Apple Pty Limited

Submission to the Digital Platform Services Inquiry (March 2024 Issues Paper)

The Australian Competition and Consumer Commission (**ACCC**) has invited submissions from interested stakeholders on the matters raised in the Issues Paper for the forthcoming Digital Platform Services Inquiry (**DPSI**) report on the competition and consumer issues arising from the data collection, storage, supply, processing and analysis services supplied by data brokers (**Issues Paper**).

Apple welcomes the opportunity to provide this submission as part of the ACCC's public consultation.

Apple considers it to be an important responsibility of digital platform services providers to protect consumers from unwanted data collection, storage and processing practices.

Apple's own commitment to privacy is implemented through a number of core principles that are applied consistently to: (a) collect only the minimum data necessary to provide a service in ways that de-link users from their identity through randomised or rotating identifiers wherever possible; (b) collect no data at all via Apple's industry leading on-device intelligence that process data on users' devices wherever possible; (c) where it is necessary to collect personal information provide user control and transparency through a clear, easily accessible overview of the processing of data; and (d) implement advanced technologies to guarantee the security of our users' data across all of our products and services. User security, platform security, data protection and other considerations (e.g. app integrity, end to end encryption) are all reasonable expectations of users and in many cases are specific requirements covered by privacy laws such as the Privacy Act (other than for example device security and on-device processing).

A. Apple provides users with the means to limit the collection of their data by third parties, and welcomes measures to limit or restrict the monetisation of consumer data by third parties

1. As the ACCC has noted in its Issues Paper, many consumers are not aware of how or when their information is being collected by businesses, or how or what that information is being used for.[1] The protection of users' privacy and security is integral to Apple's business model. At Apple, privacy is a fundamental human right, and we design and build out products to the highest privacy and security standards in the market, to protect it.

2. Apple welcomes measures to limit or restrict the monetisation of user data by all stakeholders, particularly with respect to data which is collected without the user's knowledge and

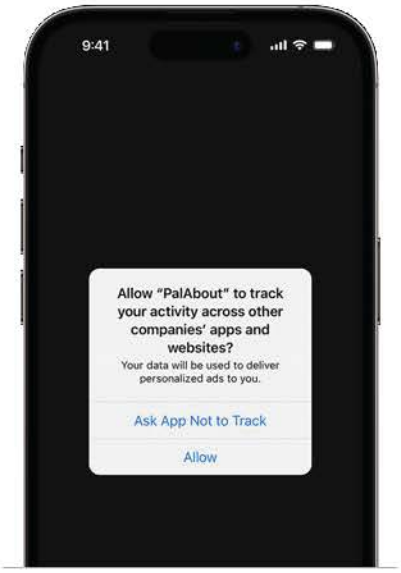
[1] Issues Paper p 3.

permission. Apple provides various mechanisms to ensure user data is private and secure, and enables users to manage how their own data is shared with third-parties.

3. Specifically, with respect to the collection of data by third-parties, Apple ensures that users are given an effective choice regarding the collection of their data (or to limit its collection, should they wish to do so) and are protected from surreptitious data collection practices by those third-parties, by:

(a) **requiring that all apps available on the App Store are vetted through Apple's rigorous App Store Review Process.** The App Store Review Process is focused on ensuring Apple delivers on its promise that apps are held to a high standard for privacy and security. iOS is widely acknowledged as the most secure operating system in the market. User trust in the App Store is critical to Apple's business model - the more users trust their mobile device and the App Store, the more they are open to downloading and discovering apps, and the more that app developers benefit. The protection of users and developers alike from fraud, malware, and unwarranted intrusion into their privacy is critical because devices such as iPhones hold information regarding a user's everyday life and so could offer access to a trove of personal data — data that unscrupulous actors could seek to collect or exploit.

