# ACCESSING PRIVATE DATA

Requesting permission:

Here are several examples of the things you must request permission to access:

1. Personal data, including location, health, financial, contact, and other personally identifying information
2. User-generated content like emails, messages, calendar data, contacts, gameplay information, Apple Music activity, HomeKit data, and audio, video, and photo content
3. Protected resources like Bluetooth peripherals, home automation features, Wi-Fi connections, and local networks
4. Device capabilities like camera and microphone
5. The device’s advertising identifier, which enables app tracking

Here are some high-level guidelines for protecting data:

1. Avoid relying solely on passwords for authentication. Take advantage of other technologies like Touch ID, which lets people authenticate with a fingerprint.
2. Store sensitive information in a keychain. A keychain provides a secure, predictable user experience when handling someone’s private information. (A keychain is an encrypted container that securely stores your account names and passwords for your Mac, apps, servers and websites, and confidential information, such as credit card numbers or bank account PIN numbers.)
3. Never store passwords or other secure content in plain-text files. Even if you restrict access using file permissions, sensitive information is much safer in an encrypted keychain.
4. Avoid inventing custom authentication schemes. If your app requires authentication, prefer system-provided features like Sign in with Apple or Password AutoFill.