White Paper | October 2024

Navigating Recent Trends in Privacy, Measurement, and Marketing Effectiveness

LYNCHPIN

E: info@lynchpin.com
T: 0345 838 1136
W: www.lynchpin.com

Table of Contents

About Lynchpin

Lynchpin is an independent analytics consultancy.

We help organisations including Canon, Hotel Chocolat, Channel 5, John Lewis, Johnson & Johnson, and Ticketmaster to use data to accelerate growth, increase sales & marketing efficiency and improve customer experience.

Lynchpin integrates data science, engineering and strategy capabilities to solve our clients' analytics challenges. By bringing together complementary expertise we help improve long term analytics maturity while delivering practical results in areas such as multichannel measurement, customer segmentation, forecasting, pricing optimisation, attribution and personalisation.

Our services span the full data lifecycle from technology architecture and integration through to advanced analytics and machine learning to drive effective decisions.

We customise our approach to address each client's unique situation and requirements, extending and complementing their internal capabilities. Our practical experience enables us to effectively bridge the gaps between commercial, analytical, legal and technical teams. The result is a flexible partnership anchored to clear and valuable outcomes for our clients.

Founded in 2005 with offices in Edinburgh and London, Lynchpin is privately owned by the management team. We operate independently of vendors to enable us to focus solely on what is in our clients' best interests, deploying our deep expertise in digital marketing, data science and CRM technologies across on-premise, hybrid and cloud deployments.

Overview

The themes of privacy, digital measurement and marketing effectiveness triangulate around a natural trade and tension: balancing the anonymity of our behaviours and preferences against the ability for brands to reach us relevantly and efficiently.

In this white paper our goal is to give you a practical and independent view of current industry trends and how to successfully navigate them.

We'll start by exploring the key privacy trends, driven by regulators, big tech and consumer behaviour, and how that is driving change.

Then we'll look at the practical impact that is having on how we measure digitally, what's changing and – equally importantly – what's not changing.

Finally, we'll explore how you can effectively measure and optimise marketing performance in the context of that change with the right blend of new and existing techniques.

Privacy Backdrop

The general global trend is that legislators are increasingly recognising the value and importance of protecting individuals' personal data.

However, those routes to protection are far from straightforward – especially when operating globally – with heady mixes of opt-ins, opt-outs and collisions between general and specific data protection legislation.

And the natural tension between protecting privacy and promoting competition means even the regulators can find themselves at practical odds with each other (or indeed themselves) when attempting to reign-in big tech for the benefit of society.

In this section we'll summarise the key legal and regulatory drivers for privacy and how that backdrop is developing in practical terms.

GDPR

The EU General Data Protection Regulation[1], the most established and influential (and indeed general) of the data protection regulations continues to be front and centre of a lot of privacy developments.

Since GDPR hit the statute books in 2018, a global driver of change has been the legal recognition that profiles based on the behaviours of individuals can represent personal data, and that a range of identifiers can indirectly identify those individuals.

Hence why digital measurement, that makes it relatively trivial to gather granular behavioural data linked to indirect identifiers such as cookies at mass scale, has come increasingly under the regulatory spotlight as personal data.

In theory the "R" in GDPR means it is a regulation – i.e. passed into law exactly as written in all EU member states (and the post-Brexit UK GDPR mirrors the EU GDPR exactly at present). However there have also been examples of different regulators in different member states taking stricter or less strict views on enforcement.

GDPR is ultimately anchored on establishing a clear purpose and legal basis for processing personal data, so it's not just what data is being gathered but also how it is being used that forms the crux of its application.

[1] EUR-Lex - 02016R0679-20160504 - EN - EUR-Lex (europa.eu)

ePrivacy Directive

Cookies and personal data can often be conflated: cookies don't always involve personal data but are still subject to consent if they are not "strictly necessary" under the ePrivacy Directive[2] in the UK and EU.

From a digital measurement standpoint this is important as anything stored on a device as an identifier, or that can be used in a similar way to an identifier stored on a device (e.g. device fingerprinting), commands additional consent requirements under ePrivacy that can be above and beyond what GDPR says. Notably while GDPR offers a number of routes to establishing a lawful basis for processing (consent being just one of those), ePrivacy *only* allows for consent.

ePrivacy is an EU directive as opposed to a regulation, which means member states legislated independently to meet the spirit of the directive, and hence there is more room for some interpretative divergence. However one aspect where there has been clear regulatory agreement is that cookies for analytics are not "strictly necessary" and hence do require consent.

The EU ePrivacy Directive from 2002 was due to be superseded by a new EU ePrivacy Regulation at the time GDPR came into force (2018)… however due to continual disagreements has not yet made it anywhere near the statute books and the lack of direct alignment between the two has arguably proved to be unhelpful.

In the UK, ePrivacy was enacted by the Privacy and Electronic Communications Regulations (PECR), which survived Brexit. This was due to be amended by a recent Data Protection and Digital Information Bill[3] in 2024 prior to this being halted by a change of government. The DPDI draft bill does have some interesting clauses that diverge from the EU, for example effectively allowing the usage of cookies for collecting behavioural data for the purpose of making website improvements without requiring consent.

