AN EXPLAINER: WHAT IS IDENTITY AND WHY DOES IT MATTER?

iab. sea+india
REGIONAL IDENTITY COUNCIL

Authors:
Alvin Liong, ilmuOne Data
Darshan Radia, Dentsu International
Samantha Pearlson, The Trade Desk
Tina Pang, Twitter
Vasuta Agarwal, InMobi
Hemant Menon, Dentsu International

Executive Summary

Identity in the world of digital advertising is the ability to identify a unique user online, allowing advertisers to reach those users for marketing of their products and services. It forms the basis for all digital advertising activity from user targeting to ROI measurement of media spends.

However, there have been and continue to be multiple changes in the ecosystem.

With Apple's App tracking Transparency framework and Google's planned deprecation of third party cookies, the world of identity is fast-changing.

In this article, we will talk about some of these changes and their impact on consumers, advertisers and other players in the ecosystem. Later in the article, we also cover aspects around what advertisers can do to deal with some of these changes; for example, building consent management platforms for getting opt-in user data, working with universal ID solutions etc.

Finally we share an assessment of impact stemming from the loss of identifiers across the ecosystem, from consumers and advertisers, to publishers and platforms, and what each stakeholder can do to better prepare themselves for the new user-first privacy-compliant world that we are stepping into.

Latest developments in Mobile privacy space

With the iO5 14.5 update in April 2021, there are multiple user privacy related changes that have been rolled out. These will have a big impact in the way advertisers think of their mobile marketing campaigns in the Apple ecosystem when it comes to aspects like targeting , measurement, efficiency management etc. On the consumer side, it gives full control back to the user when it comes to sharing their personal data with each app through an opt-in/ opt-out mechanism.

