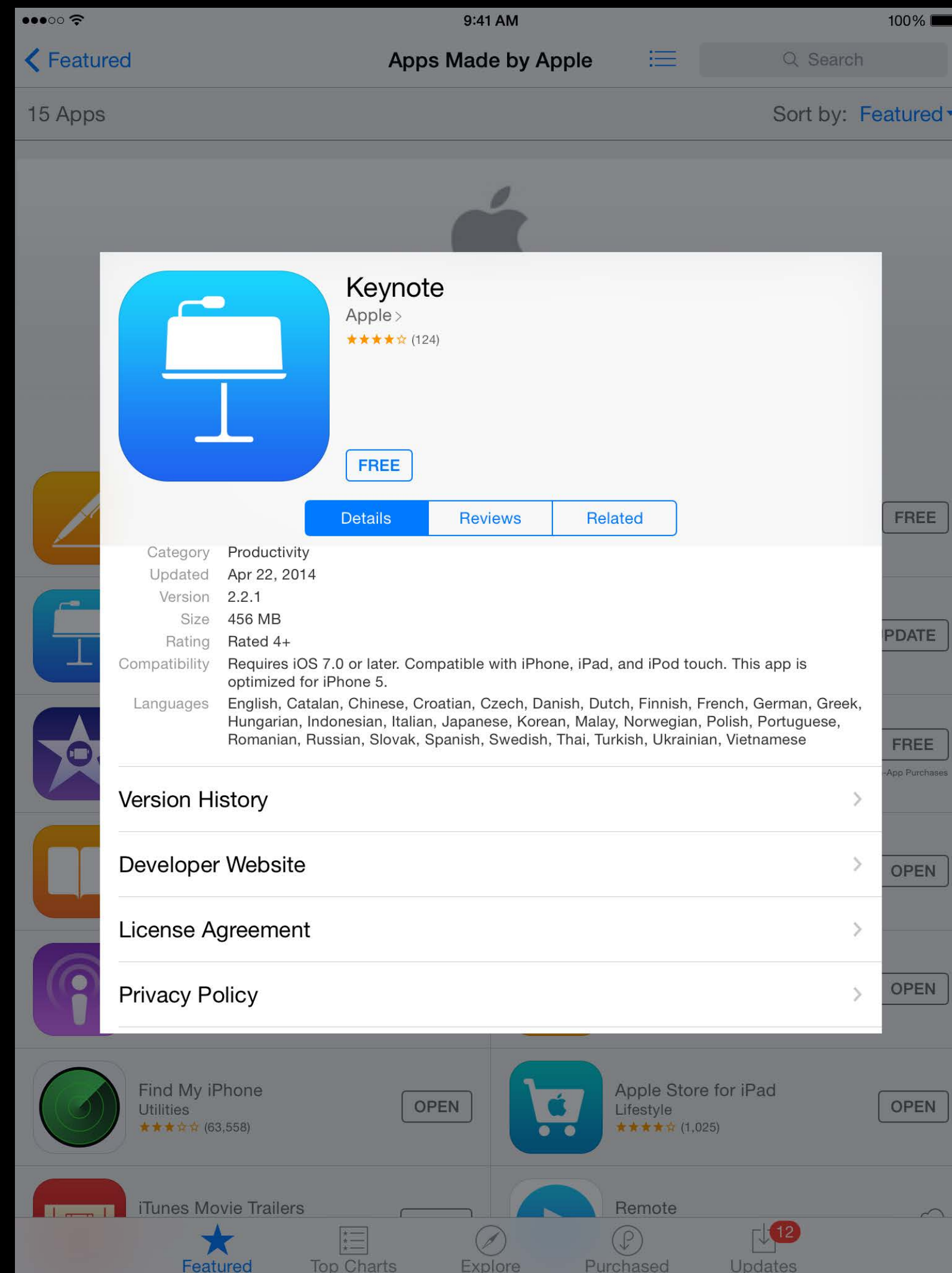
Edit English

App Name	iTunes Connect Mobile	
Description	<p>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.</p>	?
What's New in this Version	<p>Minor bug fix for push notifications. Adds support for iPhone 5.</p>	?
Keywords	iTunes,Connect,Sales,Trends,Apps,Updates,Revenue,Developer,Tools	
Support URL	<input type="text" value="http://itunesconnect.apple.com"/>	?
Marketing URL (Optional)	<input type="text" value="http:// itunesconnect.apple.com"/>	?
Privacy Policy URL (Optional)	<input type="text" value="http://"/>	?

