Privacy and Your Apps

Session 702

Georgios Kontaxis, Privacy Engineering
Katie Skinner, Privacy Engineering
“People have entrusted us with their most personal information. We owe them nothing less than the best protection that we can possibly provide.”

Tim Cook, White House Cybersecurity Summit, February 2015
Agenda

Best practices

Updates

Features
Transparency, Consent, and Control

Transparency about the use of data
Consent before collecting data
Users in control of their privacy
Allow “Maps” to access your location while you use the app?

Your current location will be displayed on the map and used for directions, nearby search results, and estimated travel times.

Don’t Allow  Allow
Location Services

Location Services uses GPS, Bluetooth, and crowd-sourced Wi-Fi hotspot and cell tower locations to determine your approximate location. About Location Services & Privacy...

Location Services settings also apply to your Apple Watch.

Share My Location

- Calendar: While Using
- Camera: While Using
- Home: While Using
- Maps: While Using
- Siri & Dictation: While Using
- Weather: While Using

System Services

A hollow arrow indicates that an item may receive your location under certain conditions.
A purple arrow indicates that an item has recently used your location.
A gray arrow indicates that an item has used your location in the last 24 hours.
Identifying Devices and Users

Random
Anonymous
Short-lived
Easy to reset
OS-provided APIs
Universally Unique Identifier

Random

128-bit values

let uuid = UUID()

<table>
<thead>
<tr>
<th>Call 1</th>
<th>8E2F725B-9E3B-459D-89C9-DAC743C174B4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call 2</td>
<td>5C8E2D37-1C56-44B3-974A-928FE4D6C00C</td>
</tr>
<tr>
<td>Call 3</td>
<td>AD748A3A-56C2-4587-A5E2-713C7DBBEED6</td>
</tr>
</tbody>
</table>
Vendor Identifier

Same for apps with the same team ID

Resets when all vendor apps are uninstalled

```swift
let idForVendor = UIDevice.current.identifierForVendor
```

<table>
<thead>
<tr>
<th>Team ID</th>
<th>App</th>
<th>Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Team ID 1</td>
<td>App 1</td>
<td>BD7FA173-A2AB-4761-A9AF-9BEE4C2C3376</td>
</tr>
<tr>
<td>Team ID 1</td>
<td>App 2</td>
<td>BD7FA173-A2AB-4761-A9AF-9BEE4C2C3376</td>
</tr>
<tr>
<td>Team ID 2</td>
<td>App 1</td>
<td>045051D9-EED8-4D35-B2E2-62E6455CAD69</td>
</tr>
</tbody>
</table>
Vendor Identifier

Same for apps with the same team ID

Resets when all vendor apps are uninstalled

```swift
let idForVendor = UIDevice.current.identifierForVendor
```

<table>
<thead>
<tr>
<th>Team ID</th>
<th>App</th>
<th>Vendor Identifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Team ID 1</td>
<td>App 1</td>
<td>BD7FA173-A2AB-4761-A9AF-9BEE4C2C3376</td>
</tr>
<tr>
<td>Team ID 1</td>
<td>App 2</td>
<td>BD7FA173-A2AB-4761-A9AF-9BEE4C2C3376</td>
</tr>
<tr>
<td>Team ID 2</td>
<td>App 1</td>
<td>045051D9-EED8-4D35-B2E2-62E6455CAD69</td>
</tr>
</tbody>
</table>
Tailoring Data Collection to Your Needs

Aggregation
Sampling
On-device processing
Raw Data May Reveal Additional Information

How frequently do users engage with my latest feature?

User 1 is a morning person
User 2 uses the app during lunch
User 3 prefers the night
Raw Data May Reveal Additional Information

How frequently do users engage with my latest feature?

- User 1 likes the feature the most
- User 2 likes the feature the least
- User 3
Aggregation Focuses on the Big Picture

How many users engage with my feature more than 10 times?

- User 1: Yes
- User 2: No
- User 3: Yes

66%
Updates
Prompting with Purpose

Some access requests require a purpose string.
Specific ask enables informed user decisions.