CCPA (et al)

There is no federal approach to consumer privacy presently in the US, but increasingly a lot of alignment between state level legislation, with California effectively leading the herd with the California Consumer Privacy Act[4].

The principles are similar to GDPR in terms of avoiding blanket profiling and sharing of data, the main difference is more of an emphasis on opt-out vs opt-in. So, while the management of the provision of withdrawal of consent might be different to GDPR, the premise is very similar in terms of restricting the sharing of digital profile data.

[2] EUR-Lex - 02002L0058-20091219 - EN - EUR-Lex (europa.eu)
[3] Data Protection and Digital Information Bill (parliament.uk)
[4] California Consumer Privacy Act (CCPA) | State of California - Department of Justice - Office of the Attorney General

EU meets US

Did GDPR make Google Analytics illegal? No, but the undermining of a key agreement around the processing of EU personal data in the US did effectively make any US owned or operated cloud service technically illegal[5] in the EU for a period until a replacement scheme was agreed[6].

It's a good example of how a global internet and regional regulators results in a lot of impracticalities, and arguably also a signal for the practical need for convergence – which we're already seeing with the likes of CCPA gradually nudging further and further in the direction of GDPR, albeit with somewhat different language.

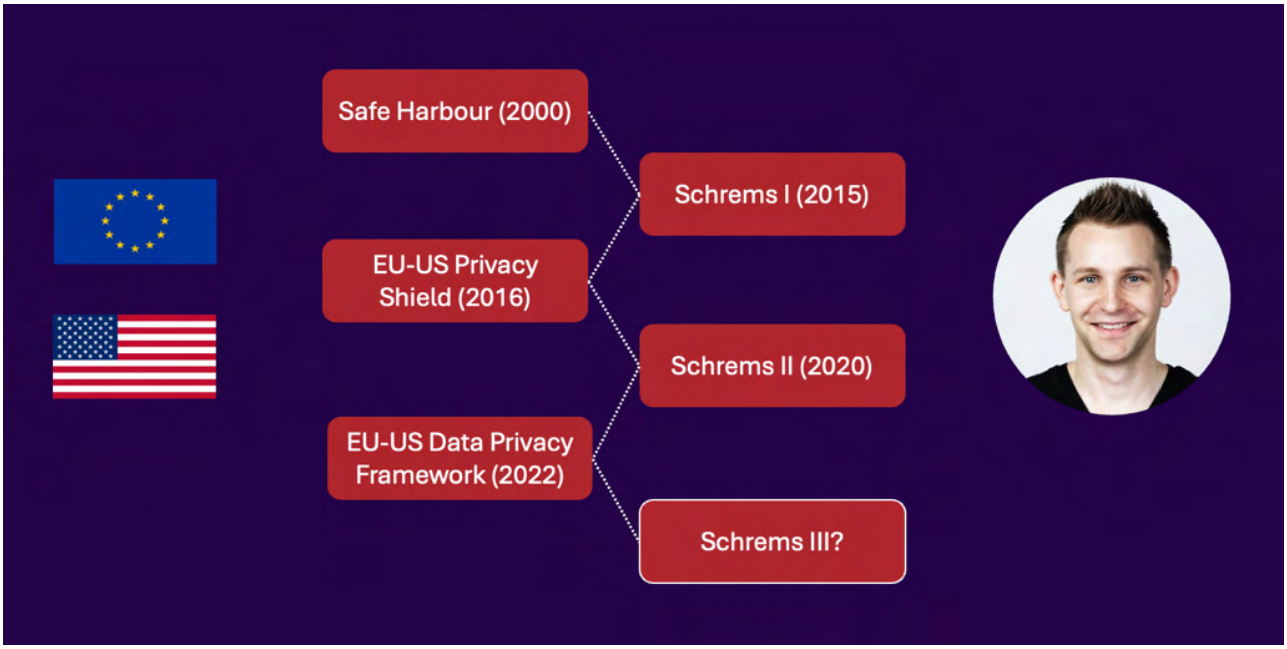


Figure 1: Schrems rulings and consequent impact on EU-US legislation

Competition

The irony is that the sharing of data, particularly across networks, has promoted competition and helped to slightly level the playing field for independent publishers and advertisers.

Meanwhile big tech (Apple, Google, Meta…) have their own highly consented first-party data set (we've all accepted Google/Meta terms and conditions at some point, right?) placing them at an even bigger advantage if it becomes harder for smaller players to engage directly in the market.