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

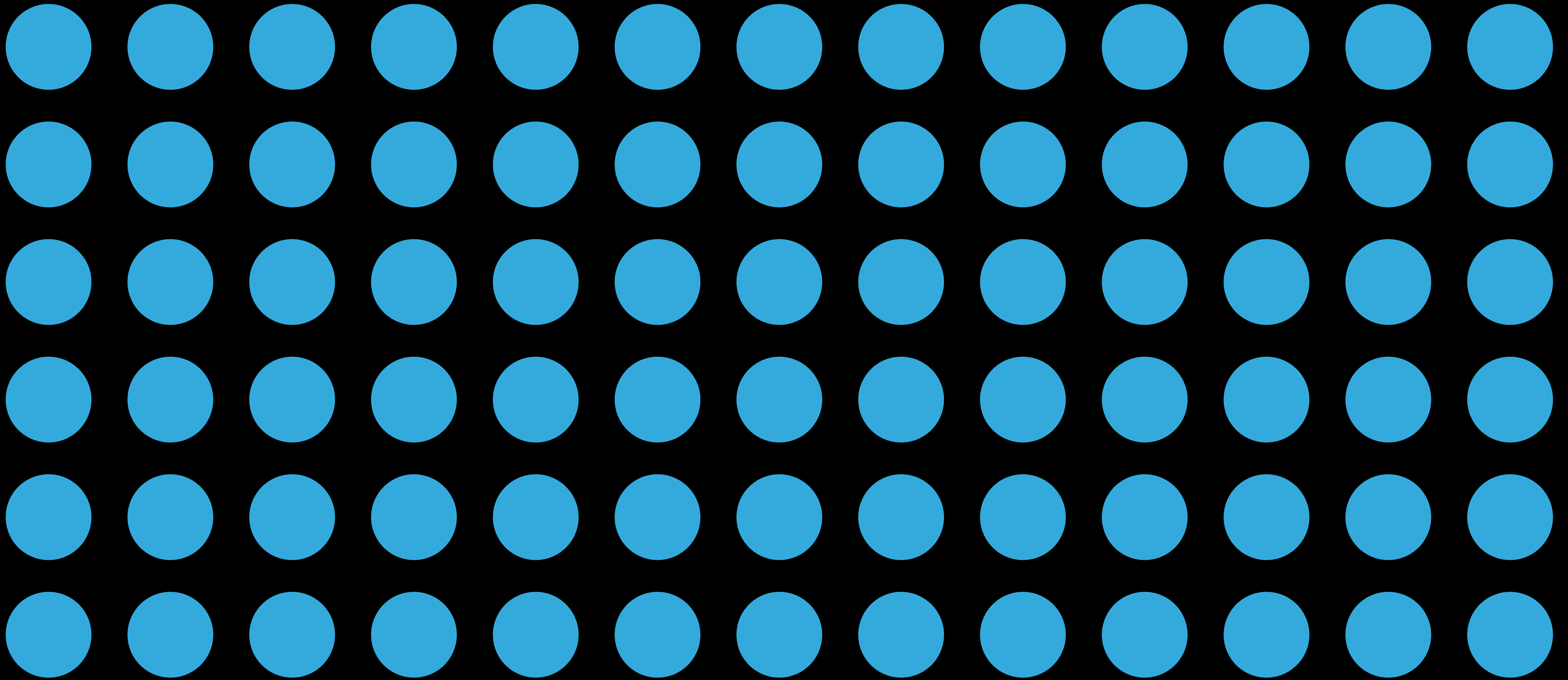
WWDC 2013

Fingerprinting