Info.plist: NSLocationUsageDescription
Prompting with Purpose

Some access requests require a purpose string

Specific ask enables informed user decisions

Info.plist: NSLocationUsageDescription
Add Purpose String in Xcode

<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>Bundle identifier</td>
<td>String</td>
<td>$(PRODUCT_BUNDLE_IDENTIFIER)</td>
</tr>
<tr>
<td>InfoDictionary version</td>
<td>String</td>
<td>6.0</td>
</tr>
<tr>
<td>Main storyboard file base name</td>
<td>String</td>
<td>Main</td>
</tr>
<tr>
<td>Bundle version</td>
<td>String</td>
<td>1</td>
</tr>
<tr>
<td>Launch screen interface file base name</td>
<td>String</td>
<td>LaunchScreen</td>
</tr>
<tr>
<td>Executable file</td>
<td>String</td>
<td>$(EXECUTABLE_NAME)</td>
</tr>
<tr>
<td>Application requires iPhone environment</td>
<td>Boolean</td>
<td>YES</td>
</tr>
<tr>
<td>Bundle name</td>
<td>String</td>
<td>$(PRODUCT_NAME)</td>
</tr>
<tr>
<td>Supported interface orientations</td>
<td>Array</td>
<td>(3 items)</td>
</tr>
<tr>
<td>Required device capabilities</td>
<td>Array</td>
<td>(1 item)</td>
</tr>
<tr>
<td>Bundle OS Type code</td>
<td>String</td>
<td>APPL</td>
</tr>
<tr>
<td>Localization native development region</td>
<td>String</td>
<td>en</td>
</tr>
<tr>
<td>Supported interface orientations (iPad)</td>
<td>Array</td>
<td>(4 items)</td>
</tr>
<tr>
<td>Privacy - Location When In Use Usage...</td>
<td>String</td>
<td>Your current location will be displayed on the map and used for directions</td>
</tr>
</tbody>
</table>
### Add Purpose String in Xcode

#### Privacy - Location When In Use Usage Description

**Key:** Privacy - Location When In Use Usage Description

**Type:** String

**Value:** Your current location will be displayed on the map and used for directions
Add Purpose String in Xcode

<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>Bundle identifier</td>
<td>String</td>
<td>$(PRODUCT_BUNDLE_IDENTIFIER)</td>
</tr>
<tr>
<td>InfoDictionary version</td>
<td>String</td>
<td>6.0</td>
</tr>
<tr>
<td>Main storyboard file base name</td>
<td>String</td>
<td>Main</td>
</tr>
<tr>
<td>Bundle version</td>
<td>String</td>
<td>1</td>
</tr>
<tr>
<td>Launch screen interface file base name</td>
<td>String</td>
<td>LaunchScreen</td>
</tr>
<tr>
<td>Executable file</td>
<td>String</td>
<td>$(EXECUTABLE_NAME)</td>
</tr>
<tr>
<td>Application requires iPhone environment</td>
<td>Boolean</td>
<td>YES</td>
</tr>
<tr>
<td>Bundle name</td>
<td>String</td>
<td>$(PRODUCT_NAME)</td>
</tr>
<tr>
<td>Supported interface orientations</td>
<td>Array</td>
<td>(3 items)</td>
</tr>
<tr>
<td>Required device capabilities</td>
<td>Array</td>
<td>(1 item)</td>
</tr>
<tr>
<td>Bundle OS Type code</td>
<td>String</td>
<td>APPL</td>
</tr>
<tr>
<td>Localization native development region</td>
<td>String</td>
<td>en</td>
</tr>
<tr>
<td>Privacy - Location When In Use Usage...</td>
<td>String</td>
<td>Your current location will be displayed on the map and used for directions</td>
</tr>
</tbody>
</table>
Exception Type: EXC_CRASH (SIGABRT)

Application Specific Information:
This app has crashed because it attempted to access privacy-sensitive data without a usage description.
The app's Info.plist must contain a NSCameraUsageDescription key with a string value explaining to the user how the app uses this data.
### Purpose String Required

