MOBILE ADVERTISING: PREPARING FOR THE BIG RE-SET

Explaining the industry's new approach to user privacy, targeting and attribution

MEF
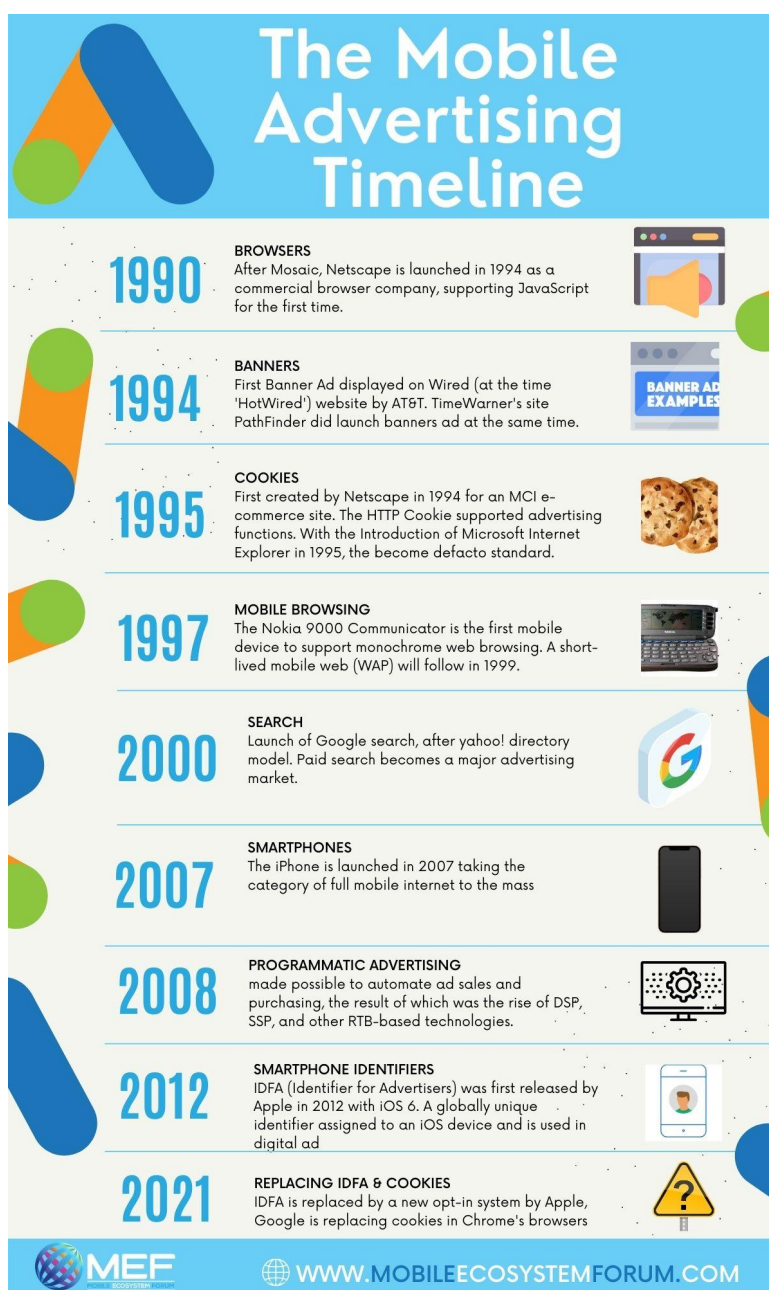MOBILE ECOSYSTEM FORUM

CONTENTS

01

EXECUTIVE SUMMARY

2021 is going to be an 'interesting' year for mobile and digital advertising. It will be the year that the industry (as we know it) dies and gets reborn - or just re-arranges itself a little.

Why? Because there is a big 're-set' coming. The impact of this re-set will be felt differently by brands, hardware platforms, AdTech firms, developers and – of course – consumers. But ultimately every stakeholder will be affected.

In this report, we will dive into:

- The present: how the mobile advertising infrastructure changed in 2021
- The past: the historical shifts that forced a change
- The future: possible alternative solutions for targeting and attribution

The Mobile Advertising Timeline

1990 — BROWSERS
After Mosaic, Netscape is launched in 1994 as a commercial browser company, supporting JavaScript for the first time.

1994 — BANNERS
First Banner Ad displayed on Wired (at the time 'HotWired') website by AT&T. TimeWarner's site PathFinder did launch banners ad at the same time.

1995 — COOKIES
First created by Netscape in 1994 for an MCI e-commerce site. The HTTP Cookie supported advertising functions. With the Introduction of Microsoft Internet Explorer in 1995, the become defacto standard.

1997 — MOBILE BROWSING
The Nokia 9000 Communicator is the first mobile device to support monochrome web browsing. A short-lived mobile web (WAP) will follow in 1999.

2000 — SEARCH
Launch of Google search, after yahoo! directory model. Paid search becomes a major advertising market.

2007 — SMARTPHONES
The iPhone is launched in 2007 taking the category of full mobile internet to the mass

2008 — PROGRAMMATIC ADVERTISING
made possible to automate ad sales and purchasing, the result of which was the rise of DSP, SSP, and other RTB-based technologies.