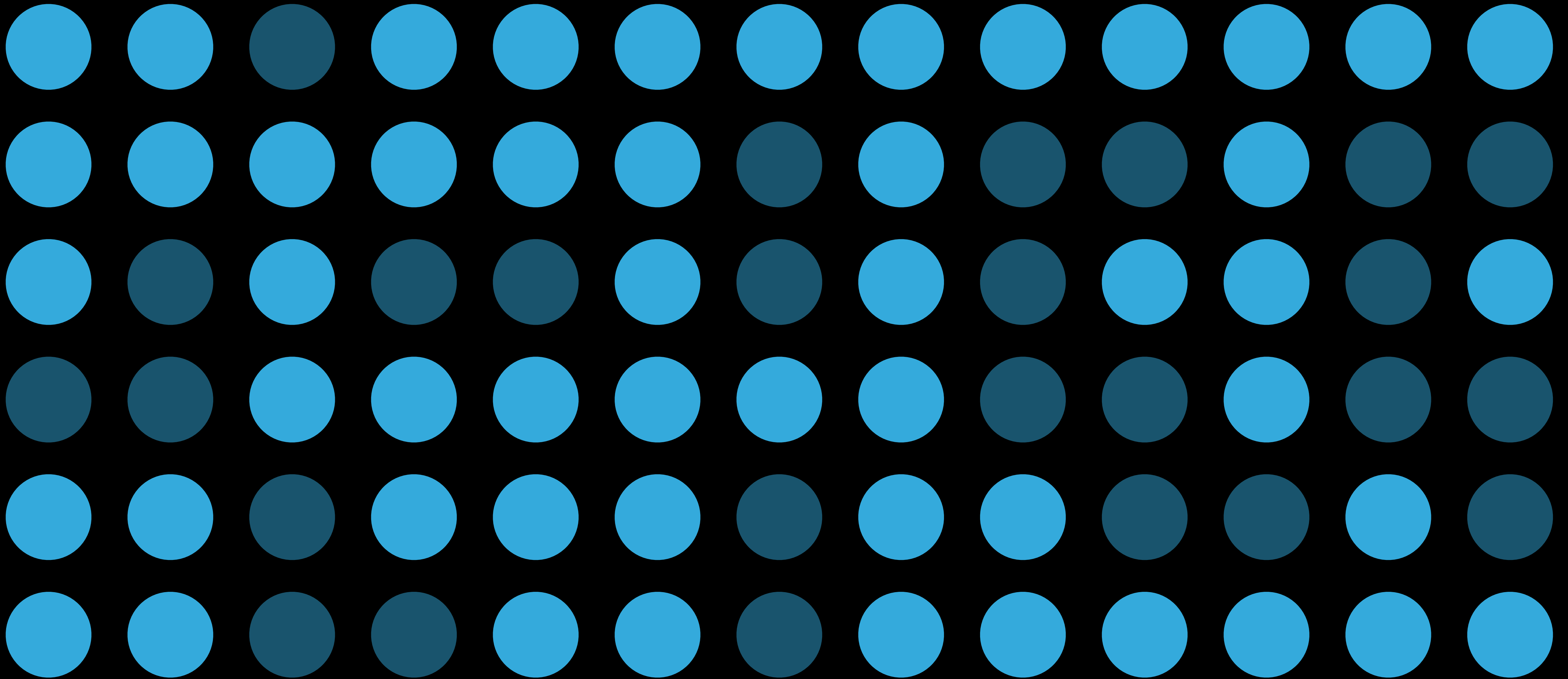
A collection of data that forms a unique, persistent “fingerprint” for a specific user or device