**iOS 10**

<table>
<thead>
<tr>
<th>Contacts</th>
<th>Camera</th>
<th>CallKit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calendar</td>
<td>Photos</td>
<td>Speech Recognition</td>
</tr>
<tr>
<td>Reminders</td>
<td>Health</td>
<td>SiriKit</td>
</tr>
<tr>
<td>Location</td>
<td>HomeKit</td>
<td>TV Provider</td>
</tr>
<tr>
<td>Bluetooth Sharing</td>
<td>Media Library</td>
<td></td>
</tr>
<tr>
<td>Microphone</td>
<td>Motion and Fitness</td>
<td></td>
</tr>
<tr>
<td>Purpose String Required</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>iOS 11</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Feature</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contacts</td>
<td>Camera</td>
</tr>
<tr>
<td>Calendar</td>
<td>Photos</td>
</tr>
<tr>
<td>Reminders</td>
<td>Health</td>
</tr>
<tr>
<td>Location</td>
<td>HomeKit</td>
</tr>
<tr>
<td>Bluetooth Sharing</td>
<td>Media Library</td>
</tr>
<tr>
<td>Microphone</td>
<td>Motion and Fitness</td>
</tr>
<tr>
<td>CallKit</td>
<td>Speech Recognition</td>
</tr>
<tr>
<td>SiriKit</td>
<td>TV Provider</td>
</tr>
<tr>
<td>NFC</td>
<td></td>
</tr>
</tbody>
</table>
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 widget.

- Don’t Allow
- Allow
Allow “Weather” to access your location?

Your location is used to show local weather in the Weather app and widget.

Select:
- Only While Using the App
- Always Allow
- Don’t Allow
CoreLocation—When In Use

Support When In Use location authorization

- NSLocationWhenInUseUsageDescription
- NSLocationAlwaysAndWhenInUseUsageDescription

Ask for location in a meaningful way

- Prompt in the right context
- Start with When In Use
CoreLocation—Legacy Apps

Linked against iOS 10

When In Use undefined

Compatibility warning
CoreLocation—Legacy Apps

Linked against iOS 10

When In Use undefined

Compatibility warning
CoreLocation—Legacy Apps

Linked against iOS 10

When In Use and Always defined
CoreLocation—Legacy Apps

Linked against iOS 10

When In Use and Always defined

Allow "Potloc" to access your location?

App explanation for always: “Your location will be used for demonstration purposes all the time.”

App explanation for while using: “Your location will be used for demonstration purposes only when you are using the app”

Only While Using the App

Always Allow

Don’t Allow
Photos

Image picker without prompting for access

Write only support

Authorization will be reset on upgrade
Photos—Image Picker

Does not require explicit authorization

Access to photos or videos the user chooses

Great for rare actions within your app

UIImagePickerController
Photos—Write-only

Ability to add items to the Photo Library

NSPhotoLibraryAddUsageDescription

Does not enable read

UIImageWriteToSavedPhotosAlbum

UISaveVideoAtPathToSavedPhotosAlbum

“Vacation” Would Like to Add to your Photos
Save some awesome photos and videos!

Don’t Allow  OK
CoreNFC

Scan for nearby NFC tags

In the foreground

NFCReaderUsageDescription

Ready to Scan

Hold iPhone near [Insert your usage description]

Cancel

Introducing Core NFC

WWDC 2017 Video
Microphone—watchOS

Recording allowed to continue in the background

Recording possible without the built-in modal UI

Requires microphone authorization

Indicator on watch face
MusicKit

Token unlocks features based and personalized and non-personalized APIs

Seamless authentication through a Music token

User’s consent is necessary

Control over the apps authorized
“Shazam” would like to access Apple Music, your music and video activity, and your media library.
...to play full songs

Don’t Allow  OK
Safari View Controller
iOS 11

Safari and other apps get their own cookies and website data.

Clearing website data in Safari also clears the data in your app.

