



Apple submission to the Senate Economics References Committee's Inquiry on the Influence of International Digital Platforms

Apple welcomes the opportunity to provide input into the Senate Economic References Committee's inquiry into the influence of international digital platforms operated by Big Tech companies.

As the Committee will be aware, many of the topics referenced in the Issues Paper are the subject of consultations, reviews or existing processes, with which Apple is engaged. Apple wishes to provide the Committee with detailed information on Apple's position on privacy, which is one of the areas of interest in the Issues Paper.

Apple considers privacy to be a fundamental human right which means we design all of our products and services to protect it. We intentionally design and build our products to the highest privacy and security standards in the market. Apple enables and values privacy for users beyond mere compliance with legal requirements. The European Union's General Data Protection Regulation (GDPR) and the Australian Privacy Act and its associated thirteen Privacy Principles play an important role in setting a floor for businesses but we believe they should never serve as the ceiling for privacy and data protection.

Apple gives effect to its commitment to privacy with four simple Privacy Pillars:

Data minimisation & On-device processing: Section 1. Our position on privacy is simple. We challenge ourselves to collect only the minimum data necessary to provide a service. In many instances this means that we do not collect data at all via our industry leading commitment to on-device intelligence or where we do collect data we do so using randomised or rotating identifiers that are not linked to a user's Apple ID. And in those cases where it is necessary to collect personal data in order to provide the service such as for the App Store, we are very clear as to what personal data is collected and why.

User control and transparency: Section 2 outlines Apple's commitment to providing users with a clear, easily accessible overview of the processing of their data. We empower our users by giving them the ability to make informed choices about the processing of their personal data.

Data security: Section 3 focuses on Apple's approach to data security. Apple employs advanced technologies to guarantee the security of our users' data across all of our products and services.

1. DATA MINIMISATION AND ON-DEVICE PROCESSING

Apple's commitment to data minimisation reflects a conviction that Apple should only collect the data it actually needs to provide a particular service. Apple collects much less

user data than many other technology companies. Apple does not rely on the tracking, analysis or monetisation of user data.

Apple collects as little user data as possible. Even where the collection of certain limited user data is strictly required to provide a service, Apple strives to collect the data in such a way that it cannot be tied to the user's identity wherever possible. For example, Apple makes use of rotating random identifiers and other privacy-preserving techniques to ensure that we do not have access to individual user data. Apple also leverages on-device intelligence to the fullest extent possible to do as much processing on the device as possible. That means Apple does not have access to that data on its server. It happens all on the user's device.

1.1 Apple collects data only where this is strictly required

Siri

Siri has been engineered to protect user privacy. A user's use of Siri is tied to a device generated random identifier that is not tied to a user's Apple ID. Furthermore, Siri uses as little data as possible to deliver an accurate result. For example, when a user asks a question about an event, Siri uses only the general location of the user to provide suitable results. If Siri is asked to read a message, Siri simply instructs the user's device to read aloud their unread messages. Siri data and user requests are not used to build a marketing profile and are never sold to a third-party.

Safari

Safari is designed to limit the amount of user information collected. Safari has several privacy-enhancing features through which Apple delivers browsing capabilities to our users without asking them to sacrifice privacy in their browsing data. Like many other Apple services, where possible, Safari's privacy protections are designed to process data on device.

Safari was the first web browser to block third-party cookies by default as far back as 2003. In 2017, Apple introduced Intelligent Tracking Prevention ("ITP"), a Safari-integrated feature that uses on-device machine learning to detect, isolate, and block tracking data that websites try to collect and store. In 2019, Apple further improved ITP by adding Fingerprinting Defence that prevents advertisers and data brokers from using the unique combination of characteristics of a device to create a "fingerprint" to track the user online. In order to accomplish this, Safari presents a simplified version of the system configuration to trackers so more devices look identical, making it harder to single one out.

When a user searches using a Private Browsing window, Safari does not save a list of the web pages visited, add typed information to AutoFill, or store the list of downloads and searches in the Smart Search field (though downloaded items remain on the device). This means that users on a shared device are not able to see which sites other users visited, what they searched for, or what they typed into web forms. When in Private Browsing mode, browsing initiated in one tab is isolated from browsing initiated in other tabs.

Location Services

Location Services acts as a safeguard between a user's location data and the apps seeking to leverage this data. This allows users to disable sharing location data with apps altogether and also provides them with a choice to share only approximate location data. When users opt to share only approximate location data, apps have access only to the approximate location — an area of about 26 square kilometres — rather than the precise location. Third parties might be interested to gain greater access to location data but granting such access without allowing the user to make clear and granular choices would undermine end users' privacy.