Does not need to be personal information

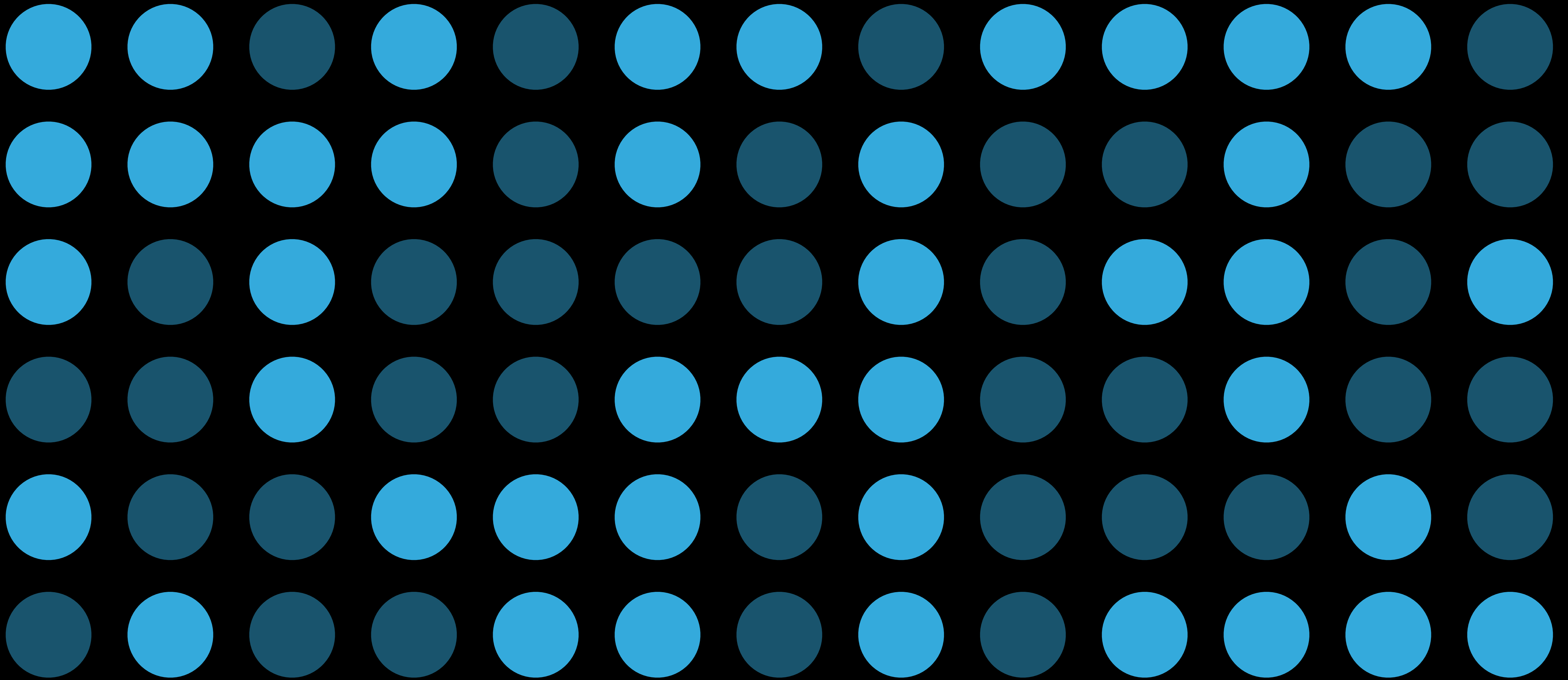
Easy to do accidentally



