Designing for Privacy

Mark Xue, Privacy Engineer
Julien Freudiger, Privacy Engineer
Designing for Privacy

Mark Xue, Privacy Engineer
Julien Freudiger, Privacy Engineer
“We at Apple can — and do — provide the very best to our users while treating their most personal data like the precious cargo that it is.”

Tim Cook
IDPPC Keynote, 2018
“And if we can do it, then everyone can do it.”

Tim Cook
IDPPC Keynote, 2018
Data Minimization
On Device Intelligence
Transparency and Control
Apple’s Privacy Principles

Security
Apple’s Privacy Principles

- Data Minimization
- On Device Intelligence
- Transparency and Control
- Security
Apple’s Privacy Principles

Data Minimization

On Device Intelligence

Transparency and Control

Security
Apple’s Privacy Principles

- Data Minimization
- On Device Intelligence
- Transparency and Control
- Security
Apple’s Privacy Principles

Data Minimization

On Device Intelligence

Transparency and Control

Security
Privacy and user experience
What’s new in frameworks
Privacy updates
Solving privacy challenges
Privacy and user experience
What’s new in frameworks
Privacy updates
Solving privacy challenges
Sign In with Apple
Sign In with Apple

Apple doesn’t track usage of your app

Only ask for name and email if you need it
dany-4ever@outlook.com
spamvortex@yahoo.com
drogonthegreat1@gmail.com
snowdontknow@yahoo.com
ghostrulez13@gmail.com
jane.appleseed@icloud.com
Sign In with Apple

Hide my email

Contact the user at an email associated with their AppleID

Apple doesn’t retain emails after delivery

Team ID scoped email address

Whitelist of incoming domains or addresses
## Fraud Detection

<table>
<thead>
<tr>
<th>Name</th>
<th>DOB</th>
<th>Contact</th>
<th>Relatives</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jane Appleseed</td>
<td>April 1, 1976</td>
<td><a href="mailto:johnny@apple.com">johnny@apple.com</a></td>
<td>Steve Jobs, Craig Federighi</td>
</tr>
</tbody>
</table>

[View More]
Sign In with Apple
Real user detection

Uses on-device intelligence

Supported on iOS at account creation
Sign In with Apple
Real user detection

Uses on-device intelligence

Supported on iOS at account creation
```swift
func authorizationController(controller : ASAuthorizationController, 
didCompleteWithAuthorization authorization: ASAuthorization){
    if let credential = authorization.credential as? ASAuthorizationAppleIDCredential {
        let realUserStatus = credential.realUserStatus
        switch realUserStatus {
        case .unsupported:
            ...
        case .unknown:
            ...
        case .likelyReal:
            ...
        }
    }
}
```
Allow “Travel Eats” to access your location?
Your location is used to find restaurants around you.

- Only While Using the App
- Always Allow
- Don’t Allow
Allow “Travel Eats” to access your location? Your location is used to find restaurants around you.

- Allow While in Use
- Allow Once
- Don’t Allow
Allow "Travel Eats" to access your location?
Your location is used to find restaurants around you.

- Allow While in Use
- Allow Once
- Don’t Allow
Location Permissions
Deferred Always

Allow "Travel Eats" to access your location?
Your location is used to find restaurants around you.

Allow While in Use
Allow Once
Don't Allow
Location Permissions
Deferred Always

In-app prompt for “Allow Once” or “While in Use

Allow “Travel Eats” to access your location?
Your location is used to find restaurants around you.

- Allow While in Use
- Allow Once
- Don’t Allow
Location Permissions
Deferred Always

In-app prompt for “Allow Once” or “While in Use

iOS generates “Always” events for your app

Allow “Travel Eats” to access your location?
Your location is used to find restaurants around you.

- Allow While in Use
- Allow Once
- Don’t Allow
Allow “Travel Eats” to access your location?
Your location is used to find restaurants around you. If you always allow access, you’ll never miss nearby Top Eats.

In-app prompt for “Allow Once” or “While in Use”

iOS generates “Always” events for your app

“Always” prompt deferred until delivery of first “Always” event
Location Permissions
Always Reminder

Periodic reminders

Once on upgrade to iOS 13

“Travel Eats” has been using your location in the background. Do you want to continue allowing this?
Your location is used to find restaurants around you. If you always allow access, you’ll never miss nearby Top Eats.