2012 — SMARTPHONE IDENTIFIERS
IDFA (Identifier for Advertisers) was first released by Apple in 2012 with iOS 6. A globally unique identifier assigned to an iOS device and is used in digital ad

2021 — REPLACING IDFA & COOKIES
IDFA is replaced by a new opt-in system by Apple, Google is replacing cookies in Chrome's browsers
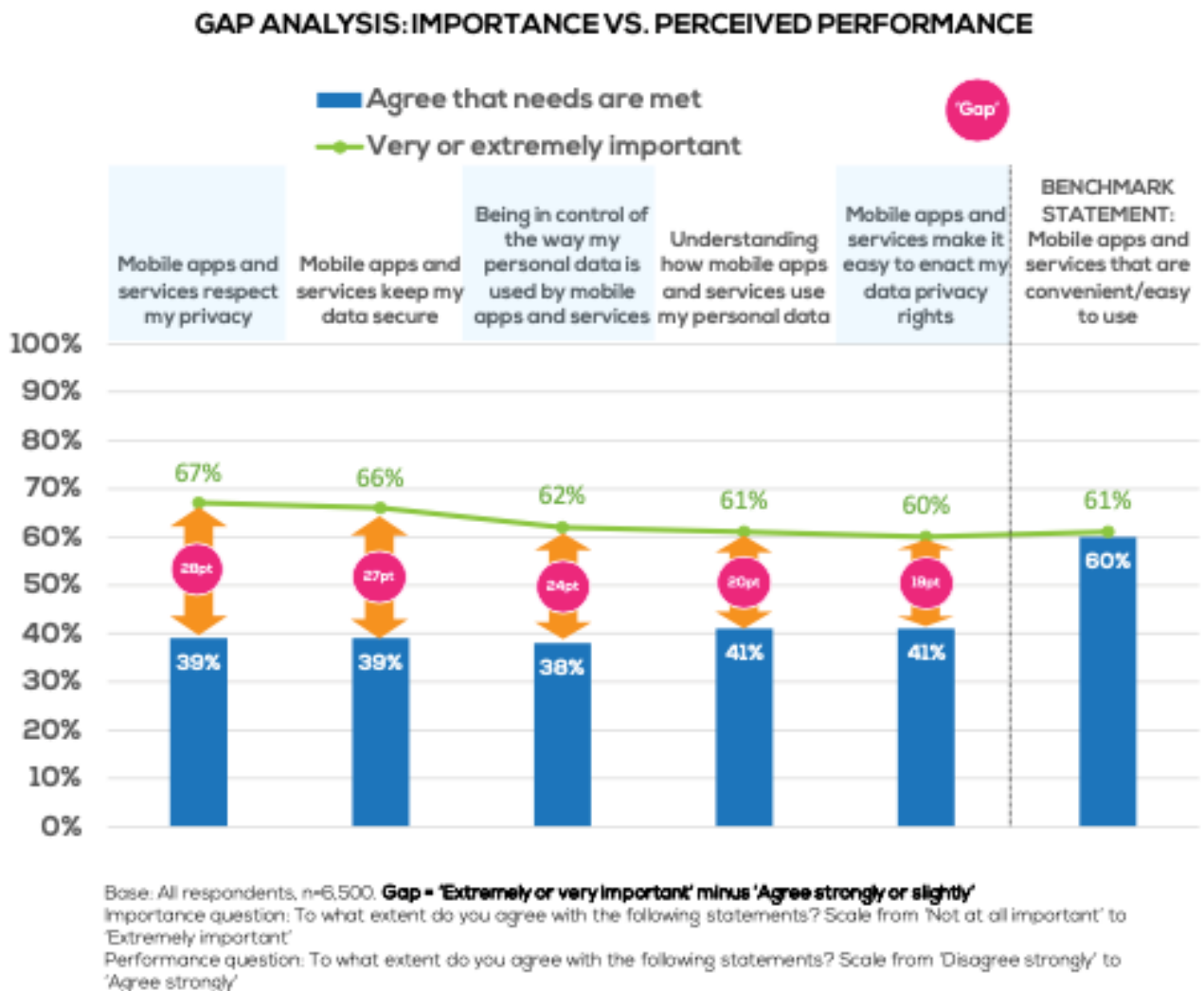
MEF — 🌐 WWW.MOBILEECOSYSTEMFORUM.COM

02

INTRODUCTION – 2021 THE YEAR OF CHANGES

What caused the wholesale transformation in digital advertising? And why now? There are three key factors to consider: the consumer backlash on tracking; Apple's privacy-focused marketing strategy; and Google's response. Let's look at each in turn.

Consumers' growing unease with personal data sharing

For many consumers, surveillance and tracking by digital advertisers has gone too far. They are unhappy seeing the same ads follow them around their digital journeys. They want their 'privacy' back. The extent of the backlash was revealed in the MEF 7th Consumer Trust Study. Our yearly global survey showed that fewer than four in ten people think apps respect their privacy:

Figure 1 Global Consumer Sentiment: unmet expectations on data privacy and security

GAP ANALYSIS: IMPORTANCE VS. PERCEIVED PERFORMANCE

Base: All respondents, n=6,500. **Gap = 'Extremely or very important' minus 'Agree strongly or slightly'**
Importance question: To what extent do you agree with the following statements? Scale from 'Not at all important' to 'Extremely important'
Performance question: To what extent do you agree with the following statements? Scale from 'Disagree strongly' to 'Agree strongly'

In response to this negative sentiment, some of the most powerful stakeholders in the ad ecosystem have acted. This process began on the desktop web. In 2019, privacy-centric browser companies (Mozilla/Firefox, Brave etc) started to change their cookie policies – blocking cookies that they identified as trackers. Apple's Safari and eventually even Google's Chrome followed suit.

The upheaval in the mobile world was even more dramatic; its 'all change' moment came in 2020 when Apple announced plans to stop its 'Identifier for Advertisers'.

**Apple makes changes to its Identifier for Advertisers (IDFA)**

For years, the mobile industry relied on Apple's IDFA unique identifier, a unique code which is linked to a specific iPhone. Advertisers could use the IDFA to track their users' activity not just on their own apps but across most digital services. Knowing a user's IDFA gave brands/agencies/publishers the ability to measure the performance of a campaign and give customers a more personalised experience.