Domain
apple.com
example.org

Cookie
= iphone 7
= john appleseed
Safari View Controller
iOS 11

Safari and other apps get their own cookies and website data

Clearing website data in Safari also clears the data in your app

---

**Domain**
- apple.com

**Cookie**
- = iphone 7

---

**Domain**
- example.org

**Cookie**
- = john appleseed
Features

Katie Skinner, Privacy Engineering
On-Device Processing
On-Device Processing

Benefits

Works anywhere

Network latency

Performance
120x
On-Device Processing
Privacy benefits

Access to user data

Security built in to iOS
• Keychain, data protection

Lower risk
On-Device Processing

Frameworks

CoreML

VisionKit

ARKit

NLP

Introducing Core ML

Hall 3

Tuesday 3:10PM
DeviceCheck
iOS, tvOS
DeviceCheck

Identifying devices

• Did this device already consume a free trial?
• Has this device paid for content but not linked that purchase to an account?
• Was this device previously used by an abusive user?
• Was this device previously used for fraudulent activities?
DeviceCheck

Assign state to a device

Privacy friendly
DeviceCheck

Per device, per developer data stored by Apple

Two bits and a timestamp

Until developer resets
• Erase install

Input to business logic
DeviceCheck

Per device, per developer data stored by Apple

Two bits and a timestamp

Until developer resets
• Erase install

Input to business logic
DeviceCheck
1. Query for token
DeviceCheck

1. Query for token
2. Send token to app server
DeviceCheck

1. Query for token
2. Send token to app server
3. Set two bit
DeviceCheck

1. Query for token
2. Send token to app server
3. Set two bit

App Server

Apple
DeviceCheck

4. Delete App
5. Reinstall App
DeviceCheck

4. Delete App
5. Reinstall App
6. Query for token
7. Send token to app server
DeviceCheck

1. Delete App
2. Reinstall App
3. Query for token
4. Send token to app server
5. Query two bit
6. Send token to Apple
7. Query for token
8. Reinstall App
DeviceCheck

1. Delete App
2. Reinstall App
3. Query for token
4. Send token to app server
5. Query two bit
6. Send token to app server
7. Apple
8. Reinstall App
DeviceCheck

Georgios’ iPhone
DeviceCheck

10. Install App

11. Query for token

12. Send token to app server
DeviceCheck

10. Install App

11. Query for token

12. Send token to app server

13. Query for two bit
DeviceCheck

10. Install App
11. Query for token
12. Send token to app server
13. Query for two bit
DeviceCheck
Query
Request to Apple to query bit state

{
    "device_token": "wlkCDA2Hy/CfMqVASHs1BAR/0sAiuRIUm5jQg0a..."
    "transaction_id": "5b737ca6-a4c7-488e-b928-8452960c4be9",
    "timestamp": 1487716472000
}
Response from Apple with the bit state

```
{
    "bit0" : true,
    "bit1" : true,
    "last_update_time": "2017-02"
}
```

Last update rounded to the month
Update bit state

{
    "device_token" : "wlkCDA2Hy/CfMqVASHs1BAR/0sAiuRIUm5jQg0a..."
    "transaction_id" : "5b737ca6-a4c7-488e-b928-8452960c4be9",
    "timestamp" : 1487716472000,
    "bit0" : true,
    "bit1" : false
}
Best practices

Handle resold or transferred devices

Relevancy based on age

Part of your app logic not sole source

Should not affect UI

• e.g. “Welcome Back!”
Identifying Devices the Right Way

Use platform supported identifiers
• Application Identifier, Vendor Identifier, Advertising Identifier

Will continue to remove entropy

Will continue to provide user control of entropy sources

Will continue to remove functionality that is being abused to uniquely identify users
Intelligent Tracking Prevention
Safari
Intelligent Tracking Prevention

Does not block content

Dynamically detects online tracking
- On-device classifier

Hinders tracking
- Isolates
- Periodically purges

User interaction temporarily whitelists domains
Cookie Partitioning

Cookies from example.com are partitioned by each domain that embeds

site1.com  site2.com
Cookie Partitioning

Cookies from example.com are partitioned by each domain that embeds

- site1.com
- site2.com
- example.com
- foo
Cookie Partitioning

Cookies from example.com are partitioned by each domain that embeds
Cookie Purging