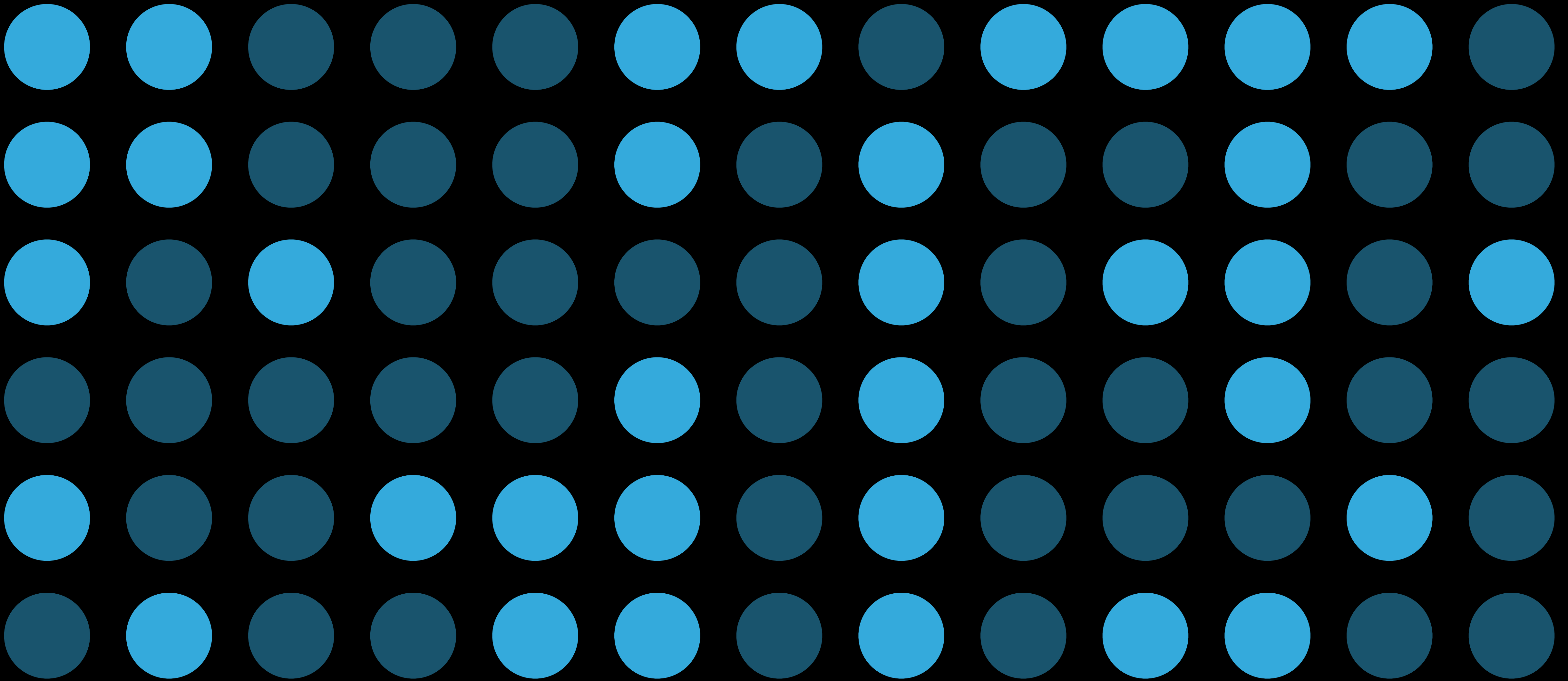
Initial user population



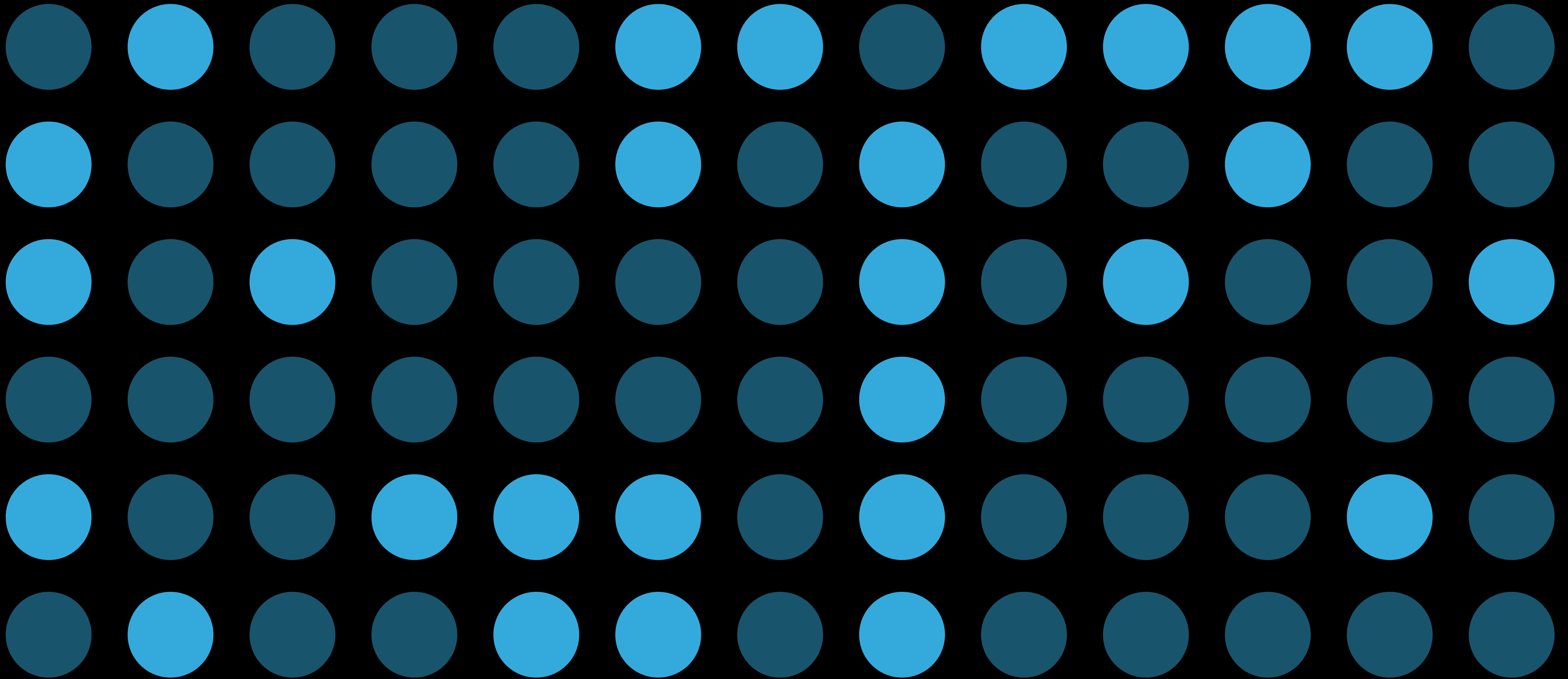
OS X Yosemite installed