In a sense, the IDFA has been at the heart of the mobile ad entire ecosystem – one worth $91.52 billion in 2020[1] in the US alone. Now, it's gone. Kind of. Apple launched a new App Tracking Transparency (ATT) feature with iOS 14.5 in the second quarter in 2021. Under the new rules, it still offers access to the IDFA, but only with an active opt-in from the user. Most users decline. According to Flurry Analytics three weeks after the launch of iOS 14.5, the worldwide opt in rate varied from 11% to 15%.

Apple's move has shifted the balance of power in the world of mobile advertising. The various mobile ad stakeholders know they must look for new ways to measure, attribute and personalise their campaigns.

---

[1] https://www.emarketer.com/content/us-mobile-ad-spending-will-manage-grow-2020

Figure 2 User Experience for data management in Apple iOS
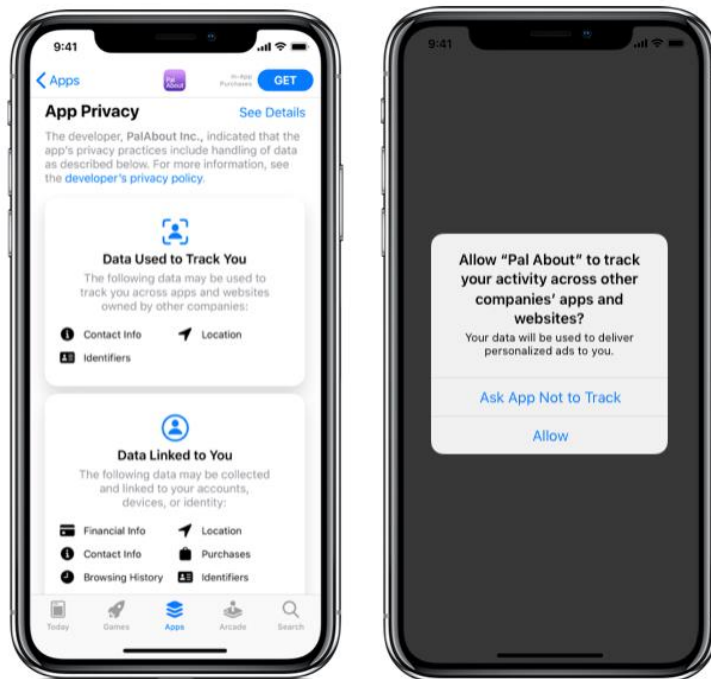
Google: phasing out third-party cookies in Chrome

Google has said little about whether it will follow Apple's lead with its own mobile identifier for Android, GAID. There is speculation it will do so, since it has adopted Apple's privacy stances in the past. (However, since Apple's iOS accounts for about 30% of the global smartphone market there will be an impact whatever Google's actions)

We can also look at what is happening on the web as an indication of Google's thinking. It is phasing out third-party cookies on its web browser Chrome, which is present on most Android phones by default. (First-party cookies that track basic data about a website's visitors are still safe.)
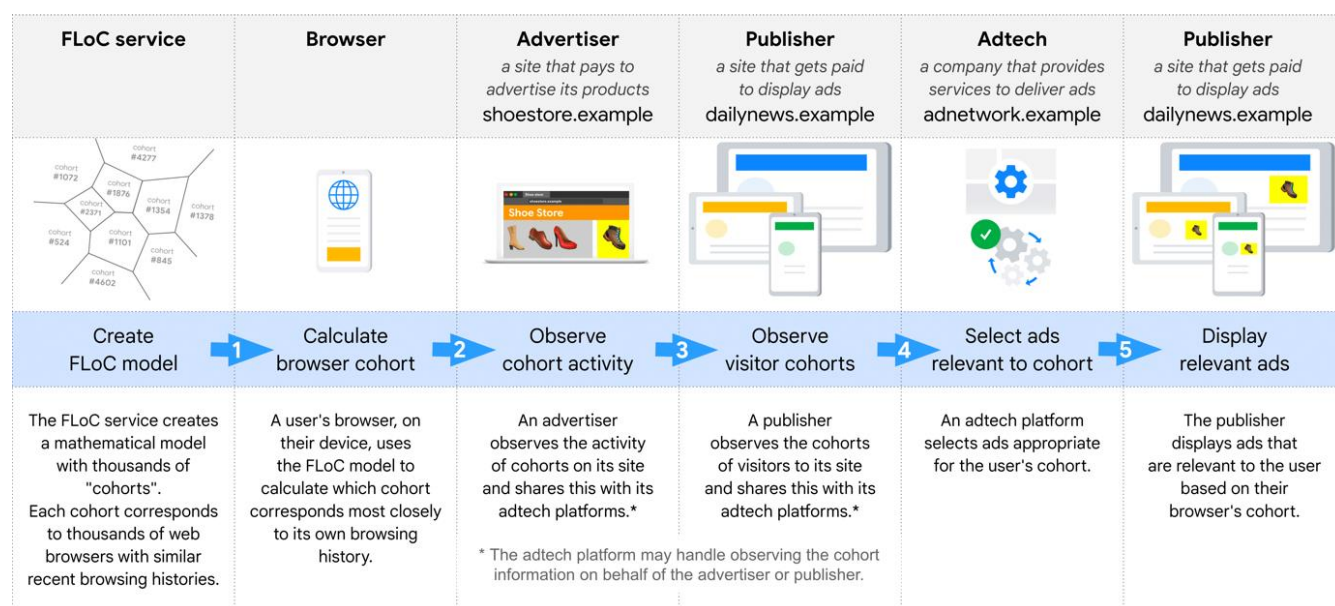
What will replace them? Google announced its primary candidate in March 2021. This is called FLoC (Federated Learning of Cohorts) for Chrome.