(b) **implementing the App Tracking Transparency feature to help users to become aware of when all apps on Apple devices, including Apple apps, may seek to collect their data for tracking purposes or for sharing with data brokers and enable users to withhold consent for those apps to do so.** All apps available on the App Store can only track a user's use of other apps and websites or access the device's advertising identifier (**IDFA**) with the express permission of the user, given via the App Tracking Transparency Framework. "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. Where an app seeks to track user data using the IDFA, the App Tracking Transparency Framework requires the app to display a prompt requesting the user's permission. A developer is also required to call the prompt if it wishes to track the user through any means even if they don't intend to use the IDFA such as the user's email address. An example of the prompt is below:



The app developer can customise the smaller text in the prompt to explain why the app is asking to track the user's activity. The developer can also explain the prompt in a prior screen if they wish and can ask the user to change their preference later. This is the same behaviour as all other privacy protected data classes on user iOS and iPadOS devices. The user can also visit the app's product page in the App Store for more details about how the app developer uses data using the privacy nutrition labels that we introduced in December 2020.

The user can then tap Allow or Ask App Not to Track. Importantly, the user can still use the full capabilities of the app, regardless of whether the user allows the app to track activity.

If the user chooses Ask App Not to Track, the app developer is prevented by the operating system from accessing the IDFA.

That is, if the user has not granted permission, the relevant app will not be able to access the IDFA and by policy is not permitted to access any data for tracking purposes.

The app tracking section in Settings[2] also lets users easily see to which of their apps they have given permission to track their activity across third-party apps, so they can change their preferences and disable apps from asking in the future.

The App Tracking Transparency Framework also applies fully to Apple apps. Apple itself does not engage in tracking consumers across third party apps in the provision of Apple-delivered advertising. Therefore, unlike third-party advertising service providers, Apple does not need to prompt users for permission to track because it does not engage in this practice. Apple simply does not track users in this way;[3] and

(c) **giving users the ability to choose whether apps can access user data.** Apps may request access to user data 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 an app wants to use this data, allowing them to make an informed decision about granting permission. Even if a user grants access, 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.

4. Beyond App Tracking Transparency, Apple also provides a significant range of additional privacy and security features that ensure users can make informed decisions to limit the data that is collected by third-parties through apps on users' devices, such as:

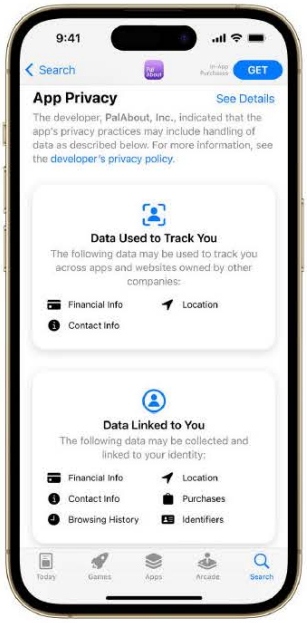
(a) **Privacy Nutrition Labels.** A developer entered section on each product page on the App Store that provides consumers a clear and easy-to-understand overview of a developer's key privacy practices, including data collected by the developer and how data may be used to track users. This is part of 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. All Apple apps comply with the requirements in relation to

---

[2] As ava ab e on Phones under Pr vacy & Secur ty > Track ng.

[3] For more nformat on regard ng App e's App Track ng Transparency feature, see https://support.app e.com/en au/HT212025.

Privacy Nutrition Labels also. The following image shows the display of the Privacy Nutrition Labels on the iPhone:



(b) **End-to-end encryption.** Apple relies on end-to-end encryption to protect particularly sensitive data (eg, Safari History, Siri information) when the user decides to rely on two-factor authentication - which 95% of Apple's users do. Apple is not able to decrypt, and has no access to such encrypted content. Advanced Data Protection has now also been rolled out, which expands the scope of data that users can protect through end-to-end encryption, to include other features such as iCloud Back-up, Notes and Photos.

(c) **Differential Privacy.** Apple transforms certain user personal data before it ever leaves the device. In so doing, Differential Privacy masks the user's personal information and prevents the personal information from being reproduced. When a user authorises an app to continually access their location data, they will be periodically reminded when that app uses the permission or changes its use.