So while privacy regulators would love to see third-party cookies (and their associated cross-site profiling) die as soon as possible, competition regulators are wary of the scope for it to potentially

[5] The CJEU Judgement in the Schrems II Case (europa.eu)
[6] Questions & Answers: EU-US Data Privacy Framework (europa.eu)

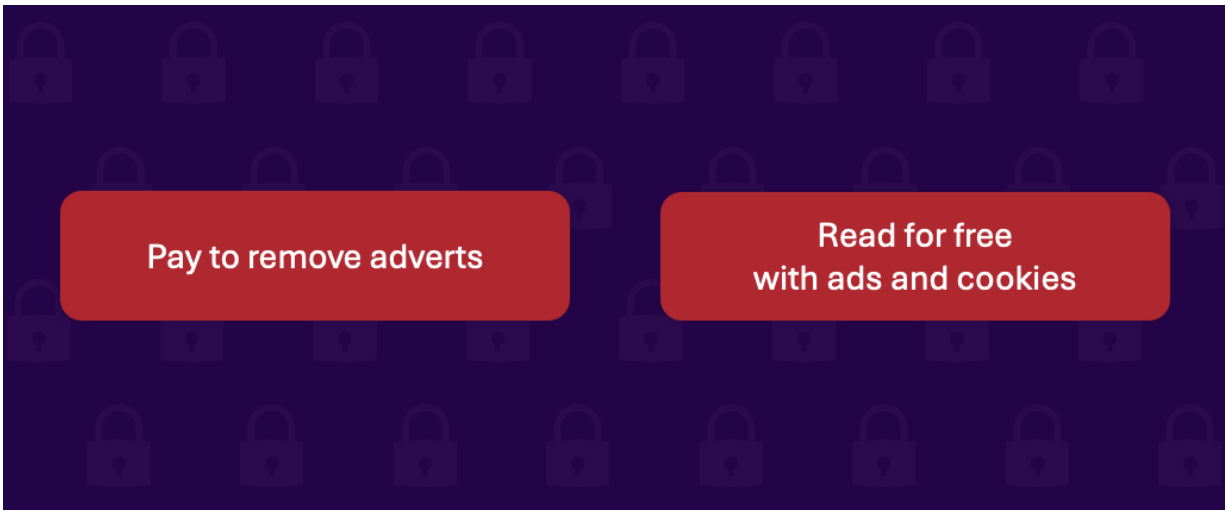
create an even less level playing field for publishers and advertisers. And Google – as a massive advertising network and the owner of Chrome - are right in the crosshairs of both.

The top and tail of Google's U-turn announcement[7] that they would continue to support third-party cookies in Chrome as opposed to deprecating them alludes rather strongly to being caught between competition and privacy regulators in a particular jurisdiction:

> *"Throughout this process, we've received feedback from a wide variety of stakeholders, including regulators like the UK's Competition and Markets Authority (CMA) and Information Commissioner's Office (ICO)…*
>
> *…We're grateful to all the organizations and individuals who have worked with us over the last four years to develop, test and adopt the Privacy Sandbox. And as we finalize this approach, we'll continue to consult with the CMA, ICO and other regulators globally."*

Consent or Pay

Some regulators have effectively accepted that curtailing the ability to sell targeted advertising could compromise the ability of publishers to continue to provide content for free. And while the principle of "consent or pay" (i.e. pay a subscription if you want to opt out of advertising tracking, otherwise you must opt in for advertising tracking to see content for free) clearly goes against the principle of consent set out in the GDPR, some are now flirting with the idea of guidance that could accept that as a solution.



[7] A new path for Privacy Sandbox on the web

In the UK, the Information Commissioner's Office (ICO) consulted in April 2024 with the industry around consent or pay, with some language suggesting they were at least somewhat sympathetic to commercial impacts of current restrictions[8]. However, they have not yet issued updated guidance following that consultation, perhaps related to a change of government in Westminster and the failure to get a new Data Protection and Digital Information Bill[9] passed prior to the election. Meanwhile, a significant majority of UK newspaper publishers have adopted consent or pay, either from a perspective of low regulatory fear or safety in numbers.

Meanwhile in the EU, the European Data Protection Board (EDPB) are grappling with similar issues, with some subtle contextual nuance starting to emerge around topics like e.g. what amount might be appropriate to charge that would still represent a "real" choice[10].

Consumer Response

Regulators influence but do not control consumer attitudes to privacy.

Whether it's opt-in or opt-out, the extent to which consumers want to even engage with a brand can come down to perceptions of trust and privacy.

81% of respondents to Cisco's 2022 Consumer Privacy Survey[11] agreed with the statement "I believe the way a company treats my personal data is indicative of the way it views me as a customer".

But how personal data is being treated can be challenging for consumers to comprehend[12] with a myriad of technical cookie preferences to navigate – and the scope for disconnect between what a brand says it will do and what it actually ends up doing based on a technical implementation with lots of moving parts.

Data on consent rates for cookies can show some extremely high variance swings across geographies[13], industries and traffic sources. But also, how the consent question is asked can profoundly impact those rates: user interfaces and the context in which they appear can easily (whether deliberately or accidentally) nudge users in a particular direction.

[8] ICO launches "consent or pay" call for views and updates on cookie compliance work | ICO
[9] Data Protection and Digital Information Bill - Parliamentary Bills - UK Parliament
[10] EDPB: 'Consent or Pay' models should offer real choice | European Data Protection Board (europa.eu)
[11] Cisco 2022 Consumer Privacy Survey
[12] Understanding of internet cookies among consumers USA 2022 | Statista
[13] Consent to cookies usage by country 2021 | Statista

Industry Response

Whatever the public messaging might be, ultimately data is money for big tech and there's a natural desire for them to have more rather than less.