The new solution creates groups (or cohorts). The cohorts reflect behaviour rather than any history of sites visited. So, if you're using FLoC, Chrome will look at your browsing history and compare it with the habits of others. You'll then be placed into a group (cohort) with thousands of others. Advertisers can then target these groups rather than specific individuals. The key point is that nothing personal leaves your device. Your browser is tracking you, but it doesn't send the information anywhere.

Google argues that this is a win for privacy, but interest groups such as the EFF are fighting the proposal by calling FLoC as a diminished tracking cookie. FLoC has not been welcomed by the other browser companies either. Google is pressing ahead. It clearly wants to protect its main revenue source, advertising.

FLoC was initially tested in only 10 countries the USA, Australia, Brazil, Canada, India, Indonesia, Japan, Mexico, New Zealand and the Philippines. The experiment excluded the EU/UK to avoid potential conflict with the European GDPR regulatory framework.

Figure 3 How Google's FLOC works

FLoC service	Browser	Advertiser *a site that pays to advertise its products* shoestore.example	Publisher *a site that gets paid to display ads* dailynews.example	Adtech *a company that provides services to deliver ads* adnetwork.example	Publisher *a site that gets paid to display ads* dailynews.example
Create FLoC model	Calculate browser cohort	Observe cohort activity	Observe visitor cohorts	Select ads relevant to cohort	Display relevant ads
The FLoC service creates a mathematical model with thousands of "cohorts". Each cohort corresponds to thousands of web browsers with similar recent browsing histories.	A user's browser, on their device, uses the FLoC model to calculate which cohort corresponds most closely to its own browsing history.	An advertiser observes the activity of cohorts on its site and shares this with its adtech platforms.*	A publisher observes the cohorts of visitors to its site and shares this with its adtech platforms.* * The adtech platform may handle observing the cohort information on behalf of the advertiser or publisher.	An adtech platform selects ads appropriate for the user's cohort.	The publisher displays ads that are relevant to the user based on their browser's cohort.

Source: Google

03

BEGINNINGS: HOW WE GOT HERE

For most of its history, advertising was contextual. Typically, brands placed their ads in relevant media. Trying to sell golf clubs? Put your ad in a golf magazine. If brands weren't doing directly contextual advertising, they were running ads in media that attracted a desired demographic. For example: selling expensive watches in newsmagazines like 'Time' and 'Newsweek'.

When digital media went mainstream in the 2000s, advertising changed. For the first time, it became possible to target not groups of people with a similar interest (or with a similar demographic profile), but individuals. Brands could track one person at a time. They could log the sites she had visited and the searches she had made – and show her relevant ads based on her profile. These ads could appear on any site. So, the consumer might be browsing a site about walking holidays, but still see an ad for saucepans.

Welcome back, visitor': the web cookie is born

What made the new world of digital advertising possible was the cookie. Cookies were not originally designed with advertising in mind. Rather, they were invented in the early 1990s to make web browsing more convenient. A cookie is a small text file that sits inside your browser. When you visit a website, the site can create a cookie to store information about you. Later, when you return, the site can use the cookie to recognise you – and therefore make the experience quicker and more personal. For example, it can auto-fill your address details.

These are first party cookies. However, it is also possible for third parties (i.e., not the web site owner) to create them too. Advertisers were among the first to spot the potential of the third-party cookie. They realised they could embed these lines of code on a variety of partner sites, and then use them build profiles on people, track them around the web and show them targeted ads.

The machines take over: programmatic advertising

In time, this kind of advertising became the norm. It became known as programmatic advertising, and it spawned a new generation of AdTech providers. These specialists replaced the old-school buying and selling of ads (by humans in ad agencies) with real-time trading by algorithmic machines.

Figure 4 The Evolution of Mobile Advertising

The Mobile Advertising Timeline

1990 — BROWSERS
After Mosaic, Netscape is launched in 1994 as a commercial browser company, supporting JavaScript for the first time.

1994 — BANNERS
First Banner Ad displayed on Wired (at the time 'HotWired') website by AT&T. TimeWarner's site PathFinder did launch banners ad at the same time.

1995 — COOKIES
First created by Netscape in 1994 for an MCI e-commerce site. The HTTP Cookie supported advertising functions. With the Introduction of Microsoft Internet Explorer in 1995, the become defacto standard.

1997 — MOBILE BROWSING
The Nokia 9000 Communicator is the first mobile device to support monochrome web browsing. A short-lived mobile web (WAP) will follow in 1999.

2000 — SEARCH
Launch of Google search, after yahoo! directory model. Paid search becomes a major advertising market.

2007 — SMARTPHONES
The iPhone is launched in 2007 taking the category of full mobile internet to the mass

2008 — PROGRAMMATIC ADVERTISING
made possible to automate ad sales and purchasing, the result of which was the rise of DSP, SSP, and other RTB-based technologies.

2012 — SMARTPHONE IDENTIFIERS
IDFA (Identifier for Advertisers) was first released by Apple in 2012 with iOS 6. A globally unique identifier assigned to an iOS device and is used in digital ad

2021 — REPLACING IDFA & COOKIES
IDFA is replaced by a new opt-in system by Apple, Google is replacing cookies in Chrome's browsers

MEF — WWW.MOBILEECOSYSTEMFORUM.COM

In this new world, when an individual arrives at a website the web owner's (sell side) advertising platform 'sells' this individual to the highest bidder (demand side platform). The winning advertiser processes information about the consumer before making a bid. It then shows a relevant ad. The entire process can take a few microseconds. For this reason, it is called Real Time Bidding (RTB).