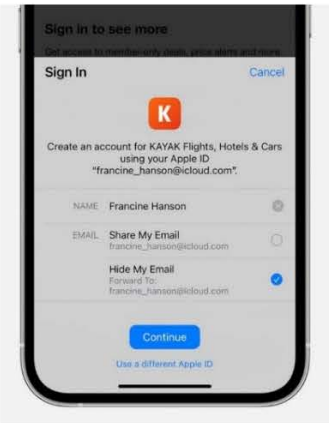
Apple also protects the content of conversations between users using FaceTime or iMessage through end-to-end encryption. In relation to iMessage, Apple protects the privacy of the content shared by end users in iMessage through end-to-end encryption, which limits the collection of data to the minimum necessary for the provision of the service. Apple does not have access to the content of conversations in transit 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 user information collected is that a certain user tried to initiate a call with another user.

(d) **Sign in with Apple (SIWA).** SIWA is a fast, easy and more private way for users to sign in to participating third-party apps and websites using their existing Apple ID login details. Apple built and designed SIWA from the ground up to respect users' privacy, and to help users keep in control of their personal information. If a participating third-party app or website asks users to provide their name and email address, Sign in with Apple automatically fills in the information from the user's Apple ID. Using Apple's **Hide My Email** service, users can keep their personal

email address private and hidden from third-party apps, websites and more. Hide My Email is built in to Sign in with Apple and iCloud+.

Hide My Email generates unique, random email addresses that automatically forward messages to users' personal inbox. Each randomised address is unique to a particular user, who can read and respond directly to emails sent to these addresses while their personal email address is always kept private. Apple does not read or process any of the content in the email messages that pass through Hide My Email, except to perform standard spam filtering required to maintain Apple's status as a trusted email provider. All email messages are deleted from Apple's relay servers after they are delivered to users, usually within seconds.

The following image shows Hide my Email as an optional feature available to users during the SIWA sign up process for a specific app or website:



For more information regarding SIWA, see https://support.apple.com/en-au/HT210318.

(e) **Location Tracking Notifications.** Apple believes that users have a right to know when an app uses their location data before a user decides to share that data indefinitely. Users know when their location data is being accessed by an app, and gives users more control over whether or not they wish to share that data.

(f) **Mail Privacy Protection.** Mail Privacy Protection hides your IP address, so senders can't link it to your other online activity or determine your location.

5. For more information regarding the various privacy features that Apple provides to users minimise the data that third-parties can access, see Apple's Privacy Features: https://www.apple.com/au/privacy/features/

B. Apple itself limits the extent of data it collects from users and has designed its devices to enhance user privacy and security

6. Apple's commitment to data minimisation is reflected in its conviction that Apple should only collect the data it actually needs to provide a particular service. For this reason, Apple has intentionally designed, and continues to innovate, its devices to ensure that users' privacy and security are prioritised and ensures that it collects much less user data than many other technology companies. Unlike many other technology companies and data brokers, Apple does not rely on the tracking, analysis or monetisation of user data for its business - rather, Apple relies on the trust that its users have instilled in its devices.

Apple's devices are designed to minimise the volume of data that ever leaves the device

7. Apple's devices themselves are designed to protect users' privacy and security and limit the data that leaves their device. Apple is a product company and does not seek to monetise user data. These core principles are reflected in innovations across Apple devices.

8. With the iPhone X, Apple launched the A11 Bionic Chip with the Secure Neural Engine. The Secure Neural Engine is integrated into the Secure Enclave - a dedicated secure subsystem in Apple devices designed to keep sensitive user data separate and secure - and powers machine learning algorithms that provide on-device intelligence and minimise the amount of data leaving the user's device. On devices with Face ID, the Secure Neural Engine converts 2D images and depth maps into a mathematical representation of a user's face.

9. Face ID and the Secure Enclave also form critical aspects of the technical architecture of Apple Pay and Apple Wallet, which is specifically designed to protect consumers when making payments - whether at a Point of Sale or on-device.