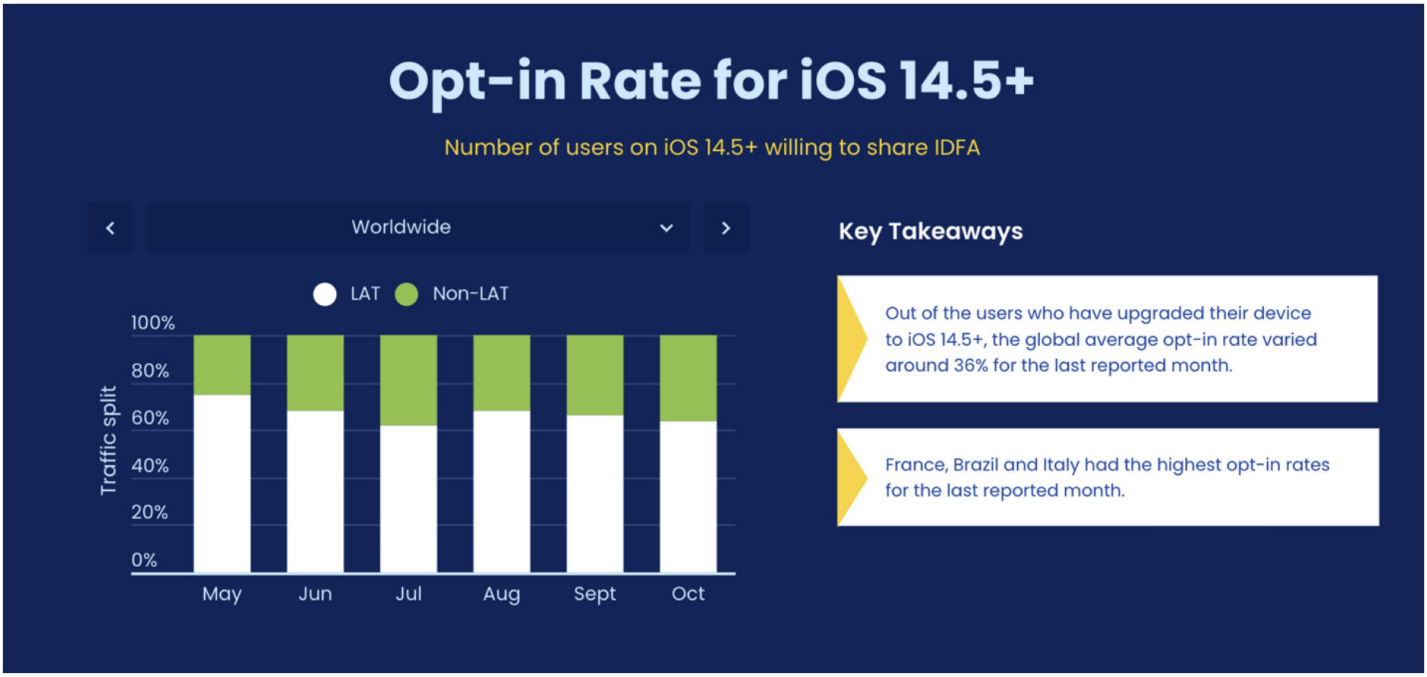
IDFA changes & impact

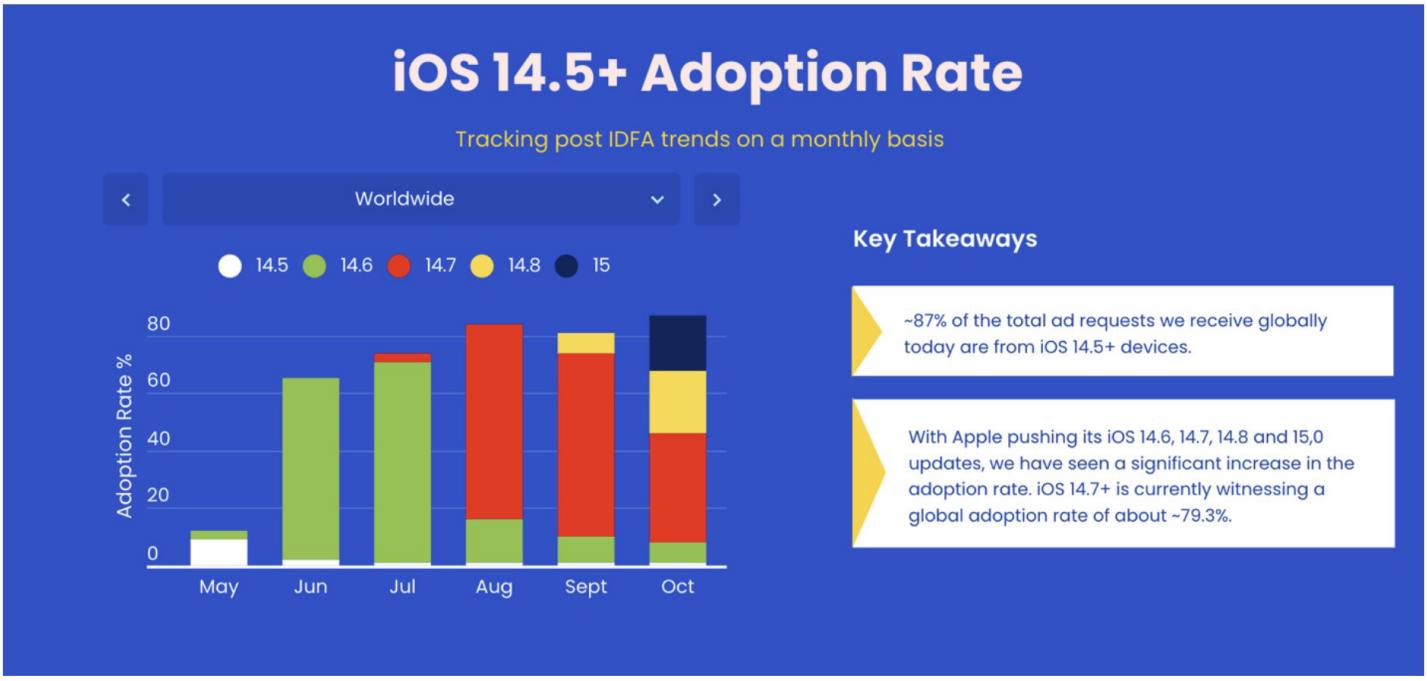
Apple enforced its App Tracking Transparency (ATT) framework in April 2021 with the release of iOS 14.5 and subsequent versions, after suffering a similar delay to Google's 3rd party cookie update, with initial launch planned for the June 2020 release.

So, what does this mean for the iOS advertising ecosystem?

This means app publishers now need to get users' permission before tracking their data across other apps or websites. With these changes, IDFAs will be available to advertisers for marketing purposes only for users who explicitly opt in. This means that no fingerprinting of individual users will be allowed on Apple iOS devices unless the user explicitly agrees by opting in to the auto prompt that all apps will have to display starting with iOS 14.5.