Programmatic advertising gave web site owners a better chance to monetise their sites. They could simply outsource the management of their ad inventory to a service such as Google's AdSense. Pretty soon, programmatic advertising came to dominate the web. In 2020, it accounted for 78.4 percent of US spending on display and video advertising.

But it also gave rise to some of the worst aspects of the online experience: spam sites, click farms, bot fraud. And, for many end users, seeing highly targeted – and retargeted – ads didn't feel like a welcome personalised experience, but an intrusive loss of control.

Figure 5 The first reported programmatic advertising

This advertising is reported to be run in 1994 on HotWired.com (today's Wired magazine) featuring an advert from AT&T. Below is the advertising[2].

Thanks to apps, mobile pursues a different path

By the mid 2010s the smartphone was taking over from the desktop. Mobile was becoming the dominant digital channel. This presented a problem for

---

[2] https://www.match2one.com/blog/what-is-programmatic-advertising/

advertisers as most user activity in mobile is in apps – and apps don't 'do' cookies.

In addition, mobile is a far more heterogeneous environment than the desktop. There are dozens of different types of devices, running different operating systems, with different mobile web browsers. Technically, it is harder to link these diverse elements than it is on the desktop.

And so, the device ID was born. Google's Advertising ID (GAID) and Apple's Identifier for Advertisers (IDFA) are the primary examples. Armed with a person's device ID, an advertiser can collect troves of data and associate it with an individual customer. What's more, this data can reveal crucial information that is not accessible on the desktop such as location.

This is all great for tracking and attribution. For example, if a consumer takes a specific action because of an ad – clicking a banner, playing a video, installing an app – the AdTech company can associate the action with an IDFA. They can pass this back to the advertiser to show the effectiveness of a campaign. Device IDs can also be helpful for cross-device targeting. For example, let's say a when a user sets up a phone, he enters an email address. That address is now inextricably linked to his device ID. So, when that email is used to access other online accounts – social networks, streaming music etc – on other devices, marketers will be able to join the dots.

04

THE BACKLASH – CHALLENGES TO THE ADVERTISING STATUS QUO

At the keynote for the 2019 Dmexco digital marketing conference Stephanie Buscemi, CMO of Salesforce, said: "We have to strike a balance between personalised experiences and privacy. Mark my word this is the new battleground for all of us." Her words summed up the biggest challenge digital marketers had faced since their industry was born.

For 20 years, the industry dedicated itself to find new ways to track people online. It did so without any real restrictions. Suddenly, it had plenty. Some came from outside – from regulators. These include EU's GDPR and ePrivacy guidelines and the California Consumer Privacy Act, which the industry is still wrestling with.

Figure 6 The Backlash History

The Mobile Ad-Backlash History
- 2015 Ad Blockers
- 2018 GDPR Roll-out
- 2019 FIngerprinting Crackdown
- 2019 Majority of users taking privacy protection action
- 2020 Apple 'Designed to Protect Privacy:
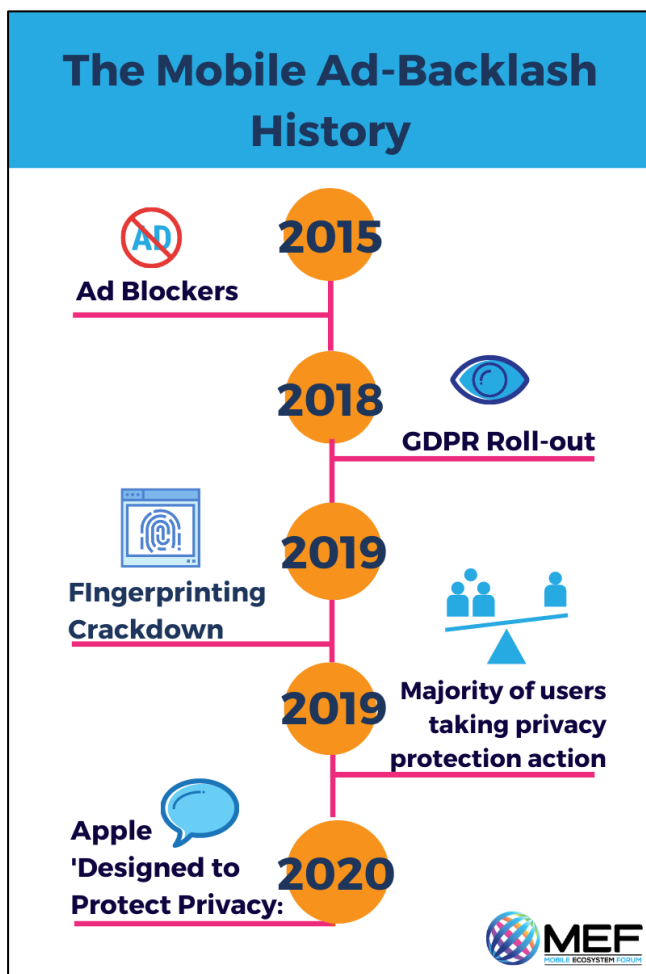
The regulators were merely responding to changing consumer attitudes. By 2019, MEF's Consumer Trust Study revealed that 84% of smartphone users said they had taken protective action to mask their identity or reduce their exposure to harm.

To make matters more complicated, the regulators themselves have come under fire for not doing enough. In June 2021, the Irish Council for Civil Liberties (ICCL) filed a lawsuit in a German court against the world's online advertising industry. It says the Data Protection Commission in Ireland, along with other regulators within the EU, have failed to act on formal complaints over the last three years. These

complaints focus on what it calls "the world's largest data breach" by the online advertising industry.

