Arianne Sabarre & Junki Yoshimura

The Data Defender

Be in control of your own personal data

The Data Defender

Arianne Sabarre & Junki Yoshimura

Over the last decade, the **integration of technology and electronics** into daily life has become increasingly prevalent. As a result, data brokers can sell such information to third-party businesses as smartphones have access to their users' **private information**. So, what is Apple doing to safeguard their consumers' data, and how does this influence marketing?

When an individual installs an app on their smartphone, companies do not have access to typical browser cookies that enable them to track their users. Instead, third-party analytics and advertising organisations employ **device identifiers** to track the numerous applications used in a system.

Trackers are often embedded into third-party code that developers use to build mobile apps. These apps frequently depend on third-party services to optimise user experiences, such as social network integration and bug reporting. Moreover, developers monetise apps by selling user information for specified advertising. This gives data brokers the ability to **collect, sell,** and **license** personal data.

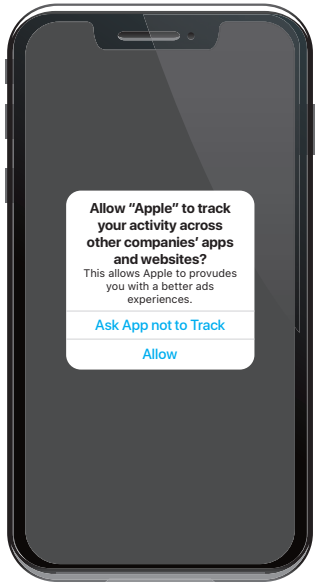


Fig. 1 *AppTrackingTransparency alert notification*

Age, contact information, purchasing patterns, health data, and **internet activity** are among the types of information data brokers may gather. Users are oftentimes unaware their data is being harvested by third-party services. However, this changed in April 2021, when Apple introduced the **AppTrackingTransparency** (ATT) framework in the iOS 14.5 update.

Since the release, all apps have been required to utilise the ATT framework as an app cannot be added to the App Store if the app tracking policy is not correctly implemented. The user's data cannot be monitored unless they have given consent and been informed on how their data will be used. This enables general users to understand how much data mobile apps collect.

The ATT framework allows for a **digestible front-end design** that is easy to understand for general iPhone users. Apple ensures app experiences, the reasoning of gathered personal data, and how the security will be used to protect private information. In ATT, Apple has standardised their

terminology for user data to guarantee that all developers use similar language.

The users' privacy should be a fundamental right, and Apple's ATT framework provides this. **'Allow apps to monitor you or not?'** is a direct question that offers the consumer control over how mobile apps use and share their private information. As a result, a major benefit of ATT is that iOS users are now aware that their data is being monitored and may take measures to preserve their confidentiality.

As marketers, the target segment audience would be **Android** and **Apple users**. The iOS release has an impact on Apple users, whilst Android devices are unaffected. Facebook will be able to track their data throughout the internet in any case. Because the data gathered on iOS will be insufficient, it may be ideal to deal only with Android clients or segmenting campaigns by device. In this case, Facebook will be categorised as the **digital marketing sector**.

Limit Ad Tracking (LAT) is an iOS tool that allows users to consent to have their identity for marketers (IDFA) traced, **restricting the amount of data** that advertisers can access from their devices. Digital marketers will find it **increasingly difficult** to target their campaigns on advertising networks due to the combination of both ATT and LAT. They can only gather limited information about user activity as it is not as detailed as what has been used in the past.

As an example, consider the Facebook Audience Network. Facebook captures a large capacity of personal data across its multiple businesses and sells it to marketers. Advertisers may use this granular data to target adverts to the users that are most likely to visit them. However, since the inauguration of ATT, **Facebook can no longer access data** acquired from untracked Apple devices other than what can be viewed inside their ecosystem.

Thus, with the publication of the ATT framework, Apple has chosen a position that disadvantages the digital marketing sector, but ultimately **maintains the confidentiality of their consumers**. The accessibility of ATT's interface is more crucial to iOS users than unique and personalised marketing.

Share of active users who allow app tracking

At a weekly rate of mobile users worldwide

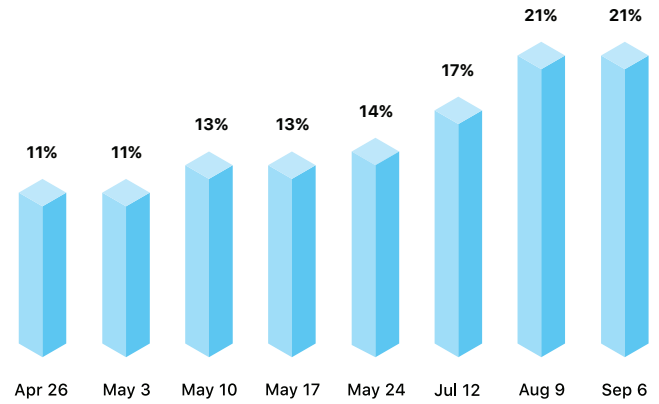


Fig. 2 *Global share of users who allow app tracking*

References:

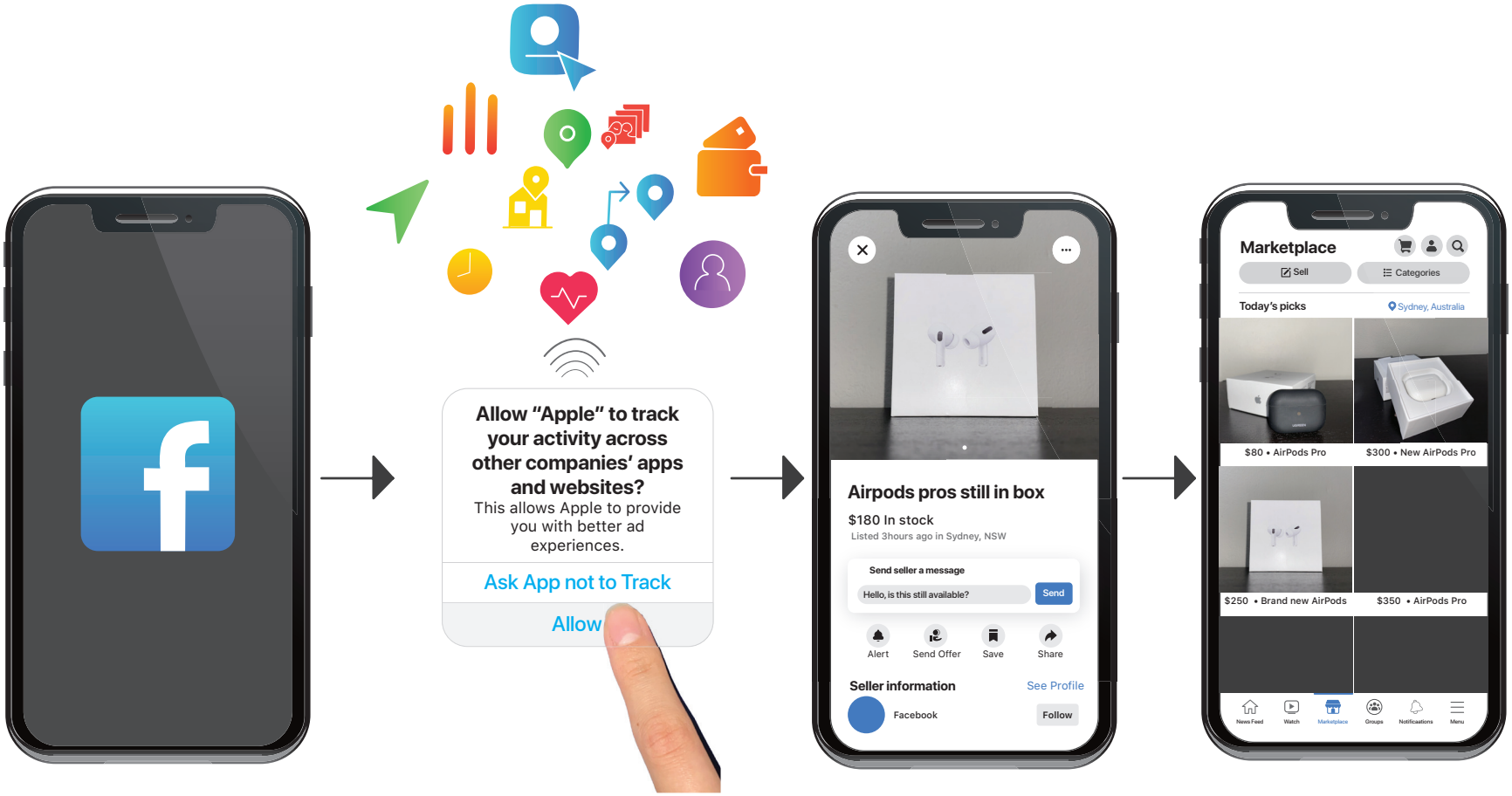
Klosowski, T. (2021, May). We Checked 250 iPhone Apps-This Is How They're Tracking You. The New York Times Wirecutter. https://www.nytimes.com/wirecutter/blog/how-iphone-apps-track-you/

Gartenberg, C. (2021, April). Why Apple's new privacy feature is such a big deal. The Verge. https://www.theverge.com/2021/4/27/22405474/apple-app-tracking-transparency-ios-14-5-privacy-update-facebook-data

Vungle. (2021). What is App Tracking Transparency (ATT) and How Does It Affect Mobile Marketing? https://vungle.com/blog/app-tracking-transparency-att/

Hoppner, T. & Westerhoff, P. (2021). Privacy by Default, Abuse by Design: EU Competition Concerns About Apple's New App Tracking Policy. Social Science Research Network. http://dx.doi.org/10.2139/ssrn.3853981

How does ATT work?



Third-Party Services are embedded into the code of apps such as Facebook.

ATT framework enables the user to decide whether they want to share their data with third-parties.

If the user gives consent, their data such as purchase patterns can be accessed by the third-party services.

The user's data is collected and used to provide targeted ads. This will pop up in areas including their Facebook feed.

Fig. 3 *Example of how AppTrackingTransparency works*