# Better Apps Through Better Privacy

Session 718

Joey Tyson, Privacy Engineer
Brandon Van Ryswyk, Privacy Engineer
Privacy is about people.
Privacy Is About People

Build trust with your users

Respect users in handling their data

Apply privacy thinking to engineering decisions
"In every way, at every turn, the question we ask ourselves is not what can we do, but what should we do."

Tim Cook, Duke University, May 13, 2018
Ask the “should” questions.
Ask Questions about Data

Why do we need this data?
Would this surprise our users?
Could we use less granular data?
How long do we need this data?
Recognize Data Assumptions
Recognize Data Assumptions

“Of course we should log this for all users.”
Recognize Data Assumptions

“Of course we should log this for all users.”

“This data couldn’t possibly be sensitive.”
Recognize Data Assumptions

“Of course we should log this for all users.”

“This data couldn’t possibly be sensitive.”

“It’s fine to apply this data in a new use case.”
Recognize Data Assumptions

“Of course we should log this for all users.”

“This data couldn’t possibly be sensitive.”

“It’s fine to apply this data in a new use case.”

“There’s no PII, so don’t worry about it.”
Recognize Data Assumptions

“Of course we should log this for all users.”

“This data couldn’t possibly be sensitive.”

“It’s fine to apply this data in a new use case.”

“There’s no PII, so don’t worry about it.”

“We already protect this with encryption.”
Create Privacy Guarantees

Write high-level statements about privacy expectations

Decide in planning, verify in implementation

Examples:
• “We cannot read your messages in transit between devices.”
• “Analytics data does not identify you personally.”
• “We only retain aggregate usage data.”
Align data practices with use cases.
Handle Data with Caution

Data brings power—and danger

Gathering data adds overhead and liability

Unexpected data adds more risks and distrust
Use Proportional Data Collection

Collect only what is needed to achieve the goal
Collect consistently with user expectations
Do not collect without a clear reason
Use Privacy Techniques

Develop a toolbox
Adjust to match use case
Apply across systems
Build technical enforcements
Example: Activity Sharing

De-identified  Aggregation  Control
Example: News

De-identified  Aggregation  Control
Example: Photo Memories

De-identified

Coarse

On-device
Big Ideas to Remember

Privacy is about people

Ask the “should” questions

Align data practices with use cases
Building Privacy in Your App

Accessing User Data

Data Stewardship
Building Privacy in Your App

Accessing User Data

Data Stewardship
Accessing Data on iOS
Use Out-of-Process Pickers

Available for Contacts, Camera, and Photos

Will not trigger a permission prompt

Default method for accessing data
Use Out-of-Process Pickers

```swift
let contactPicker = CNContactPickerViewController()

let cameraPicker = UIImagePickerController()
cameraPicker.sourceType = .camera

let libraryPicker = UIImagePickerController()
libraryPicker.sourceType = .photoLibrary
```
<table>
<thead>
<tr>
<th>Protected Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bluetooth Sharing</td>
</tr>
<tr>
<td>Calendars</td>
</tr>
<tr>
<td>Camera</td>
</tr>
<tr>
<td>Contacts</td>
</tr>
<tr>
<td>Health</td>
</tr>
<tr>
<td>HomeKit</td>
</tr>
</tbody>
</table>
Requesting Access

Only what you need
Only when you need it
Only rely on the API for status

Allow “Maps” to access your location while you are using 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
Include Purpose Strings

Required for requesting access

One method for transparency

Explains the reason for a request
Include Purpose Strings

Required for requesting access
One method for transparency
Explains the reason for a request
Unhelpful Purpose Strings

""

"

"true"

"NSLocationAlwaysUsageDescription"

"Advertising"

"This app requires location"

"Used to provide you more relevant content"
Helpful Purpose Strings

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

“We’ll use your location to determine what’s available to you and show you live games, events, and news from your area.”
Helpful Purpose Strings

“This app uses your location to show nearby stops and stations, and allows you to plan trips from your current location.”
Managing Access

Apps should not require access to protected resources
Build fallbacks if user declines access
Verify in case user revokes access
Stay aware of third-party SDKs
Provide ongoing transparency
WiFi Network Information

Now requires AccessWiFiInformation capability

Used to check if an accessory is on the network

Enable only when necessary for your use case

Turning on AccessWiFiInformation will...
- Add the AccessWiFiInformation feature to your App ID.
- Add the Access WiFiInformation entitlement to your entitlements file
Health Records

Accessing Health Records with HealthKit

WWDC18
Differential Privacy
Differential Privacy
Differential Privacy

Differential Send
Accessing Data on macOS
## Protected Resources

<table>
<thead>
<tr>
<th>Location Services</th>
<th>Mail</th>
<th>Camera</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contacts</td>
<td>Messages</td>
<td>Microphone</td>
</tr>
<tr>
<td>Calendars</td>
<td>Safari Browsing History</td>
<td>Automation</td>
</tr>
<tr>
<td>Reminders</td>
<td>HTTP Cookies</td>
<td></td>
</tr>
<tr>
<td>Photos</td>
<td>Call History</td>
<td></td>
</tr>
<tr>
<td></td>
<td>iTunes Backups</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Time Machine Backups</td>
<td></td>
</tr>
</tbody>
</table>
Protected Resources

Access to resources may now trigger a prompt.

Prompts apply to any third-party app process.

Includes apps outside the App Store.

Purpose strings will be required.

“Watch Grass Grow” would like to access your calendar.
Your calendar is used to schedule optimum grass-watching times.