Browsers start to block cookies

By the mid 2010s users had started to install ad blockers to prevent ads from loading (and slowing down their browsing experience). By 2019, according to the MEF Consumer Trust report, 17.2% of smartphone users were reported to be using ad blocking.

Smaller browser firms ran with this new desire for privacy. In 2015, Mozilla launched 'Private Browsing with Tracking Protection' for Firefox. It let users "block content like ads, analytics trackers and social share buttons that may record your behaviour without your knowledge across sites." It was the first of many similar moves. In 2017, Apple introduced Intelligent Tracking Prevention in Safari to limit the ability of sites to use cookies.

However, the nuclear option on cookies was finally detonated by Google. Because Google makes so much money from ads, few expected it to restrict third party tracking in Chrome. That changed in January 2020 with a blog. The title said it all: "Building a more private web: A path towards making third party cookies obsolete." Google wrote: "Users are demanding greater privacy – including transparency, choice and control over how their data is used – and it's clear the web ecosystem needs to evolve to meet these increasing demands."

A clampdown on fingerprinting

When browser firms started to disable cookies, some web site owners looked for other ways to identify users. Fingerprinting – also called probabilistic attribution – became a popular option. But again, there was a backlash. Many argue that fingerprinting is a bigger threat to user privacy even than the cookie. Why? Because it is entirely non-transparent.

So, what is fingerprinting? When you visit a web site or app, its owner can legitimately collect technical data without asking explicit permission: the browser type, the operating software, the device type, screen size, display ratio, language preferences and so on. Individually, these credentials don't say much, but combined they can form a unique fingerprint. Sites and apps can use this fingerprint to identify and target you with relevant ads. This happens in the background, without your knowledge. And you can't delete your fingerprint as you can third-party cookies.

For these reasons, the browser firms are opposed to fingerprinting. By 2019, they had all taken action to prevent it. However, some AdTech firms believe there is still potential in fingerprinting and are developing solutions that deploy the tech in a privacy-preserving way (see 'Alternatives' section below).

Mobile and apps: Apple goes all-in on privacy

It was a matter of time before the 'revolt' against tracking and surveillance on the desktop web came to mobile. As we have seen, the defining moment came in June 2020 when Apple revealed changes to the IDFA.

At time of writing, Google had made no significant changes to its ID, GAID. However, there have been reports suggesting that the company is talking about it internally – though it's unlikely the company will go as far as Apple.

05

ALTERNATIVES – WHAT WILL HAPPEN NOW IN MOBILE ADVERTISING?

Every stakeholder in the digital ad ecosystem is now facing up to the same challenge: how to deliver a personal experience – and measure the effectiveness of ads – without collecting private information. Let's look at the some of the options.

Figure 7 Alternative Mobile Advertising ID
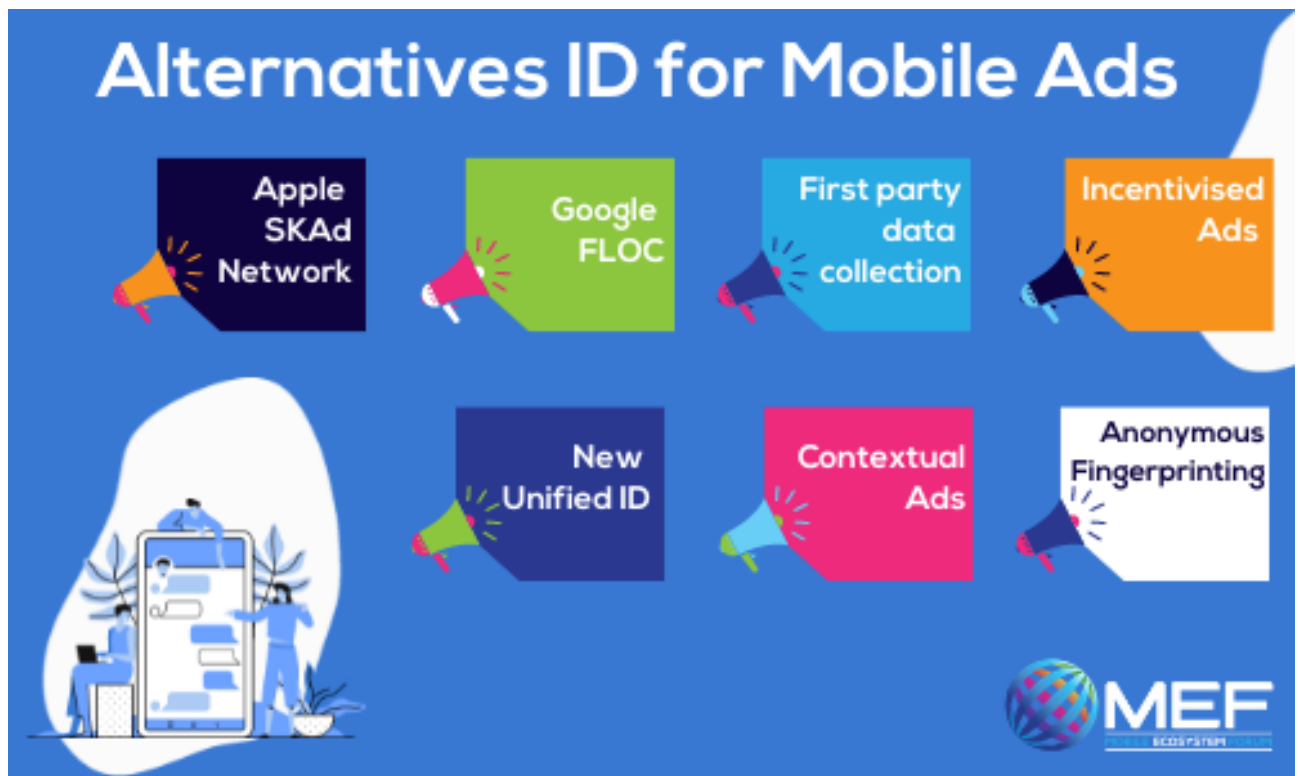
Apple's SKAdNetwork

The demise of IDFA will not stop advertisers from showing ads. But it will make it harder to measure the results of their campaigns. Aware of this, Apple unveiled a new privacy-safe framework for mobile attribution.