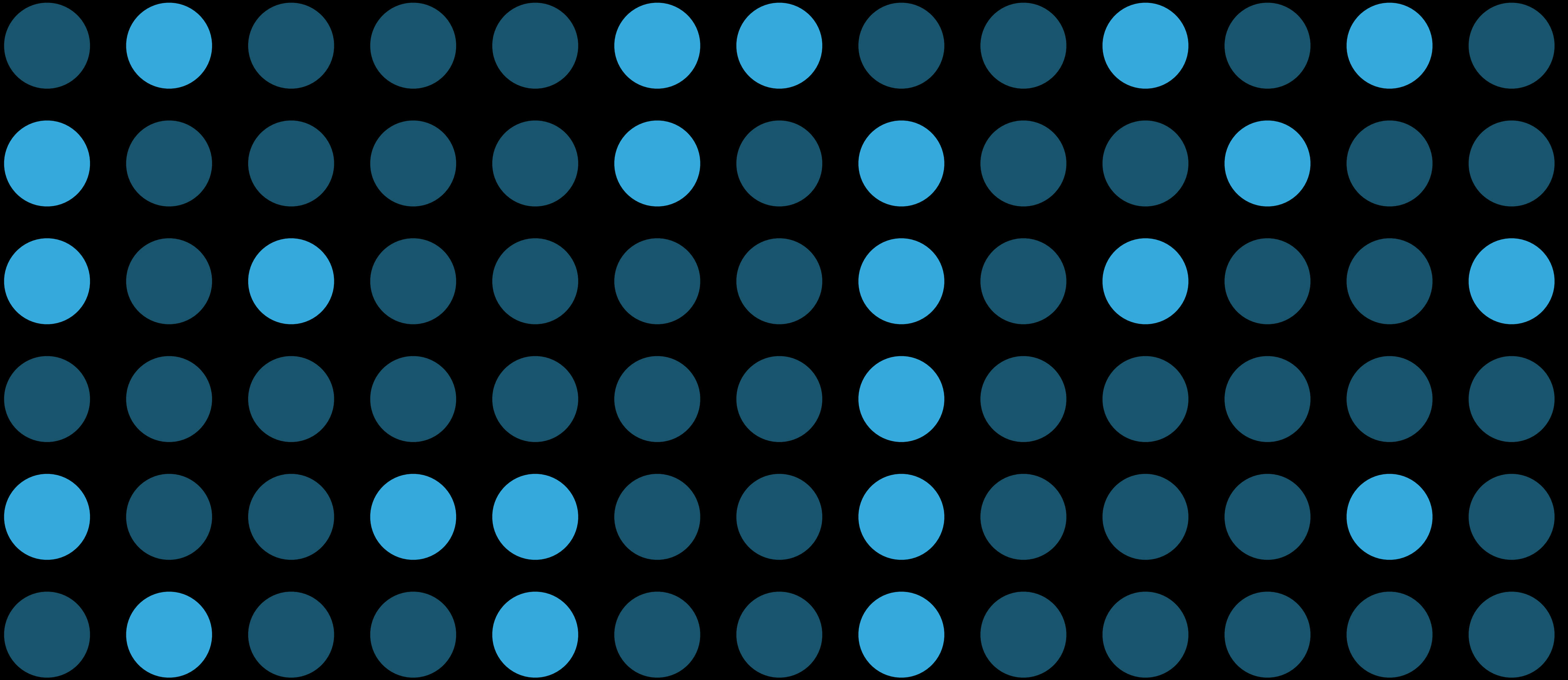
Screen resolution 1920x1280



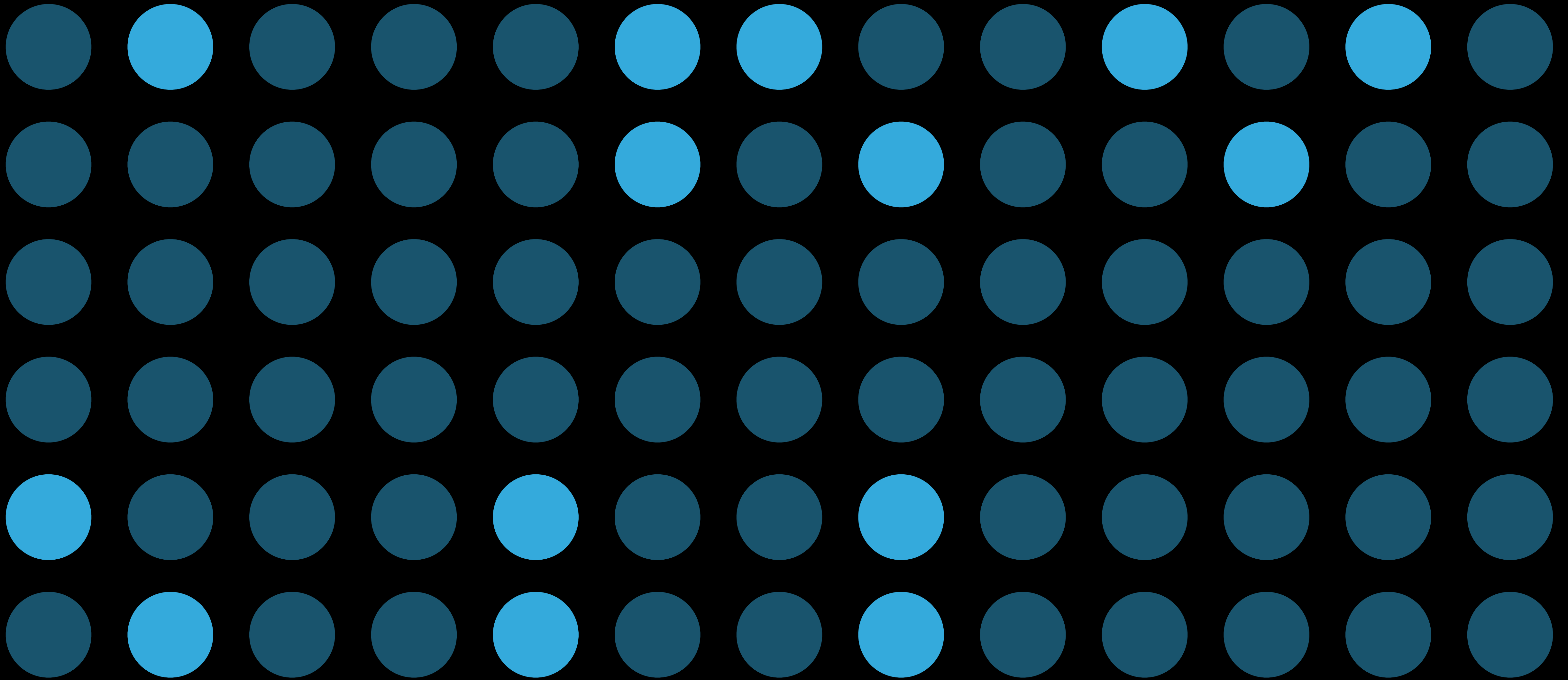
PST timezone