With this, what we expect is that the proportion of users opting into user tracking will be lower than earlier and, consequently, advertisers will likely have a much smaller pool of addressable users on Apple devices. According to the InMobi IDFA Resource Center, as of Aug 2021, we see a global opt-in percentage of 37% for IDFA usage. And, with only two-thirds of the iPhone users having upgraded to iOS 14.6, this is expected to improve further.





WHAT WAS IDFA USED FOR?

- First, identity and targeting. Advertisers recognize users in the ecosystem and target or retarget them in pursuit of their advertising goals.
- Secondly, efficiency and value management. IDFA is used to power efficiency-driving technology such as frequency capping, ad rotation, dynamic creative optimization and pricing/prediction.
- The third and last is measurement and attribution. IDFA has been the most critical component of the iOS measurement chain, powering multi-touch attribution, last-click attribution, last-view attribution, etc, and is the basis on which all mobile media is measured.

THE IMPACT OF THE IDFA-RELATED CHANGES FOR ADVERTISERS

- **Identity and targeting** - the lack of an IDFA removes the ability to build user profiles. Audience targeting and retargeting is expected to be restricted to less than 20% of the iOS user pool, according to Post-IDFA release by Gamesbeat in May 2021.
- **Efficiency and value management** - demand-side platforms and exchanges face challenges enforcing frequency caps on user impressions to optimize campaigns efficiently. Typical campaigns are expected to move from using IDFA-based optimization to an in-session or non-persistent ID-based frequency capping to prevent wastage of impressions on the same user.
- **Measurement and attribution** - performance-focused advertisers will be unable to use Mobile Measurement Partners for attribution (except for opt-in users) and will instead have to use Apple's SKAdNetwork (SKAN). Third-party measurement and attribution (multi-touch attribution, cross-device tracking, view-through attribution) will only be possible for opt-in users since they all use IDFAs. With iOS 14.6, more updates have come in on the attribution front with install-validation postbacks to multiple ad networks (up to 5) that sign their ads using version 3.0. There is also a new feature - Private Click Measurement for privacy-preserving measurement of ad clicks across websites and from iOS apps to websites in iOS and iPadOS 14.5 betas.

How advertisers can build their mobile marketing strategy post-IDFA:

- Advertisers focused on brand awareness should focus more on KPI-led campaigns or utilize AI-powered contextual targeting, instead of user-level targeting. KPI-Based Advertising: Since KPIs such as Video Completion Rates (VCR), Click-Through Rates (CTR), viewability, etc, are not impacted by IDFA, advertisers can opt in to deals based on KPIs like VCR, CTR; and viewability.
- Contextual Targeting: Advertisers can request curated inventory packages that only pass on ad requests matching their user profile based on supply parameters like app, app category, network, operating system, device hardware version, and the like.

WHAT DO PERFORMANCE-FOCUSED ADVERTISERS NEED TO DO?

- The only way for performance advertisers to measure and attribute installs is with Apple's SKAdNetwork (SKAN) framework for their Limit Ad Tracking or non-consented traffic. Because SKAN is a framework that's relatively new to the entire ecosystem, advertisers could expect tech fixes and upgrades along the way as the ecosystem sees broader SKAN adoption.
- In the absence of IDFA, post-install activity will be impacted. Hence, advertisers should expect to pay higher prices for consented traffic and rely more on upstream metrics like CTR and VCR.

Consumer Flow - App Tracking Transparency

The App Tracking Transparency feature allows Apple iOS 14+ users to have more control over how their personal data is tracked and collected by app developers.

WHY ARE YOU SEEING THESE PROMPTS?

Apps display a pop-up notification and this prompt will ask users to give or deny access to their device identifier. During this stage, users will need to make a decision if they allow or deny access to data the app wants to collect, and how and what they want to do with it.