Cookies from example.com are purged on a regular basis

- Site1.com
  - example.com
  - foo

- Site2.com
  - example.com
  - bar
Cookie Purging

Cookies from example.com are purged on a regular basis
Intelligent Tracking Prevention

User interaction

Safari will not delete cookies and website data from example.com
• If example.com is a first party site
• If the user taps, clicks, or fills out a form

Do not rely on storage if a user does not interact with your site

Ensure your analytics package does not rely on third party cookies
Differential Privacy
Differential Privacy

Launched on iOS, macOS

Millions of donations per day

Building better products with privacy

New uses
Differential Privacy

New use cases

Learn commonly used Health data types

• Learn ‘steps’ not 10,678 steps
Learning Popular Emojis with Privacy

Julien

Jessie

Jason

Frequency

...
Learning Popular Health Data Type

Julien
Jessie
Timmy
Learning Popular Health Data Type

Julien

Jessie

Timmy
Learning Popular Health Data Type

- Steps
- Flights Climbed
- Height
- Weight
- Lean Body Mass
- Heart Rate
- Blood Glucose
- Blood Pressure
- Copper
- Blood Fat%
- Body Fat%
- Calories
- Body Fat
- Active Energy
- Exercice Minutes
- Basal Body Temp
- Resting Energy
- Iron
- Niacin
- Carbohydrates
- Caffeine
- Dietary Cholesterol
- Chloride
- Caffeine
- Exercise Minutes
- Resting Energy
- Basal Body Temp
- Active Energy
- Copper
- Blood Pressure
- Blood Glucose
- Lean Body Mass
- Heart Rate
- Weight
- Height
- Flights Climbed
- Steps

- Julien
- Jessie
- Timmy
Differential Privacy

New use cases

Learn web domains that cause performance issues

Reach out to developers
Build great features
Build great features + respect user privacy
More Information

<table>
<thead>
<tr>
<th>Session</th>
<th>Location</th>
<th>Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introducing Core ML</td>
<td>Hall 3</td>
<td>Tuesday 3:10PM</td>
</tr>
<tr>
<td>Introducing MusicKit</td>
<td>Grand Ballroom B</td>
<td>Tuesday 3:10 PM</td>
</tr>
<tr>
<td>Introducing ARKit: Augmented Reality for iOS</td>
<td>Hall 3</td>
<td>Tuesday 5:10 PM</td>
</tr>
<tr>
<td>Natural Language Processing and your Apps</td>
<td>Hall 3</td>
<td>Wednesday 9:00AM</td>
</tr>
<tr>
<td>What's New in Photo APIs</td>
<td>Hall 2</td>
<td>Wednesday 1:50PM</td>
</tr>
<tr>
<td>Vision Framework: Building on Core ML</td>
<td>Hall 2</td>
<td>Wednesday 3:10PM</td>
</tr>
<tr>
<td>What's New in Location Technologies</td>
<td>Grand Ballroom B</td>
<td>Thursday 3:10PM</td>
</tr>
<tr>
<td>Introducing Core NFC</td>
<td>WWDC 2017 Video</td>
<td></td>
</tr>
<tr>
<td>Lab Name</td>
<td>Location</td>
<td>Time</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>---------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Security &amp; Privacy Lab</td>
<td>Technology Lab D</td>
<td>Tue 1:50PM–3:50PM</td>
</tr>
<tr>
<td>iCloud Photo Library &amp; PhotoKit Lab</td>
<td>Technology Lab G</td>
<td>Wed 9:00AM-11:00AM</td>
</tr>
<tr>
<td>Location and Mapping Technologies Lab</td>
<td>Technology Lab B</td>
<td>Wed 11:00AM-1:00PM</td>
</tr>
<tr>
<td>Security &amp; Privacy Lab</td>
<td>Technology Lab J</td>
<td>Wed 1:00PM–4:20PM</td>
</tr>
<tr>
<td>Core ML and Natural Language Processing Lab</td>
<td>Technology Lab D</td>
<td>Thu 11:00AM-3:30PM</td>
</tr>
</tbody>
</table>