1.2 Apple avoids identifying individual users

Apple protects users' identities by avoiding collecting data that allows identifying individuals wherever possible. Apple utilises various de-identifying techniques to ensure that information cannot be linked back to an individual. This creates challenges for Apple both in terms of counting end users, but also in terms of obligations that may require it to share information with business users.

Apple also makes use of random identifiers rather than persistent identifiers where possible to better protect user privacy. For example, when a user uses Siri Suggestions, Look Up, Visual Look Up, or types in Search, Spotlight, Safari search, or #images search in Messages, only limited information is sent to Apple to provide up-to-date suggestions. Any information sent to Apple does not identify the user, and is associated with a 15-minute random, rotating device-generated identifier.

1.3 Apple processes users' data on-device

On-device processing is a key tenet of Apple's privacy-by-design architecture: data that stays on device is data that remains entirely under the user's control. With on-device processing, user data is not put on Apple's—or anyone else's—servers. As data stays entirely on device under a user's control, Apple is not able - even if we wished to do so - to share such data with third parties. That is a decision that is entirely for the user. Over the years Apple has deliberately increased the use of on-device processing. This was a conscious business decision taken to protect ever increasing amounts of users' personal data. Apple processes personal data on the device for several apps and features, thereby minimising the amount of data available to Apple.

Siri

Siri has always processed user requests in a non-identifiable manner by leveraging device-generated identifiers. Apple has further enhanced Siri's privacy protections over the years by transitioning more of Siri's processing away from Apple's servers to the user's device itself. This enables Siri to carry out many requests mostly with on-device data. For example, Apple launched on-device speech recognition to avoid obtaining audio recordings in iOS 15. This means that the audio of users' Siri requests are processed directly on the user's iPhone by default.

Face ID and Touch ID

Face ID and Touch ID data is converted into mathematical representations that are encrypted and protected by the iOS device's Secure Enclave. The Secure Enclave is a dedicated secure subsystem integrated into the main processor on Apple's devices. The Secure Enclave is isolated from the main processor to provide an extra layer of security and is designed to keep sensitive user data secure even when the application processor kernel becomes compromised. This data therefore never leaves the user's device and is not synced across a user's devices, using iCloud.

Location data

Although a user's iPhone keeps track of the user location to provide personalised services (e.g., predictive traffic routing) when the user has turned on Location Services, the data is encrypted and stored only on the user's device. Security best practices are integrated to protect data.

Health data

Health data is encrypted and stored locally in HealthKit, a purpose-engineered, on-device storage mechanism that protects the user's privacy in respect of this especially sensitive data. Encrypted, on-device storage ensures that an app can access this information only when the user has permitted it to do so. If the user does back up the information to iCloud and enabled the two-factor authentication, the data is then end-to-end encrypted such that neither Apple nor any third party can access it.

2. USER CONTROL AND TRANSPARENCY

Apple provides features to empower our users to easily control and make informed choices about the processing of their data.

2.1 Users are in control of data access

Apple users value the just-in-time prompts managed by iOS and iPadOS which allow them to make decisions as to whether to provide access to their data such as photos, contacts and calendar in a clear and efficient manner. The examples below illustrate how Apple has implemented the general principle of our users' control over their data.

App Tracking Transparency Framework

App developers need to receive the user's permission through the App Tracking Transparency Framework in order to track them across apps and websites or access their device's advertising identifier. Tracking in this instance refers to linking user or device data collected from an app with user or device data collected from other companies' apps, websites, or offline properties for targeted advertising or advertising measurement purposes. Tracking also refers to sharing user or device data with data brokers. If the user has not granted permission to this tracking, the relevant app will not be able to access any user data. Users can change their preference for any app or prevent apps from asking this permission entirely. This applies across all apps on the device and ensures that, similar to Apple's apps, third-party apps do not track end users' data without them being informed and in control of the process.

Personalised Ads

Apple gives users the option to choose whether to receive targeted ads. Such ads are provided through Apple Search Ads on the App Store and in News. They are provided by linking data to the device-generated and random identifier. Apple prompts all end users to choose whether or not to agree to receive Personalised Ads on the App Stores. Approximately 80% of the end users have chosen not to receive personalised ads.