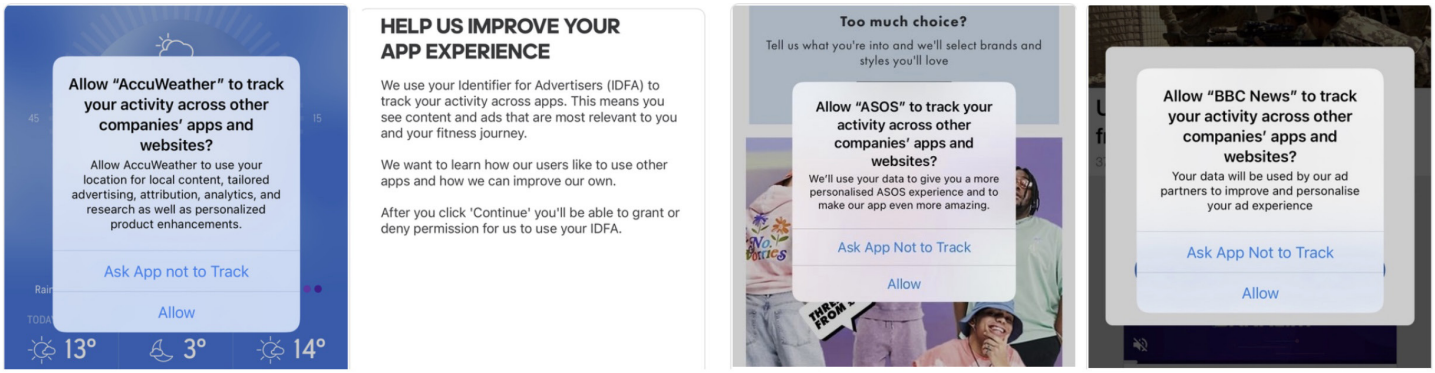


Image Source: https://www.attprompts.com/

WHAT DOES IT MEAN FOR THE USER?

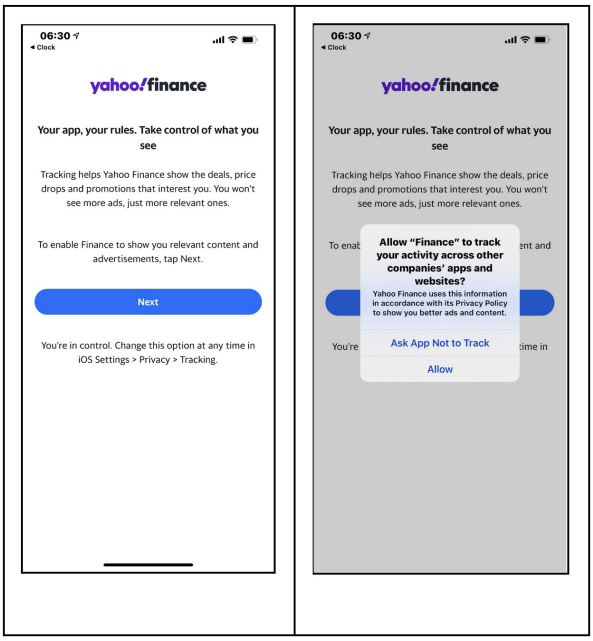
In short, App Tracking Transparency (ATT) allows the user to control which apps can track their activity across apps and websites. Users are now given the option to enable or disable this feature.

WHAT HAPPENS WHEN YOU ASK APP NOT TO TRACK?

If you choose 'Ask App Not to Track', the app developer can't access your IDFA, and the app is not allowed to track your activity or share any information about you with a third party.

WHAT HAPPENS WHEN YOU ALLOW AN APP TO TRACK YOU?