Apple is to some extent simultaneously pushing a "privacy first" and "Apple first" agenda depending on how you perceive their motivations. iTunes and other platforms are increasingly walled gardens of first-party data for Apple. Meanwhile, they have led (via iOS and Safari) in restricting the data available to others – blocking third-party cookies by default and restricting other forms of measurement via intelligent tracking prevention.

Meta has perhaps been hit most directly from an advertising perspective by some of those changes based on their reliance on highly targeted advertising – and their primary response has been to encourage advertisers to share as much personal data as possible in response (e.g. hashed emails of customers) to re-enable their ability to join the dots.

Google sits in the middle of a lot in general and has been moving more gingerly in various directions to try and appease regulators while protecting its advertising revenue streams. They are attempting to be more explicit around consent attached to specific data points relating to how they might be used across the Google ecosystem. And their attempts to launch a privacy sandbox effectively shift the processing of more personal data into the browser on device, with less sharing of the underlying data underpinning profiles and targeting as a result.

Impact on Digital Measurement

The regulatory tide alongside industry and consumer response is impacting digital measurement, but more in some areas than others.

In this section, we'll consider the practicalities of what's changing now, what's not changing and what is coming over the horizon soon.

Debunking "Cookieless"

First-off, the phrases "cookie apocalypse" and "cookieless future" need some very clear context to avoid being unnecessarily dramatic.

Admittedly if you run an advertising network that is totally dependent on third-party cookies to profile the behaviours of individuals across the internet and then resell those audiences, then you'd be forgiven for seeing some existential challenges on the horizon.

But cookies themselves are not going away any time soon. They will still be core to the operation of most websites as the primary means of recognising that series of browser requests are coming from the same user: keeping us logged in as we move across pages, maintaining our shopping baskets and ultimately enabling any form of transaction.

And the first-party cookies that are used for first-party measurement and analytics are not going away either, they just need consent – which is legally not a new thing (ePrivacy is over 20 years old) – just a topic that regulators have been far hotter on in recent years.

The Two (or Three) Internets

When we look at digital analytics data, there's a common and understandable misconception that we're measuring one internet and one audience in the same terms. A user is a user, a click is a click, and it all sums up to a picture of what's happening.

In reality the figures we see from any digital measurement tool are an average of at least two different internets with different underlying rules of engagement.

Apple (Safari and iOS): blocks third-party cookies by default[14], automatically deletes first-party measurement cookies after hours/days/weeks depending on how sensitive it thinks they are, removes click identifiers that might identify an individual, requires an operating system opt-in for mobile apps to share data with third parties.

Google (Chrome and Android): does none of the above (yet).
Fundamentally and by design, you have less practical visibility of your Apple audience, especially

[14] Tracking Prevention in WebKit | WebKit

when looking at longer-term cause and effect. And if that audience is significant in volume, it can significantly skew the average.

And then there's the third (invisible) internet: the users that block all tracking using whatever tools they can find and/or use other browsers (e.g. Brave) that are even more privacy first than Apple or simply just opt-out or refuse to opt-in to any measurement.

Key Measurement Changes

Overall, there are three key changes taking place (at different rates across different ecosystems):

1. An increasing focus on gathering consented first-party data.
2. An increasing usage of machine learning to try and plug the gaps in consented data sets.
3. New ways of sharing context around preferences of users with less intrusion into their privacy.

Consented First-Party Data

For first-party measurement (i.e. your own digital analytics of behaviour on your own websites) then cookies are not going away, but they need opt-in consent. So the focus should be on making sure users are presented with transparent opt-ins for how tracked behaviours are being used.

Consent management is getting increasingly granular, as the same cookie value could potentially be used for very different purposes once that value passes into a broader ecosystem. This is the crux behind Google's Basic Consent Mode[15], enabling those flags of "how can this data be used" to be transmitted and hopefully respected alongside those data points.

Businesses can enhance their own first-party measurement by encouraging users to log into their website and mobile apps and capturing a stronger user ID based on that for first-party measurement.

One thing to watch out for however is the sharing of first-party data with other parties in a way that might breach the captured consent. A classic example of that might be passing a hashed email address of a converting user to Google[16] or Meta[17] to enable them to link it back to prior advertising exposure on their networks.

That's great for Google and Meta as it replaces a third-party cookie with something even stronger for tracking across websites (you don't "clear out" your email address that often). But not good for

[15] Set up consent mode on websites | Security and Privacy hub | Google for Developers
[16] About enhanced conversions - Google Ads Help
[17] About advanced matching for web | Meta Business Help Centre (facebook.com)

your users if they didn't opt in for their individual behavioural data to be shared with a third-party in this way.

Modelling the Gap

Even before cookie opt-ins, we never had 100% coverage from digital measurement (some users would use ad blockers that blocked any kind of tracking).

But as up-front consent has become the norm for first and third-party analytics, that non-consented gap becomes more significant and visible (e.g. the consent rate from your consent management platform).