Don’t Allow  OK
Accessing Data on the Web
Storage Access API

Engage with logged-in content from embedded third parties

Including from domains classified as trackers
Storage Access API

1st party cookies
- news.example
- video.example
Request Storage Access

<script>
function makeRequestWithUserGesture() {
    var promise = document.requestStorageAccess();
    promise.then(
        function () {
            // Storage access was granted.
        },
        function () {
            // Storage access was denied.
        }
    );
}
</script>
<button onclick="makeRequestWithUserGesture()">Play video</button>
Request Storage Access

<script>
function makeRequestWithUserGesture() {
    var promise = document.requestStorageAccess();
    promise.then(
        function () {
            // Storage access was granted.
        },
        function () {
            // Storage access was denied.
        }
    );
}
</script>

<button onclick="makeRequestWithUserGesture()">Play video</button>
Request Storage Access

<script>
function makeRequestWithUserGesture() {
    var promise = document.requestStorageAccess();
    promise.then(
        function () {
            // Storage access was granted.
        },
        function () {
            // Storage access was denied.
        }
    );
}
</script>

<button onclick="makeRequestWithUserGesture()">Play video</button>
Storage Access API

1st party cookies
- news.example
- video.example

Request cookies for video.example
Storage Access API

1st party cookies
- news.example
- video.example

Request cookies for video.example
Do you want to allow "video.example" to use cookies and website data while browsing "news.example"?

This will allow "video.example" to track your activity.

[Don’t Allow] [Allow]
Storage Access API

1st party cookies
- news.example
- video.example

Request cookies for video.example
Storage Access API

1st party cookies
- news.example
- video.example

Return cookies for
- video.example
Intelligent Tracking Prevention 2.0

Cookies from domains classified as trackers partitioned immediately

Cookies can’t be used in a 3rd-party context

Cookies purged

0 days

30 days without interaction
Storage Access API

1st Party Context

video.example

3rd Party Context

news.example

video.example
Storage Access API

Days since interaction: 0

First party

video.example
Storage Access API

Days since interaction: 5

- First party
- Third party

website1.example

video.example
Storage Access API

Days since interaction: 10

- First party
- Third party

website2.example

video.example
Storage Access API

Days since interaction: **25**

- First party
- Third party
- Third party
- Third party

**website3.example**

**video.example**
Storage Access API

Days since interaction: 5

- First party
  - 5 Days
- Third party
  - 5 Days
  - 10 Days
  - 25 Days
Storage Access API

Days since interaction: **5**

- First party: 5 Days
- Third party: 5 Days, 10 Days, 25 Days, 45 Days
Building Privacy in Your App

Accessing User Data

Data Stewardship
Data Stewardship

Deletion

Device Tracking

Third-Party Partners

Machine Learning
Deletion
Clean Up Deleted Data

- Recognize data flows going outside your app
- Ensure consistency across systems
- Update data shared with Operating System
  - Siri Shortcuts
  - Notifications
  - Passwords
delete(with:completion:)
deleteAll(completion:)
Notifications
UNUserNotificationCenter

removeDeliveredNotifications(withIdentifiers:)
removeAllDeliveredNotifications()
Passwords

ASCredentialIdentityStore

removeCredentialIdentities(with:completion:)
removeAllCredentialIdentities(_:)

[Image of a key icon]
Device Tracking
You Might Want to Know...

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

Set two bits of data per device

Stored by Apple with timestamp

Persist across reset or erase install
DeviceCheck

Do not rely on unsupported device tracking methods

• Continuing to remove entropy (unique device attributes)
• Continuing to remove functionality being abused to uniquely identify users
Third-Party Partners
Third-Party Code

You’re responsible for all code in your app
Understand data access or transfers
Be complete when giving transparency
Avoid unnecessary requests for resources
Third-Party Vendors

Data flow to 3rd parties from your servers
Know your partners’ data practices
Be transparent about all use cases
Machine Learning
Face ID

Built with privacy-friendly machine learning
Easy to add Face ID authentication to your app
Use the LocalAuthentication framework
ARKit 2

Uses machine learning to model the environment
Create, persist, and share map of environment
Collect this map only if needed for your feature
Use MultipeerConnectivity API for end-to-end encryption
Create ML + Core ML
Create ML + Core ML 2.0

Easier than ever to add on-device machine learning to your app

Train models on your Mac

Evaluate models on your user’s device

Avoid collecting sensitive user data
Privacy Questions for ML
Does my model reveal training data?

Fredrikson et al., Model Inversion Attacks that Exploit Confidence Information and Basic Countermeasures, ACM CCS 2015
Can I infer more about my users than they expected?

Gyroscope → Accelerometer → Speed

[Images of a running person and a bicycle]
Can I infer more about my users than they expected?

Gyroscope → Accelerometer → Speed

- Running
- Cycling
- Wheelchair
Mitigations

Ensure you train on the right data

Keep model complexity proportional to goal
Privacy is about people.
Great features and privacy
Great features and privacy
Summary

Privacy is about people

Ask the “should” questions

Align data practices with use cases
<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Understanding ARKit Tracking and Detection</td>
<td>Hall 1</td>
<td>Thursday 5:00PM</td>
</tr>
<tr>
<td>Privacy Lab</td>
<td>Technology Lab 1</td>
<td>Thursday 5:00PM</td>
</tr>
<tr>
<td>Privacy Lab</td>
<td>Technology Lab 2</td>
<td>Friday 2:00PM</td>
</tr>
</tbody>
</table>