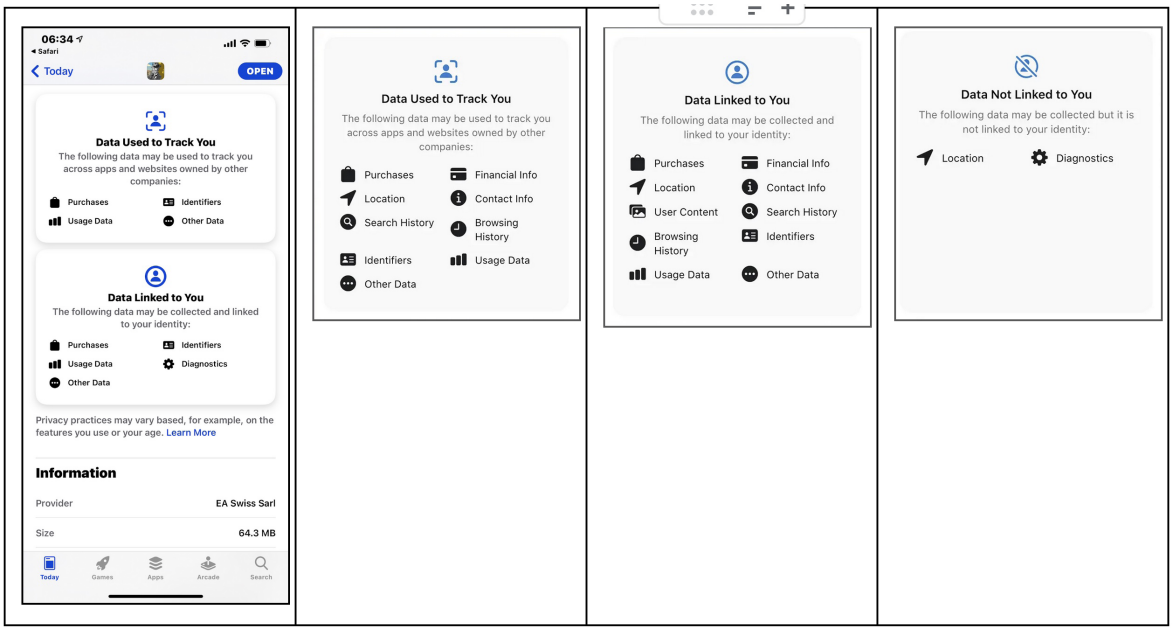
When you click on 'Allow' it allows the app to **track your activity**, and you have given your approval/permission for app developers to share information about you to an advertising profile that can track you across apps and also across the web.



WHAT'S BEING TRACKED?

Apple have categorised this into 3 groups to help us understand what data is being collected by an app and how your personal data will be used.

1. Data Used to Track You - this is what will be shared across different apps and companies.
2. Data Linked to You - the data that is collected by the app and company but not shared.
3. Data Not Linked to You - data that will be collected is generally used for analytics.



WHAT YOU NEED TO KNOW?

1. Go to App Privacy details on the App Store to better understand an app's privacy practices.
2. Read about the Data Collection and how your data will be used.
3. **It's all within your control** - know your controls - you can turn the tracking on/off or on based on your needs; and you can also control if you wish to see the prompt every time you download a new app.
4. Lastly, know that **you can change your mind anytime**, head into Settings to change it. App Tracking Transparency settings can be changed on each individual app level. It's all within your control.

Desktop browser (Cookies) changes

In June 2021 Google announced that Chrome will phase out support for third-party cookies in late 2023, pushing back the previous deadline from 2022.

Cookie alternatives have been developed since Google's initial announcement in January 2020, including: LiveRamp Identitylink (IDL), UnifiedID 2.0, ID5, and Nielsen Identity Sync among others, and each are at different stages of development and testing in APAC.

Marketers are having to face the cookieless world from a targeting and measurement perspective and it is abundantly clear that having a robust first party data strategy is going to be essential in maintaining direct dialogue with consumers.

This is not always easy to do, especially for small to medium sized businesses that lack the resources to collect large amounts of data. However, it is a problem every advertiser will face and it's an ever-evolving space.

The focus recently has shifted away from what will be lacking when cookies are removed, to how to gain consumers' trust in order to have meaningful conversations with them that are aligned with marketing and communications objectives.

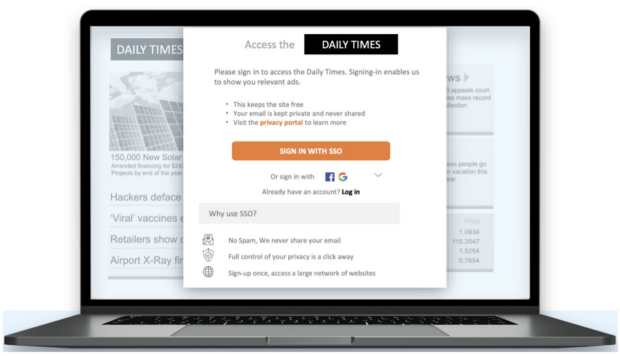
This is a pivotal time in our industry and as everyone grapples with alternatives for both targeting and measurement in the desktop environment, the deprecation of the cookie is arguably not the worst thing that could happen.

CONSUMER FLOW - COOKIES

The consumer flow will differ based on how brands choose to collect consumer data. Some are exercising creativity and using competition formats; while others are asking for feedback. This test and learn period will be essential in finding the 'right' way for both brands as well as consumers.