Change to Only While Using
Always Allow
Location Permissions

No compatibility breaking API changes

Test for “Allow Once” and “Always” behaviors

Ensure your use of “Always” provides clear user value
Changes to Bluetooth Permissions

User consent required for all CoreBluetooth API’s

Applies to apps linked with any SDK

`NSBluetoothAlwaysUsageDescription` in Info.plist
// Changes to Bluetooth Permissions

import CoreBluetooth

let centralManager = CBCentralManager(delegate: self, options:nil)
//iOS will now prompt the user for access to bluetooth
...

func centralManagerDidUpdateState(_ central: CBCentralManager) {
    let authorizationStatus = central.authorization
    switch authorizationStatus {
    case .notDetermined:
        ...
    case .restricted:
        ...
    case .denied:
        ...
    case .allowedAlways:
        ...
    }
}
// Changes to Bluetooth Permissions

import CoreBluetooth

let centralManager = CBCentralManager(delegate: self, options:nil)

// iOS will now prompt the user for access to bluetooth

func centralManagerDidUpdateState(_ central: CBCentralManager) {
    let authorizationStatus = central.authorization
    switch authorizationStatus {
    case .notDetermined:
        ...
    case .restricted:
        ...
    case .denied:
        ...
    case .allowedAlways:
        ...
    }
}
// Changes to Bluetooth Permissions

import CoreBluetooth

let centralManager = CBCentralManager(delegate: self, options:nil)
// iOS will now prompt the user for access to Bluetooth

... func centralManagerDidUpdateState(_ central: CBCentralManager) {
    let authorizationStatus = central.authorization
    switch authorizationStatus {
    case .notDetermined:
        ...
    case .restricted:
        ...
    case .denied:
        ...
    case .allowedAlways:
        ...
    }
}
macOS Permissions
Access to data

Contacts
Calendars
Reminders
Photos
Full Disk Access
macOS Permissions

Access to data

Contacts

Calendars

Reminders

Photos

Full Disk Access

Desktop

Documents

Downloads

iCloud Drive

Third-party cloud storage

Network volumes

Removable volumes
macOS Permissions
Access to user activity

Camera

Microphone
macOS Permissions
Access to user activity

Camera
Screen recording
Microphone
Keyboard Input Monitoring
macOS Permissions
Automation

Synthetic Input Events
AppleEvents

Advances in macOS Security
WWDC App

Security Lab
Thursday, 2:00
Privacy and user experience
What’s new in frameworks
Privacy updates
Solving privacy challenges
Intelligent Tracking Prevention
Privacy Preserving Ad Click Attribution

Measure ad campaign conversions

Without tracking individual users
Privacy Preserving Ad Click Attribution
Privacy Preserving Ad Click Attribution
Privacy Preserving Ad Click Attribution
Privacy Preserving Ad Click Attribution
Privacy Preserving Ad Click Attribution
Privacy Preserving Ad Click Attribution

NEW
Privacy Preserving Ad Click Attribution
Privacy Preserving Ad Click Attribution

NEW
Privacy Preserving Ad Click Attribution
Privacy Preserving Ad Click Attribution

Clicked on search.example ad for SneakerNet
Privacy Preserving Ad Click Attribution
Privacy Preserving Ad Click Attribution

Made a purchase on SneakerNet
Privacy Preserving Ad Click Attribution

Conversion from search.example to SneakerNet
Privacy Preserving Ad Click Attribution

Conversion from search.example to SneakerNet
Privacy Preserving Ad Click Attribution

Conversion from search.example to SneakerNet
Privacy Preserving Ad Click Attribution

<a adDestination="SneakerNet.example" adCampaignID="55"... >
Privacy Preserving Ad Click Attribution

<a adDestination="SneakerNet.example" adCampaignID="55"... >
Privacy Preserving Ad Click Attribution

<a adDestination="SneakerNet.example" adCampaignID="55"... >
Privacy Preserving Ad Click Attribution
Privacy Preserving Ad Click Attribution

search.example/.well-known/ad-click-attribution/20
Privacy Preserving Ad Click Attribution

CampaignID and ConversionID each limited to 64 possible values

Attribution delayed 24–48 hours to prevent correlation

Attribution sent in ephemeral browsing session

Clicks and Conversions in private browsing are not recorded
Privacy Preserving Ad Click Attribution

Safari Technology Preview 83

iOS 13 and macOS Catalina

Submitted to W3C

webkit.org/blog
Speech Recognition
// Offline Transcription

import Speech

let recognizer = SFSpeechRecognizer()

if recognizer.isAvailableForLocalRecognition() {
    let request = SFSpeechRecognitionRequest(requiresLocalRecognition: true)
}

import Speech

let recognizer = SFSpeechRecognizer()

if recognizer.isAvailableForLocalRecognition(){
    let request = SFSpeechRecognitionRequest(requiresLocalRecognition: true)
}

// Offline Transcription
// Offline Transcription

import Speech
let recognizer = SFSpeechRecognizer()
if recognizer.isAvailableForLocalRecognition(){
    let request = SFSpeechRecognitionRequest(requiresLocalRecognition: true)
}

TestFlight Feedback
Improved TestFlight Feedback

Submit feedback directly from Screenshot UI
Can submit feedback along with crashes
User in control of sharing feedback
Available on iOS 13 with TestFlight 2.3
Privacy and user experience
What’s new in frameworks
Privacy updates
Solving privacy challenges
Only for apps that declare com.apple.developer.networking.wifi-info entitlement

And

- Configured a Virtual Private Network
- Configured a Wi-Fi Network using NEHotspotConfiguration
- Obtained location permission
Notes Field in Contacts