10. 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.

11. On Apple Pay, consumers use biometric authentication (by way of Face ID or Touch ID) or their passcode to authorise payments via on-device-only processing. Full card numbers are not stored on the consumer's device or on Apple servers. Instead, a unique proxy Device Account Number (or Token) is created, encrypted, and then stored in the Secure Element. This unique Device Account Number is encrypted in such a way that Apple cannot access it. At the time of transaction, the Apple device transmits both the Token and a single use "dynamic cryptogram" that is unique to each transaction and validated by the payment network. Unlike other mobile payment providers, Apple believes that using Apple Pay does not require users to sacrifice privacy for the sake of security — they can have both in equal measure.

Apple collects data only where the user has received clear and unambiguous information and where it is strictly required for the functioning of its devices and apps

12. Apple collects as little user data as possible. For example, further to the features Apple offers to users aimed at limiting the collection of data by third parties (as explained above), Apple:

    (a) **gives users an additional privacy choice related to Apple's own limited data collection practices across a limited number of first party apps** – a choice that third parties do not give users. As this is an additional consumer choice about the use of their data, Apple proactively presents users with a more prominent, unavoidable option to choose between Personalised Ads On or Off for Apple-delivered advertising.[4] This choice screen is presented upon launch of the App Store or of Apple Stocks or Apple News in Australia and informs users as to the purpose of Personalised Ads and its privacy practices, so that the user can decide whether to turn on or off Personalised Ads. Approximately 80% of the end users have chosen not to receive personalised ads;

    (b) **when users choose to have personalised advertising, relies exclusively on a limited amount of first-party data such as account information like gender, age range, address, downloads purchases and subscriptions for Search Ads advertising.**. Apple's advertising platform does not track users, meaning that it does not link user or device data collected from our apps with user or device data

[4] As ava ab e on Phones under Pr vacy & Secur ty > App e Advert s ng.

collected from third parties for targeted advertising or advertising measurement purposes, and does not share user or device data with data brokers.[5] Ads are only served to minimum cohort sizes of 5000 users meaning microtargeting is not possible and Apple has designed its ads serving such that Apple does not know what ads an identifiable user has received or interacted with.

By contrast, most major advertising platform companies — including Meta and Google — do not offer users a choice of disabling the use of first-party data for targeted advertising. And those that do offer such a choice bury it beneath a cumbersome process involving numerous settings screens. Apple is once again at the forefront, by expressly and unavoidably prompting users for permission to use first-party data to deliver Personalised Ads; and

(c) **ensures that users interacting with any Apple product or feature are aware of how their personal data is collected, processed and disclosed through the display of the Data & Privacy icon and associated privacy information.** Apple's Data & Privacy icon is presented to users when first interacting with any Apple product or feature that processes user data. The Data & Privacy 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. The following image shows the display of the Data & Privacy icon on iPhone:[6]

13. Apple will otherwise only collect user data where it is strictly required for the functioning of the users' apps and devices. For example:

(a) **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

[5] See further https://www.app e.com/au/ ega /pr vacy/data/en/app e-advert s ng/.

[6] See further https://www.app e.com/au/pr vacy/contro /

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.

(b) **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.

(c) **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.

The limited data collected by Apple is done in such a way as to maximise the privacy and security of its users

16. 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 it does not have access to individual user data.

17. 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.

18. Random identifiers are also used 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.

19. Apple also leverages on-device intelligence to do as much processing on the device as possible. 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.

20. 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. For example:

    (a) 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.

    (b) **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 isolated from the main processor, never leaves the user's device and is not synced across a user's devices, using iCloud.

    (c) **Location data** is encrypted and stored only on the user's device.

    (d) **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.

21. For more information regarding the limited data collected by Apple, see Apple's Privacy Policy, available at https://www.apple.com/au/legal/privacy/en-ww/ and Apple's Privacy Nutrition Labels, available at https://www.apple.com/au/privacy/labels/.