What isn't yet clear at this stage is exactly how cookie-alternative ID consent collection will appear to users; however a Single Sign On has been indicated as a form of consent collection.

The image below is for illustration purposes only.



Once a user signs in, the site will load as usual with the universal ID being used for tracking and measurement by advertisers. As we will be operating within a multi-ID environment until the end of 2023, this process will happen alongside cookie collection and targeting, as normal.

If a user chooses not to sign-in until cookies have been removed, this will likely have no impact to users as advertisers will still be able to use cookies for targeting and measurement of campaigns.

At some point, the publisher may decide to restrict content to users who choose not to consent to universal IDs, or the user will be exposed to a different ad landscape. Since the user has opted out of sharing data in exchange for relevant advertising, the ads that they may see will likely feel out of place and disruptive.

There is still a lot that remains unclear regarding how this change will be reflected to users, but what is clear is that the value exchange needs to be made much clearer to users than it currently is for cookie acceptance.

Important details shouldn't be hidden in pages of legal jargon. Ultimately users need to be clear on the exchange, be empowered to make a real choice regarding their data, and have the ability to change their consent status, should they choose to.

What can be done now: Consent Framework

Consumers practically do everything online, and increasingly so since the onset of the pandemic, be it shopping, paying bills or availing themselves of new services. All our digital interactions require some level of personal data sharing and we need to be assured that our digital experiences are worth trusting, and that our data will be used for its intended purpose in a privacy safe environment.

- First-party cookies are the lifeline of digital businesses enabling them to remember key pieces of information about users and to collect user analytics data.
- Third-party cookies allow publishers to monetize their websites, and enable advertising and marketing.

The identity landscape is becoming more complicated. New privacy regulations are evolving globally. These include -

- European Union: General Data Protection Regulation (GDPR) the gold standard
- USA: California Consumer Privacy Act (CCPA)
- USA: Children's Online Privacy Protection Act (COPPA)
- Brazil: General Data Protection Law (LGPD)
- Singapore: Personal Data Protection Act (PDPA)
- India: Personal Data Protection Bill (PDPB)
- Japan: Act on the Protection of Personal Information (APPI)
- New Zealand Privacy Act.

These regulatory frameworks require organizations to make sure their customers know who is in control of their data and how their data is being used across the value chain. Consumers should be offered complete control on the levels of consent and approve how their data will be processed with preferences around opt-in or opt-out upfront.