SKAdNetwork promises to help advertisers know which ads result in desired actions without revealing which specific devices – or people – took those actions. In this new world, when someone does something after clicking on an ad, Apple itself generates a cryptographic token and returns it to the ad network. The token reveals no device-specific or personal information. This way, the advertiser (or agency) can gauge the overall impact of campaigns but not link them to identifiable users

Google Federated Learning of Cohorts (FLoC)

Soon after Google joined the war on cookies, it set up a project called the "Privacy Sandbox" to test ideas that will keep advertising relevant and personal without intrusive tracking. As we discussed in our intro, Google's main bet is on Federated Learning of Cohorts (FLoC). The approach "hides individuals in the crowd" and uses on-device processing to keep a person's web history private on the browser.

Google has tested the concept and is pleased with the results. It says advertisers can expect to see "at least 95 percent of the conversions per dollar spent when compared to cookie-based advertising". FLoC has received a lot of criticism though. Some regulators have expressed concern that it might involve the illegal collection of data without consent. Other opponents have pointed out that trackers might be able to reverse-engineer the cohort-assignment algorithm to identify an individual user.

They have also presented a more fundamental objection around the very idea of information collection. Here is how the Electronic Frontier Foundation put it.

> *"You should have a right to present different aspects of your identity in different contexts. If you visit a site for medical information, there's no reason it needs to know what your politics are. Likewise, if you visit a retail website, it shouldn't need to know whether you've recently read up on treatment for depression. FLoC erodes this separation of contexts, and instead presents the same behavioural summary to everyone you interact with."*

First party data collection

If the end of the cookie and the deprecation of the IDFA make it harder to collect third party data, then one obvious alternative comes to mind: collect more first party data.

Before we dive into this, let's re-cap the different types of data.

Figure 8 Type of Collected Data

Zero party data
This is data actively shared by the customer. It can include information such as preferences, purchase intentions, opinions and more. Customers usually provide this data via surveys.
First party data
The behaviour data a publisher can collect on users because they have actively opted in.
Second-party data
Someone else's first-party data. Only available with consent.
Third-party data
A collection of multiple first-party data sources aggregated across websites and apps by data specialists and publishers.

Obviously when app makers and site owners collect first-party data they can then track customer behaviour and monitor performance with legal consent. So how can they get this consent? The most obvious strategy is to limit features to those that don't sign in. Conversely, they could reward people for registering. A study by Privitar revealed that consumers will provide data to receive:

- Discounts/deals – 34%
- More personalized offerings – 22%
- Updates/notices and relevant products and services – 20%

It seems that most stakeholders are looking more seriously at first party data collection. Merkle's 2021 Customer Engagement Report found 52% of respondents said they are prioritizing strategies that can help them collect more first-party data.

Many industry insiders believe a focus on first party data consent is the only way to go. Cheetah Digital is a highly visible advocate. Andy Gladwin, Cheetah's Senior Director of Global Mobile, says:

> *"The amount of data available is shrinking, and consumers have made it clear they find data collection creepy. So, the importance of direct relationships has never been greater. Brands need to take control of their destinies and create a consensual value exchange with their customers in return for data. This can be monetary – discounts etc – but it needn't be. It could offer access to unique content or simply being served with a more tailored personal experience. Ultimately, this not only reduces the dependency on third parties, but more importantly builds the foundation for stronger and longer lasting customer relationships."*

New types of unified ID

Only a minority of brands and app makers will be able to build large audiences of opted-in customers. The giants – Google, Facebook, Amazon – will likely keep their logged-in walled garden advantages post cookie. What about the rest? How can they compete?

One option is the unified ID. Here, multiple companies can pool together – anonymously – their lists of opted-in users.

An example of this is Zeotap's universal ID+ product. Publishers and advertisers that sign up for ID+ get a tokenised key (unique to them) for every opted-in user. They can then connect to the ID+ 'graph' to reach opted-in users of other sites and apps. Florian Lichwald, MD of Zeotap, says:

> "ID+ allows companies to connect users across sites and across the open web again. Effectively it replaces the cookie in a privacy-preserving way. And it works wherever there is an opted in user and a log-in event: mobile web, desktop web and apps."

Zeotap's solution exists alongside others. The most visible of these is arguably Trade Desk's Unified ID 2.0. It uses consumers' anonymized email addresses. At the point of login, the consumer gets to see why the industry wants to create this identifier and set their preferences on how their data is shared. Many of the big players in AdTech have signed up for it. They include PubMatic, OpenX, SpotX and Criteo.

One of the obstacles to the unified ID idea is proving the identity of those that sign up. Email is not a perfect ID given the popularity of disposable 'burner emails' and Apple's temporary 'Sign In With Apple SSO' service, which generates a unique, random email address that forwards to a user's personal email.

It's also possible that criminals could set up sites, sign up vast numbers of email customers (which are in reality bots) and wait for the ad revenue to pour in.

The above scenario brings the industry back to an age-old problem: how to prove this user is human – without making the authentication experience intolerable. For this reason, it's possible the AdTech industry might look towards biometric solutions such as those offered by companies such as iProov.