Access to notes field requires entitlement

• `com.apple.developer.contacts.notes`

File a Contacts entitlement request at

developer.apple.com/contact/request/contact-note-field/
Notes Field in Contacts

Access to notes field requires entitlement
• com.apple.developer.contacts.notes

File a Contacts entitlement request at
developer.apple.com/contact/request/contact-note-field/
import UIKit

func application(_ app: UIApplication, openurl: URL, options: [UIApplication.OpenURLOptionsKey : Any] = [:]) -> Bool {
    let sourceApplication = options[.sourceApplication]
    ...
}

Custom URL Schemes

Source Application only if from the same developer
Custom URL Schemes

Source Application only if from the same developer

```swift
import UIKit

func application(_ app: UIApplication,
    openurl: URL,
    options: [UIApplication.OpenURLOptionsKey : Any] = [:]) -> Bool {
    let sourceApplication = options[.sourceApplication]...
}
```
Game Center Player Identifiers

Two new scoped identifiers

- teamPlayerID team-scoped player identifier
- gamePlayerID game-scoped player identifier

Existing playerID is deprecated
Contextual Information

Provide entry points into your apps

- NSUserActivity
- SiriKit INInteraction
Contextual Information

Provide entry points into your apps
- NSUserActivity
- SiriKit INInteraction
Data Stewardship

```swift
delete(with: completion:)
deleteAll(completion:)
```
Privacy and user experience
What’s new in frameworks
Privacy updates
Solving privacy challenges
Machine Learning

Find My

Home
Machine Learning
Machine Learning

Train a machine learning model

• Without collecting sensitive user data
• While personalizing the model to the user
• While improving the user experience
Data
Data Collection
Data Collection

User Data

Random identifiers
Round
Sample
Data Collection

User Data
Random identifiers
Round
Sample

User studies
Diverse set of participants
Ongoing studies
Data Collection

User Data
- Random identifiers
- Round
- Sample

User studies
- Diverse set of participants
- Ongoing studies

External datasets
- Public data sets
- Partnerships
On-Device Training
On-Device Training

Training data

MLMODEL

Cloud
On-Device Training

Training data

MLMODEL

MLMODEL

NEW
Background Tasks API

BackgroundTasks Framework

- BGProcessingTaskRequest
- BGTaskScheduler

Your Background tasks run as long as your app is regularly used
Private Federated Learning
Private Federated Learning
Private Federated Learning

Diagram showing the process of private federated learning, where data is collected on a mobile device and sent to the cloud for training. The trained model is then sent back to the mobile device.
Private Federated Learning
Private Federated Learning
Private Federated Learning
Private Federated Learning
Private Federated Learning
Updates Can Be Sensitive
Updates Can Be Sensitive
Updates Can Be Sensitive
Private Federated Learning

A. Bhowmick et al. Protection Against Reconstruction and Its Applications in Private Federated Learning, 2018
Private Federated Learning

A. Bhowmick et al. Protection Against Reconstruction and Its Applications in Private Federated Learning, 2018
Use Cases

QuickType keyboard

Vocal Classifier for personalized Hey Siri

And more
Machine Learning

Evaluate a machine learning model
• Without collecting user data
• With fast inferences
• Without Internet connection latency
Inference
Inference

Input

Inference
On-Device Inference
On-Device Inference
On-Device Inference
CoreML

Optimized for Apple Neural Engine

Easily convert existing models to CoreML

Expanded coverage of model architectures
Face ID data never leaves the device.
Machine Learning

Find My

Home
Find My
Find devices when they are offline

• While making sure lost devices cannot be tracked
• Without revealing identity of finders to Apple
• Without allowing Apple to know the location of lost devices
• Without compromising all day battery life
iCloud

PubKey 2

Owner

Nearby phone
iCloud

PubKey 2

Owner
iCloud

PubKey 2

Owner
iCloud

PubKey 2

Owner
Apple does not know the location of any offline devices or finders.
Unexpected Bitcoin mining  Cold homes  Failed fridges

Denial of service  Locked homes  Mass surveillance

Intercepted communications  Unexpected recordings

Compromised cameras  Botnets  Ransomware

Cold showers  Loud music  Uncontrollable alarms

Unexpected personal data sharing  Failing dog feeders
Compromised cameras
Home

Allow users to view their security cameras from anywhere

• Without unexpectedly sharing camera videos with others
• Without allowing Apple to access camera content
• While enabling smart camera experiences
HomeKit Secure Videos

iCloud

Owner

Living Room

Kitchen

Bedroom
HomeKit Secure Videos

- iCloud
- Owner
- Living Room
- Smart detection
- Bedroom
- Kitchen
HomeKit Secure Videos

iCloud

Owner

Living Room

Kitchen

Bedroom
Only you can see the video from your camera.
Great features and privacy.
Great features and privacy.
Summary
Summary

Design with privacy in mind
Summary

Design with privacy in mind

Privacy is chance to innovate
Summary

Design with privacy in mind

Privacy is chance to innovate

Share your privacy assurances with your users
More Information

developer.apple.com/wwdc19/708