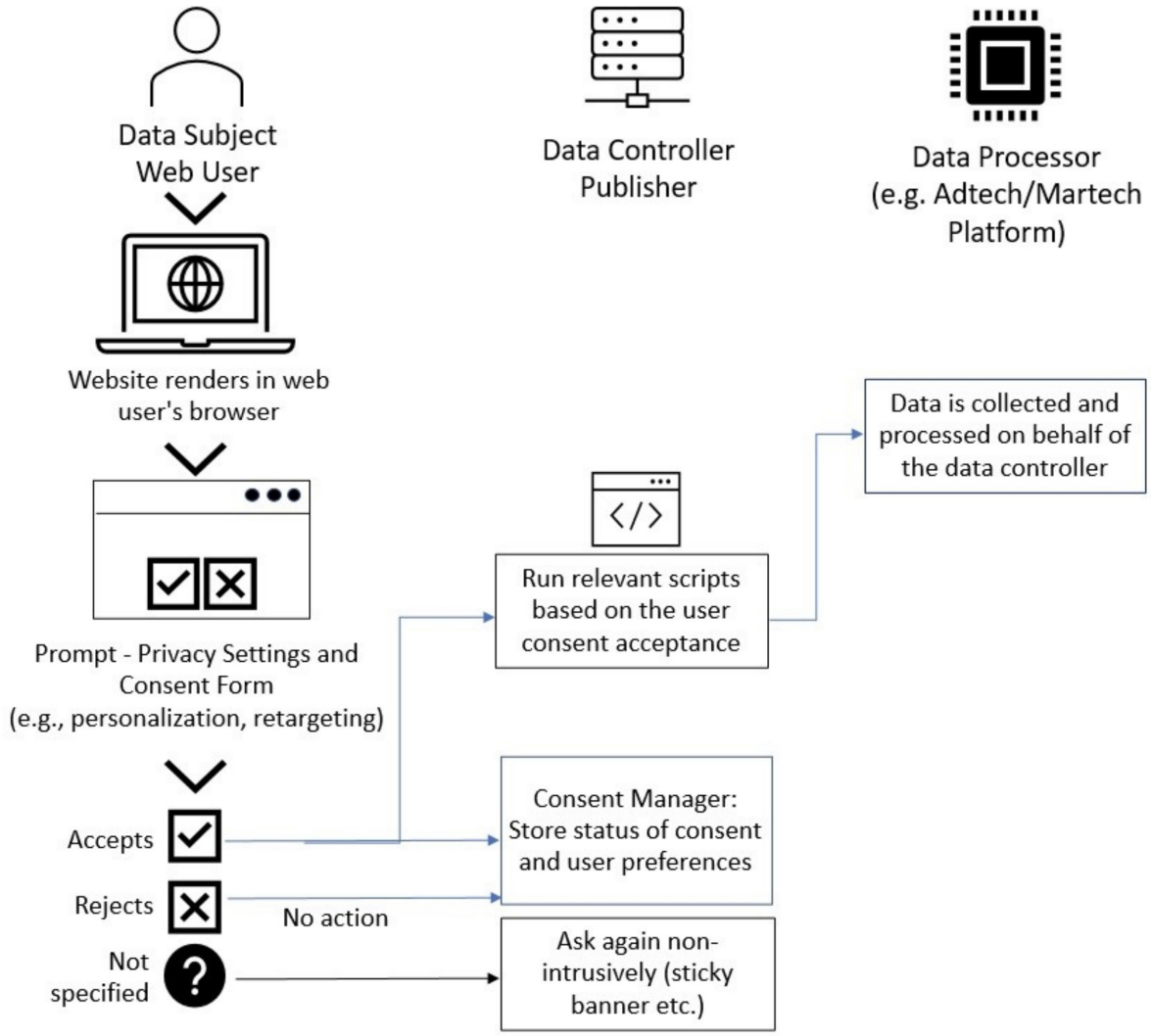
Consent Management Platform (CMP) helps organisations store proof-of-consent and consumer preferences, manage requests to alter consent; and offer transparency into data collection and usage practices. CMP allows brands to automate the consent process within the applicable regulatory frameworks.

What are the latest developments and next steps?

Organisations need to consider the following when implementing or upgrading their CMP as it should -

- help meet the applicable regulatory obligations
- help in collection and management of consent - displaying consent pop-ups/widgets to users, collecting and storing visitor consent preferences and keeping record of changes, managing visitors' requests to access or erase their data
- help keep a record of collected data - consented users (identifier - email/cookie/device ID), timestamp of consent, specific purpose of opt-in, and if the consent was changed or withdrawn
- offer a self-service interface to users allowing them to manage their consent and data.

Process of collecting and storing user consent



The industry is preparing for the third-party cookieless future. Identity solutions are evolving as alternative solutions including Google's trust tokens (that enables websites convey user's authenticity with limited information from one context to another and help combat fraud without passive tracking) and Federated Learning of Cohorts (FLoC), a type of web tracking through federated learning where people are grouped into "cohorts" based on their browsing history for the purpose of interest-based advertising. These solutions are at different levels of development and testing in APAC, and while they process data with a greater level of anonymity, they still need to collect and process personal data to enable audience targeting.

While this space is still evolving, there is a lack of compatible rules around how these identities would be established and authenticated and how they would be integrated, potentially creating fragmentation of the open web. These new frameworks face the same risks and challenges as third-party cookies today, and need the empowered consent of end users.

Consent is still the foundation for compliant tracking regardless of the identity solutions in the works. Organisations cannot ignore the importance of consent management. Consent must be at the center of data privacy and tracking, and is all about consumer respect and trust, a transparent and privacy-safe environment with the overall goal of improving online experiences.

What will the impact be to consumers and key Industry players?

The deprecation of identifiers is bound to change the fabric of digital and push the ad industry into evolving their marketing technology practices while giving them an opportunity to rethink their current marketing strategies. The change will impact everyone from consumers to businesses operating in the ecosystem and will segregate us into two pools broadly -

1. Walled gardens: will consist of closed-door systems that control their own applications, media and/or data such as Google, Amazon, Facebook and the like.
2. Open internet: independent players who make information/variables freely available without any ulterior motives

So what will happen? The impact stemming from the loss of identifiers will impact users/consumers, advertisers, publishers, and platforms.