Machine learning has been used for some time within advertising networks to try and fill the gaps and infer when something that couldn't be measured was "likely to have happened". It's not magic: it just uses the patterns in consented data to try and predict what was likely to have happened for the non-consented audience.

This is now moving into the realms of first-party analytics too, most obviously with modelled data in Google Analytics and Google Ads based on "cookieless pings" sent from users that don't consent to cookies when using their Advanced Consent Mode[18] functionality.

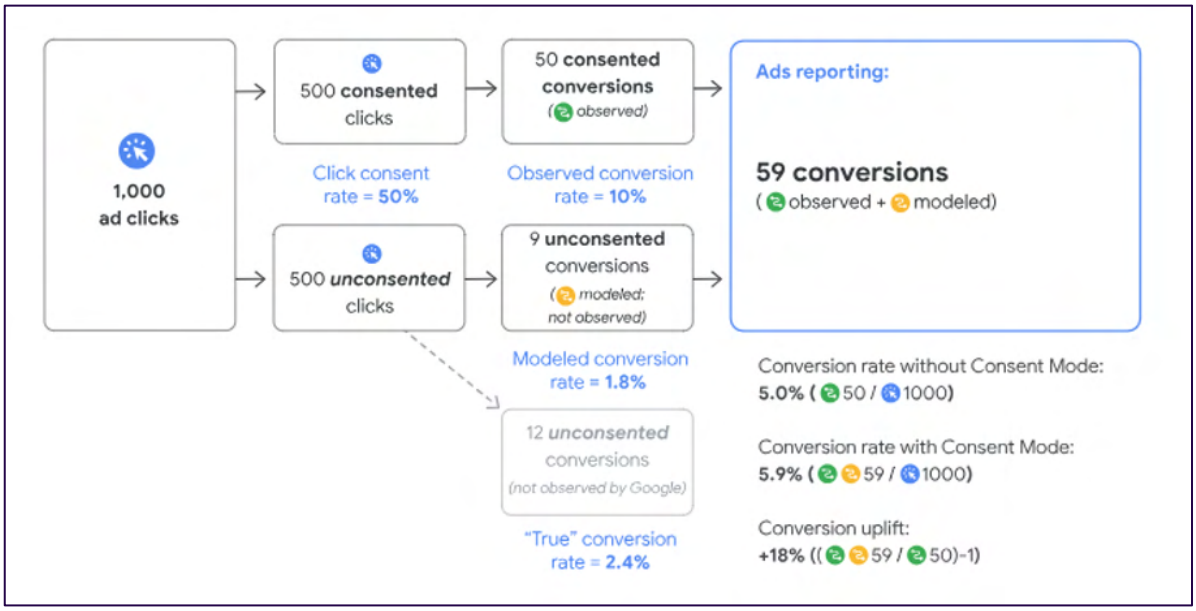


Figure 2: Example of modelled data in Google Ads

While sending data to Google with no cookie identifiers takes it out of the realm of ePrivacy/PECR, care should still be taken around what these cookieless pings might disclose – other identifiers are

[18] Set up consent mode on websites | Security and Privacy hub | Google for Developers

likely still there (e.g. IP address) that would require some lawful basis under GDPR to be established.

Sandboxes and Clean Rooms

Sandboxes and clean rooms are both ultimately ways of anonymising user data while sharing some context designed to improve relevance for users and advertisers.

The main difference is that a sandbox is more likely to live in a user's browser, whereas a clean room is more likely to operate as a centralised controlled environment where data is uploaded.

Google's Privacy Sandbox[19] is still subject to competition concerns and on a very limited roll-out for market testing. Ultimately, its purpose is to facilitate (the continuation of) several things:

1. Conversion attribution. Critically not by saying "this user converted", but "for this campaign, out of these number of clicks, this number converted". The role of the sandbox is to restrict the level of detail available – which can even include the timing of conversions – to make it credibly unlikely anyone could ever link the activity back to an individual.
2. Targeting. Being able to infer potential preferences about a user that might influence what kind of offer they would be receptive to. Whereas previously the underlying behaviours that might infer those preferences were shared across advertising networks, the role of the sandbox is to make the inference and then disclose (to the user and to advertisers) what interest buckets (or "topics") the user falls into.
3. Re-targeting. Like attribution, the goal here is to enable an advert to be shown to a group of users that have engaged previously without disclosing the identity of any of those users.

Does Apple have a sandbox? Yes and no. SkAdNetwork[20] (SKAN) is basically a sandbox for measurement, in that it achieves the same anonymisation of campaign-level attribution. There's no equivalent at this stage for targeting or re-targeting; equally, unlike Google, Apple is not an advertising company so may not be equally motivated to provide such functionality. Hence the Chrome/Android vs Safari/iOS worlds could continue to diverge.