Access Permissions

Apps may request access to features such as a user's location, contacts, calendars, or photos. The App Sandbox provides protection to user data by limiting an app's access to resources requested through entitlements. Users receive a prompt with an explanation the first time a third-party app wants to use this data, allowing them to make an informed decision about granting permission. Even if a user grants access once, this can be changed at any time in Settings. In addition, no app can access the microphone or camera without the user's permission. In iOS 14 and iPadOS 14 or later, when an app uses the microphone or camera, the user's device displays an indicator to let the user know it is being used — whether the user is in the app, in another app, or on the Home Screen. In addition, the Control Center shows the user if an app has recently used the microphone or camera.

2.2 Users can make informed choices

A user, when first interacting with an Apple product or feature, is presented with service-specific information. This information describes the data collection and use practices for the specific product or feature, creating a layered privacy notice structure. This ensures that users have an effective choice and any consent to data use on Apple products is fully informed.

The below examples illustrate how Apple provides users with meaningful information regarding the processing of their personal data, allowing them to take steps to control and limit the extent of such processing.

Data & Privacy Icon

Apple holds itself to a high standard. Apple's Data & Privacy Icon is presented to users when first interacting with any Apple product or feature that processes user data. The icon links to more detailed on-screen information and the more detailed service-specific privacy information which reflects the privacy practices of each service and feature. These are available to users subsequently on their devices and at any time at <https://www.apple.com/legal/privacy/data>. This allows Apple to have transparent and easily accessible information for end users to understand how their personal data is collected, processed and disclosed

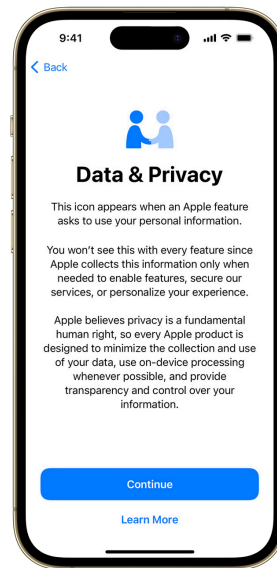
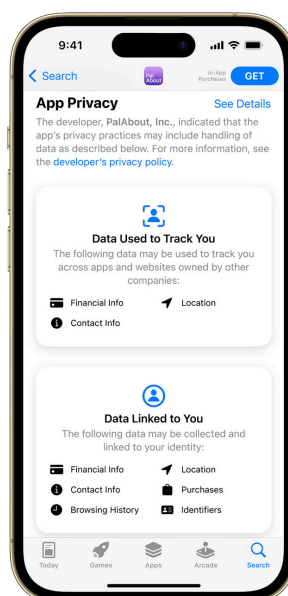


Figure 1 - Display of the Data and Privacy Icon on the iPhone

Privacy Nutrition Labels

Product pages on the App Stores feature a section that provides self-reported summaries prepared by developers of some of their privacy practices in a simple, easy-to-read label. This shows how developers are collecting and using users' data, including information like a user's location, browsing history, and contacts. The same applies to Apple's own apps. This is part of Apple's industry leading, ongoing work to increase transparency and control over users' data. Apple will continue to update this feature and work with developers to ensure that users can make informed choices.

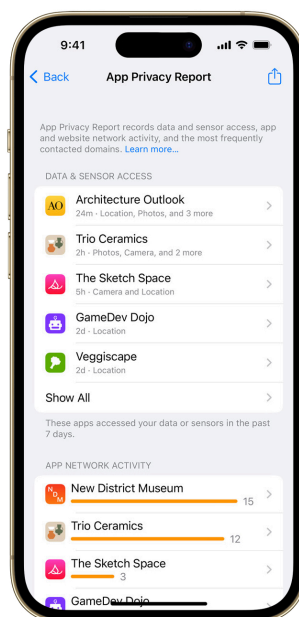
Figure 2 - Display of the Privacy Nutrition Labels on the iPhone



App Privacy Report

The App Privacy Report records encrypted data on device and sensor access, app and website network activity, and the most frequently contacted domains. Through this report, users are able to see how often their location, photos, camera, microphone, and contacts have been accessed by apps during the last seven days as well as which domains apps have contacted. Users therefore have full and easy visibility into the ways apps use the privacy permissions a user has granted them, as well as their respective network activity. Together with Privacy Nutrition Labels, this feature provides users with a complete picture of how the apps, including Apple's apps, treat user privacy.

Figure 3 - Display of the App Privacy Report on the iPhone



SECURITY

Security, data protection, and other integrity considerations are explicitly required by privacy laws such as the Privacy Act.