Contextual advertising

As behavioural targeting becomes harder, many advertisers are re-appraising 'old fashioned' contextual advertising. In other words, placing ads on relevant apps and sites. In the offline world, contextual advertising is straightforward. There are a limited number of magazines, TV shows and so on to choose from.

Online, the options are far greater. For contextual marketing to work in this context, an advertising system needs to know what a campaign is about so it can place ads on relevant web pages. And then it needs to analyse the context of millions of sites/apps to find a good match.

There are now plenty of specialists who can automate this process using machine learning. **They argue that contextual advertising has three key benefits:**

- **A better user experience** - Contextual advertising delivers only relevant content to users
- **More user privacy** - Contextual ads target users without relying on private information
- **Higher engagement rates** - One study claims a 2.2x higher rate of recall for contextual ads.

Homam Hosseini, **Chief Commercial Officer at** Sam Media, is one of those who believes strongly in contextual advertising – especially in the context of app install advertising:

"It's how we do our app install campaigns. From our point of view, I want to know what user is doing now, and target them that way. We're not so interested in tracking them around the web or re-targeting them across devices. Also, contextual 'placement' advertising is 20 percent cheaper than targeting. So, the new changes could be good for us."

Another proponent is Manuel Pacreau, VP of Operations at Addict Mobile. He believes the industry will inevitably go 'back to the future' and focus harder on context and creative. He says:

"A lot depends on the evolution of SKAdNetwork and probabilistic attribution. Apple might change its approach and we may end up with some granularity of data in the future. But in general advertisers have to accept they are going to have less data to help them target consumers. What can they do? Well, they can think more about the creative elements of their campaigns. They can craft ads that appeal to a specific demographic group and place those ads where they think those groups will be – and not let algorithms make all these decisions"

Anonymous fingerprinting

Although Apple and the browser companies have acted to curtail fingerprinting (see above), many believe the technology will evolve into new methodologies so long as they can be made anonymous and aggregated rather than individualised. They include Thomas Kothuis, CEO of digital entertainment specialist Media Elements Group. Media Elements' sister company Verve Group is now beta testing a solution – ATOM – that uses anonymous on-device fingerprinting to target individual users.

ATOM creates a probabilistic segment by drawing on a device features, app metadata, advertisement interactions and more. It then uses machine learning models to infer characteristics (such as age, gender, interests and so on) from these initial inputs. The ATOM system aggregates these imputs into a cohort larger than 100 users and then makes assumptions about the user in order to deliver relevant ads. None of the data ever leaves the device.

Verve is currently refining these models (using its own in-house apps) so that it can ship them as an SDK to publisher partners and app developers. Kothuis is optimistic about the future of mobile advertising and believes the mobile

content community will find privacy-preserving solutions faster than many other groups.

> *"I think there's a common misconception that tracking is no longer possible because of Apple's actions. But this is not true. There will be alternatives like ATOM, but they just won't be as instant as before. In our corner of the mobile business, I think we're pretty comfortable with this. We had to wait for MNOs to pay us before we could see the results of our campaigns. We are used to doing projections based on historical activity and non-user-specific characteristics."*

Incentivised advertising

Over the years, many companies have experimented with the idea of paying people to watch ads. It solves the problem of consent since the participants have to opt in. Now, with the recent changes in digital advertising, this idea is being revived. The browser company Brave launched a services called [Brave Rewards](#) based on this model.

And then there are [smaller companies such as Weare8](#). MEF member PMConnect is currently helping Weare8 to reward ad viewers with mobile credit. James Macfarlane, Group CEO of PMConnect, says:

> *"I'm not surprised at the privacy backlash. We've seen the gathering of user data go from something useful to something that has turned into exploitation. But it's good to see new ideas. Weare8 is an interesting one. In fact, we're working with them on expanding the rewards so that customers use their credit to buy services like Netflix."*

06

FINAL THOUGHTS...

For all the debate, it is still not clear how much end users care about data privacy. There is certainly a growing concern among users of tracking, perceived by some as surveillance. Yet, there is also evidence that plenty of people seem happy to trade personal information for 'free stuff'.

What is not in doubt is that the industry is changing. Cookies are on the way out. And Apple is using marketing campaigns to position itself on the side of data privacy for mobile apps too. This marketing may well shape the public's views over the next few years,

It is incumbent on industry stakeholders to find new solutions that give users a personalised experience and maximise return on investment for advertisers without harvesting data.

There is plenty of this work going on – and MEF members are at the heart of it. Join MEF's working groups on Personal Data & Identity and Mobile Content & Advertising to continue the debate and discussion.

Established in 2000, the Mobile Ecosystem Forum is a global trade body that acts as an impartial and authoritative champion for addressing issues affecting the broadening mobile ecosystem. As the voice of the mobile ecosystem, it provides its members with a global and cross-sector platform for networking, collaboration and advancing industry solutions. The goal is to accelerate the growth of a sustainable mobile ecosystem that delivers trusted services that enrich the lives of consumers worldwide.

Launched in 2015, MEF's Future of Messaging Programme is a dedicated industry programme that promotes a competitive, fair and innovative market for mobile communication between businesses and consumers. Programme participants represent different regions and stakeholder groups working collaboratively to:

- Produce and publish best practice frameworks, papers and tools to accelerate market clean-up and limit revenue leakage
- Educate buyers of messaging solutions
- Promote business messaging as a premium and trusted channel
- Drive knowledge across the ecosystem of new platforms, technologies and procedures to address the evolving messaging landscape
- Develop the value-chain to support new use cases

MEF

MOBILE ECOSYSTEM FORUM

MOBILEECOSYSTEMFORUM.COM

MEF   MOBILE ECOSYSTEM FORUM