[19] Privacy Sandbox | Google for Developers
[20] SKAdNetwork | Apple Developer Documentation

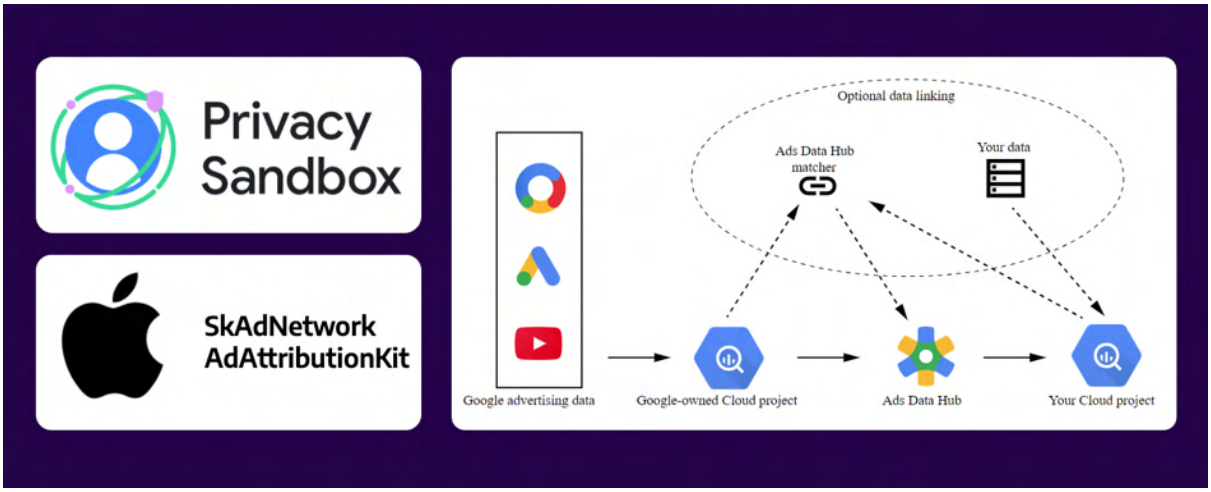


Figure 3: The sandbox landscape – Google vs Apple

Clean rooms operate more between larger brands and advertisers, or between established advertising networks, and use an independent entity to deliver anonymisation by grouping and encrypting. These sorts of exchanges are not new, but the level of scrutiny on the privacy enhancement is likely to be ever-increasing as more first-party data is injected into these environments.

Digital Measurement - Changes, Impact and Recommendations

When thinking about impact, it's worth starting off with a view of what your browser/device market share looks like between Apple/Google/Other – that tells you e.g. how much Intelligent Tracking Prevention (ITP) is already compromising your data and how important Google's Privacy Sandbox could be to your advertising targeting strategy.

Start with a focus on making sure your own first-party measurement is as consented and as complete as possible – and consented specific to how the data will actually be used, not just the fact an identifier exists in a cookie. Make sure all your click activity is properly tracked in your own analytics with campaign tracking parameters.

You can enhance your own first-party data however by capturing a stronger user ID when a user is signed in, and particularly in the Apple world that can substantially increase accuracy.

Then it's critical to make sure consent is acted on consistently: if a user has not opted in to their data being shared with a third-party like Meta, that needs to apply whether it's client or server-side measurement and whether the identifier is a cookie or a hashed email address.

Finally, ultimately the functionality of privacy sandboxes will be utilised by the vendors and networks that start increasingly using them for targeting/measurement/re-targeting as their third-party cookie pools start to diminish further. The more up-to-speed you are with the latest versions of their technologies, the more ready you will be to take advantage of the functionality as it lands.

Driving Marketing Effectiveness

We've seen how digital measurement and the ability to drive relevancy from targeting and re-targeting is changing. In this final part we consider what that means for driving marketing effectiveness and making good choices on where to invest.

Third-Party Cookies – Much of a Loss?

Whilst the AdTech industry might lament the "cookie apocalypse" in relation to the demise of third-party cookies, in practical marketing terms is there really much to cry about here?

A counterpoint might be that we're lamenting something that's either long gone, or wasn't that good in the first place:

1. The demise of third-party cookies is already here for the Safari/iOS internet. So, you've already been living in that "(3rd party) cookieless future" for likely a substantial proportion of your userbase.
2. Third-party cookies are/were used a lot for measuring and attributing the post impression/view "impact" of display. But ultimately a post-view conversion – especially with a long tracking window of months - never proved any incrementality, and for network advertising having confidence that the initial advertising view was actually an advertising view as opposed to just a cookie drop could be doubtful.

Certainly, some conveniences and levellers are going. Perhaps smaller and more niche advertisers are the most impacted, losing the ability to quickly strike up a look-a-like model with a network by sticking a third-party tag on their site.

Increasingly, advertising use cases such as retargeting, audience exclusions and look-a-like targeting are being fulfilled by the activation of first-party data as opposed to using third-party cookies.

Third-party cookies are just a technical means of sharing data, and this "activation" is ultimately no different when media channels are being used, albeit using different identifiers and data points. Notably from a privacy perspective, personal profiles are still being shared when hashed email addresses are used to match audiences.

Attribution

Single-touch (likely last-click) and multi-touch (algorithmically weighted across all the touchpoints leading to purchase) attribution is still going to be a critical tool for understanding what is and is not working from a digital marketing perspective.