3.1 Security is a core design principle

Every Apple device combines hardware, software and services designed to work together for maximum security and a transparent user experience in line with Apple's policy to keep our users' data safe. Apple employs a combination of a wide range of market-leading hardware, system, application, services and network security measures, as outlined in the comprehensive [Apple Platform Security paper](https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf).¹

3.2 Keeping data safe through encryption

Apple uses encryption standards that are robust against current crypto-analysis techniques and are implemented through well-maintained software to keep users' data

¹ https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf

safe in transit and at rest. This is consistent with some of the goals of the DMA, to preserve end user security, including end-to-end encryption (cf. Articles 7(3) and 7(4)).

End-to-end and user-controlled encryption

Apple relies on end-to-end encryption to protect particularly sensitive data (e.g., Safari History, Siri information) when the user decides to rely on two-factor authentication which 95% of our users now do. When the user opts in, Apple is not able to decrypt the content and has no access to such encrypted content. In addition, Apple has rolled out Advanced Data Protection² that expands the scope of data that users can protect through end-to-end encryption, now also including e.g., iCloud Back-up, Notes and Photos.

Apple also protects the content of conversations between users using FaceTime or iMessage through end-to-end encryption. In relation to iMessage, Apple protects the privacy of the content shared by end users in iMessage through end-to-end encryption, which limits the collection of data to the minimum necessary for the provision of the service. For instance, to facilitate the exchange of the encrypted keys, users only provide Apple with a "handle" to identify themselves, such as a phone number or email address. Apple does not have access to the content of conversations due to end-to-end encryption. Apple does not provide advertising or sponsored content on iMessage. Apple also protects the content of conversations between users using FaceTime through end-to-end encryption. Apple does not have access to the content of FaceTime audio or video calls. The only information collected in this regard is that a certain user tried to initiate a call with another user.

Data-at-rest and data-in-transit encryption

Where no end-to-end encryption is used, Apple deploys multiple layers of protection, including encryption of data-at-rest and in-transit. In particular, this applies to a number of services on which the content is encrypted when it is transferred and when it is stored on Apple servers. Apple recently released Security Keys, which strengthens Apple's existing two-factor authentication by allowing end users to make use of third party hardware security keys in one of two factors required for authentication for Apple ID.

Files on personal devices

With regard to files on personal devices, Apple has deployed user-controlled encryption to limit access to such devices. iOS and iPadOS devices use a file encryption methodology called Data Protection while the data on Mac computers is protected with a volume encryption technology called FileVault.

3.3 User security on App Stores

Apple is dedicated to protecting our users from malware and keeping our different App Stores safe. To do this, Apple takes sensible precautions with regard to third party apps, as further described below. Maintaining and building up these protections is and will continue to be a critical aspect of the integrity of Apple's operating systems and the devices running them.

² <https://support.apple.com/en-us/HT212520>

App Sandbox

The App Sandbox provides protection to system resources and user data by limiting a developer's app's access to resources requested through entitlements. This creates secure silos to protect the data of end users across the device.

Developer verification

To develop and install apps on iOS or iPadOS, developers must register with Apple giving their real-world identity. This ensures that apps on the App Stores are submitted by identifiable persons or organisations and deters the creation of malicious apps. Apple also ensures that iOS native apps come from known developers that have joined Apple's Developer Program and have agreed to follow the Developer Program License Agreement, including its terms and conditions related to the privacy and security of user data. Apps must also follow the App Store Review Guidelines. Before offering their apps on the App Stores, developers must also go through an app review process, through which Apple reviews compliance with those rules.

3.4 Keeping users' data safe by design and through innovation

Users expect Apple to engineer our products with privacy in mind from the ground up, to react quickly to changing security threats and to constantly develop new features and ways to keep users' data safe. A few examples are set out below.

Apple Wallet

Apple Wallet takes full advantage of the privacy and security built into iPhone and Apple Watch. When or where a person uses their cards, passes or keys in Apple Wallet, these are never shared with Apple or stored on Apple servers, and credentials are securely stored inside the Secure Element of supported devices. The Secure Element hosts specially designed applets to securely manage and store access credentials, ensuring that they cannot be extracted.

Secure software updates

Apple regularly releases software updates to address emerging security concerns. The update process uses system software authorisation to check that only copies of operating system versions that are actively being signed by Apple can be installed on iOS and iPadOS devices, or on Mac computers with the Full Security setting configured as the secure boot policy in Startup Security Utility. With these secure processes in place, Apple can stop signing older operating system versions with known vulnerabilities and help prevent downgrade attacks.

iMessage Contact Key Verification

Apple is introducing a new feature allowing users that opt in to be alerted in case of a security concern that prevents the verification of the identity of the person they are communicating with in a secure manner.

Apple welcomes further engagement with the Committee.