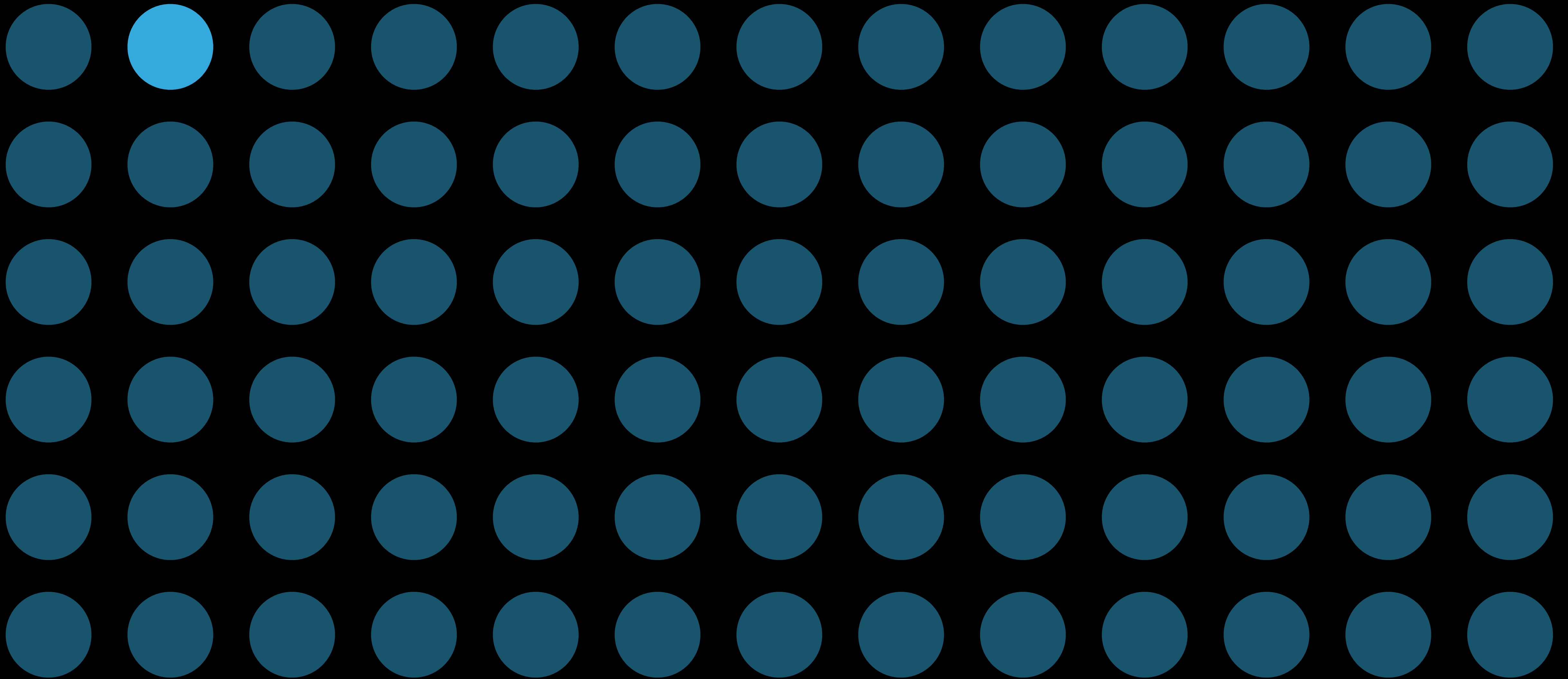
Java installed



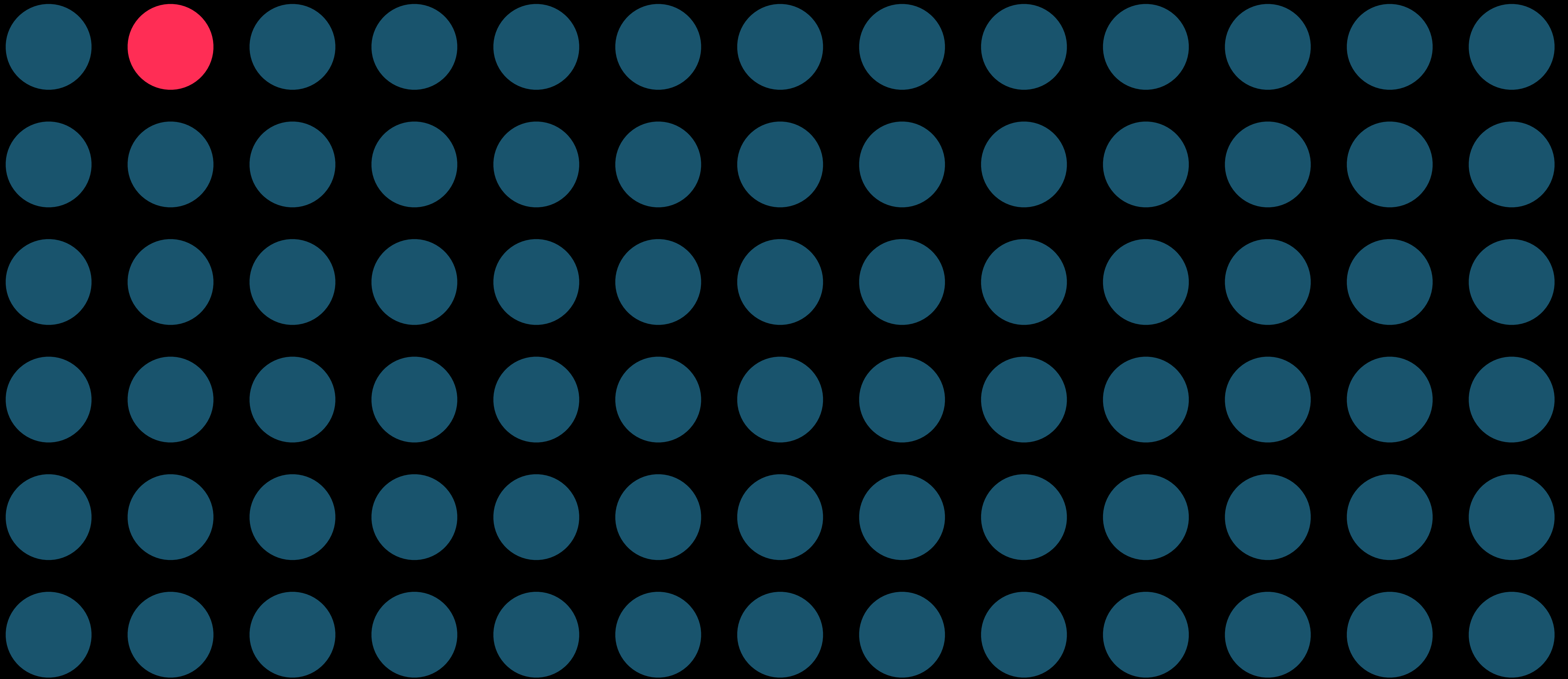
Cookies enabled



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/iphonesprogrammingguide/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