Post-click measurement from your first-party digital analytics tool is not going away, and still represents a controlled and more importantly neutral source for measurement.

However, it is subject to some change. And Apple's curtailment of cookie durations means longer attribution windows become less reliable to measure, potentially reinforcing the role of attribution in driving shorter-term optimisation outcomes.

Figure 4: Example of customer journey with attribution constraints

The main change is around post-view attribution (i.e. this specific user saw this ad on this site and then converted on another site). Doing this at an individual level is already constrained due to third-party cookie curtailment from Apple, and if Chrome reduces or eventually removes third-party cookie support that capability will essentially disappear.

Privacy sandboxes will likely help in terms of campaign-level, single-touch attribution (i.e. how many people that saw this ad went on to convert), but that will need to be an overlay to a post-click model rather than integrated at a user level based on how deliberately anonymised the data set will be.

The ROI Question

So, if attribution is getting more challenging to do holistically, does that mean it's going to get harder to measure and assess Return On Investment?

Another way of looking at it is that attribution has always been better at understating shorter as opposed to longer-term impact and has always been better at measuring the bottom of the funnel (which tends to be more directly measurable) than the top of the funnel. Not to mention it being very much focused on digital channels.

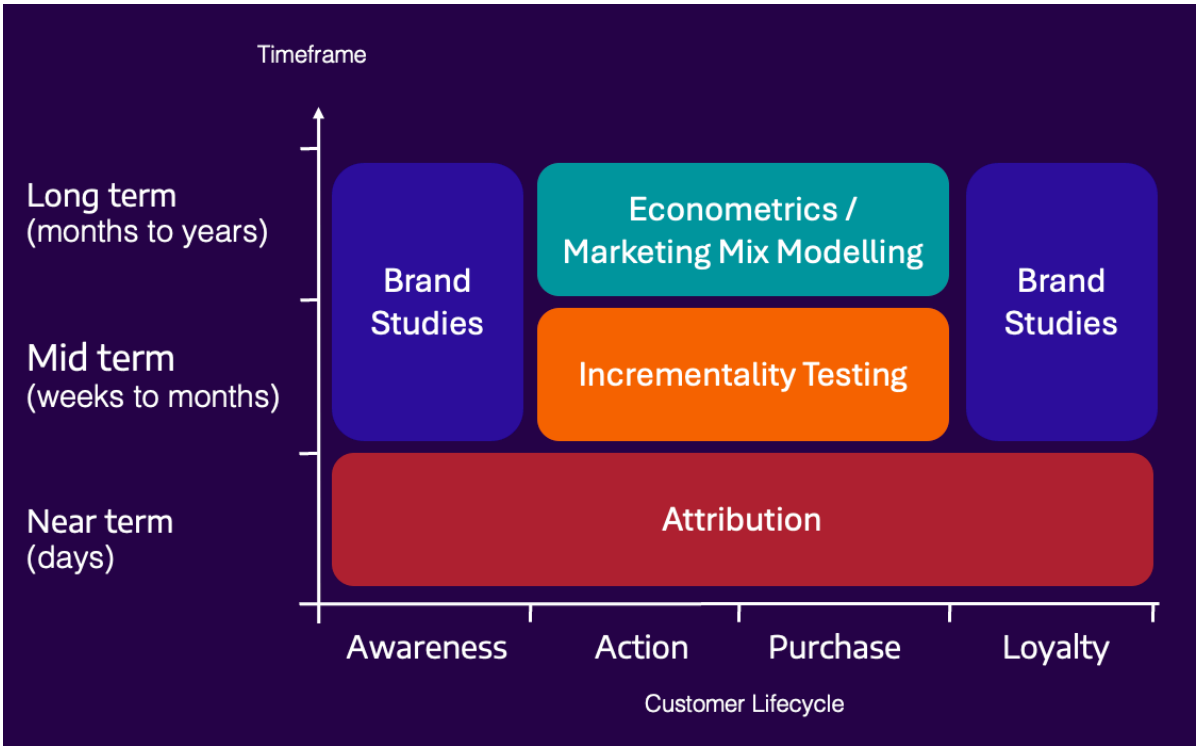


Figure 5: Measuring marketing impact by timeframe and across lifecycle stage, adapted from the IAB and Econsultancy

Reframing the question, it's worth reconsidering what tools and techniques are most relevant for answering the ROI question, and for a lot of marketers the answer will be more than one.

Which brings us to Econometrics, MMM and Incrementality Testing.

Econometrics and MMM

Econometrics and MMM (media or marketing mix modelling) are techniques for understanding the potential cause and effect of investments on outcomes. They essentially use historical data to build a predictive model that can forecast what would be likely to happen as an outcome for a particular profile of investment.

The terms are sometimes used somewhat interchangeably, but can indicate the scope of inputs and outputs: Econometrics typically indicating the broadest scope of inputs, including broad economic indicators; Marketing Mix Modelling more focused on the 5 Ps of Marketing, so including things like pricing and promotions; and Media Mix Modelling more constrained to focus on which channels marketing spend is being deployed in.