IMPACT ON CONSUMERS

Consumers are more than ever aware about privacy with emails around privacy, cookie banners, policy updates notifications, cookie preference settings etc. Consumers are becoming more aware of changes in the landscape. An August 2021 study by KPMG reported that on the consumer front, people are becoming even more skeptical and wary about their data being collected. 86% of the respondents said they feel a growing concern about data privacy, while 78% expressed fears about the amount of data being collected.

Consumers are firmly in the driving seat of how their data is used by various companies. Along with control, it also gives them visibility and understanding into which company captures or manages their data. Since they must give explicit consent for their data to be collected it should also avoid cases of 'hidden' data collection. Personalisation of digital content (digital experience as we know it) outside of a brand/media owner's owned and operated properties will become less common. For example, ads will become less relevant and 'boring'; however, consumers who visit a particular brand website are still likely to be shown personalised communications.

IMPACT ON ADVERTISERS

As identifiers deprecate it will be important for brands to understand how their marketing KPIs will be affected. As an immediate effect of identifiers deprecating, advertisers will lose the capability of ad personalisation, especially for acquisition-focused campaigns. Another area of impact will be measurement, and campaigns are bound to see fluctuations in performance reporting. Brands working with third-party audience data (data where the reliance is on third party digital identifiers) will see diminishing pools of audiences and a drop in sufficient scale for media buying. Advertisers will need to develop newer prospecting strategies and heavily rely on other tactics. Along with exploring newer tactics, advertisers will also lose frequency capping which will lead to overserving of ads which in turn will impact the efficacy of advertising.

It is also critical that brands understand how their marketing KPIs will be affected. For example, without third-party cookies most display/programmatic view-through conversion data will disappear, but that does not mean consumers have stopped converting after seeing banner ads. Additionally, without third-party cookies, popular methodologies used to understand advertising incrementality, like A/B testing, audience holdouts, and uplift studies will likely diminish.

This does not mean advertising value is lost. Advertisers must look to more durable methods, like intra-platform solutions and consumer identity, to obtain these measures of effectiveness. By understanding the specific impacts to measurement (such as frequency capping, ad rotation, dynamic creative optimization and pricing/prediction) as isolated from other changes, brands can use the data still available to deliver accurate estimates of metrics that are no longer tracked and should use the next year to establish their own benchmarks.

IMPACT ON PLATFORMS/AD TECH PLAYERS

The platforms best positioned to move into an identifier-less future are the ones that own both ad inventory and a first party data ecosystem; every other platform is trying to partner up to fill gaps in the equation.

By nature of business, walled gardens like Google, Facebook, Amazon etc are best positioned to evolve their offerings into more promising solutions as identifiers fade away. The more independent ad technology players are looking to be more collaborative through strategic partnerships that preserve the value of their assets.

Specifically, demand side platforms might not lose their appeal since most of them enable granular targeting and campaign management through other parameters (than third-party audience data) like site whitelists, content categories, keywords, location, time of day/week, browsers, devices, first-party audiences etc) as well as access to vast inventory sources.

Supply Side Platforms (SSPs) working with data-rich publishers will see an impact in yields too with the limited visibility of users. Big names in the SSP world like Pubmatic are building ID management solutions for the publishers, that promise industry-wide interoperability as well as privacy-focused addressability.

Data providers that depend on third-party identifiers will face an existential threat to their business models. It is important to note that not all third-party data providers depend on identifiers (the likes of Visual DNA that aggregates data in a transparent manner through quizzes).

IMPACT ON PUBLISHERS

Large digital publishers generate a significant portion of their revenue by monetising their user data through third party partnerships. With identifier deprecation, this will no longer be possible, which might result in a loss of revenue for digital publishers in the short term and requiring them to develop new strategies for revenue generation from the audience data they produce. It's already being reported that advertisers are seeing a 15% to 20% drop in revenue since the change. In addition to this both large and small publishers who work with independent ad tech players to monetise inventory might see fluctuations in yields due to system dependency on digital identifiers to match advertiser demands.

Conclusion

As we navigate the evolving world of mobile and online identity it is clear that some long-held beliefs are going to need to change, as will some outdated practices.

This doesn't have to be all doom and gloom. While there will be some growing pains, those who successfully move into the brave new world will be those who are able to think outside of the box and who put TRUST at the center.