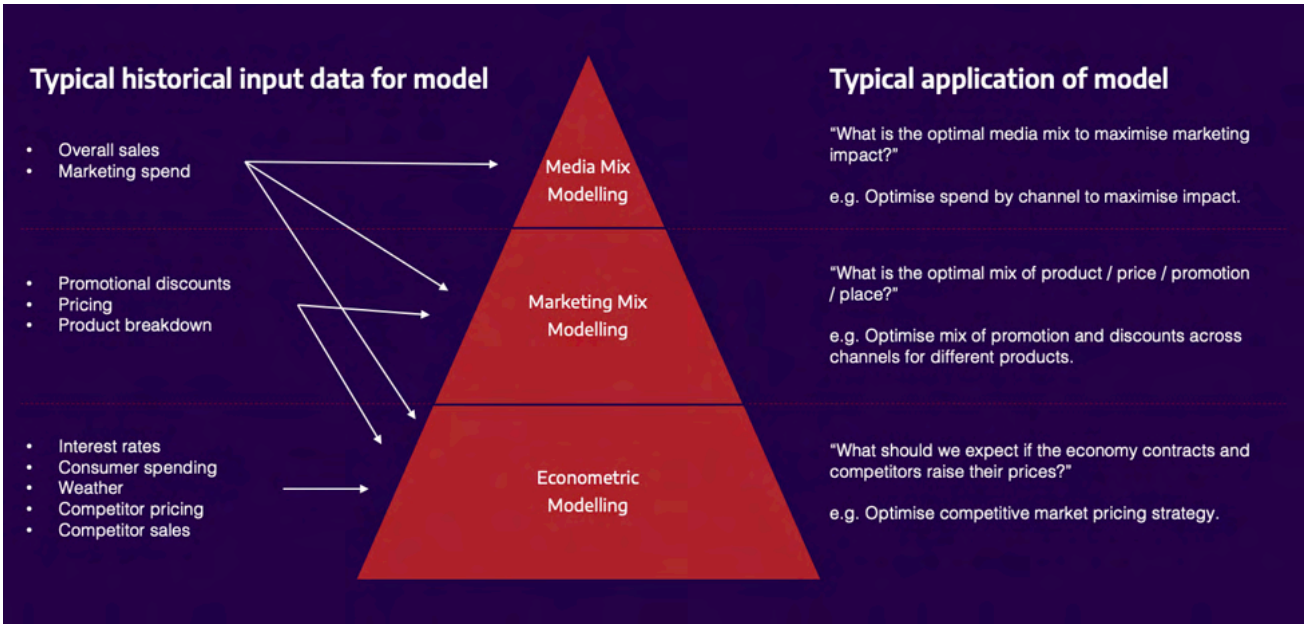


Figure 6: Typical inputs and applications of MMM and Econometric modelling

Irrespective, one of the simultaneous strengths and weaknesses of an approach like MMM is that it does not rely on user-level data – it simply looks at trends of inputs and outputs such as investment levels, promotions and sales.

The weakness of this is that it doesn't work well for isolating the impact of very specific granular pieces of activity, especially within digital channels. So it's certainly not a replacement for attribution when looking at in-flight campaign optimisation of keywords or placements.

But it's biggest strength is increasing in the context of the curtailment of direct upper-funnel measurement: it doesn't matter if you can measure the individual responses of individuals or not, as long as you know how your spend varied over time you can start to model the incremental value of it over a baseline of not marketing at all, and use that to optimise the investment mix across online and offline channels.

Incrementality Testing

Whereas Econometrics and MMM focus on modelling and forecasting the longer-term relationship between a range of inputs and outputs, incrementality testing is focused on proving the causality of a specific piece of activity.

Sometimes called control experiments, incrementality tests rely on establishing an audience that do not receive that piece of activity and then measuring the increase in e.g. sales revenue arising from an audience that did receive the activity.

Incrementality testing can be underpinned by cookies or other customer identifiers – indeed the most established form of it is in direct marketing channels such as email, where a pool of email

addresses is reserved as a control group and don't receive the email. But it can also work by supressing activity in particular geographic areas where direct customer identification is not viable – which could get increasingly relevant in situations where cookies are being increasingly curtailed across advertising networks.

Balanced Approach

For large multichannel advertisers, a balance of results from multi-touch attribution, incrementality testing and MMM has always offered the most comprehensive view across shorter and longer-term impact and different level of granularity of activity (e.g. channels vs keywords).

So, what's changing in that balance?

Attribution has always been focused on measuring up from the bottom of the funnel. That visibility is now being constrained in 3 senses: a less complete overall sample of user data due to opt-in consent requirements for measurement, a more restricted view of post-click impact based on Intelligent Tracking Prevention, and less visibility of post-impression impact due to the curtailment of third-party cookies.

That means for understanding the impact of anything further up the funnel, techniques like incrementality testing become more important, and control pools may need to be defined more at a geo rather than cookie-level.

Finally, MMM is simultaneously becoming more accessible (e.g. with open-source frameworks such as Robyn[21]) and more sophisticated – with the practical demands and capability to overlay seasonality and achieve more granularity (e.g. daily/weekly basis) to make it more actionable.

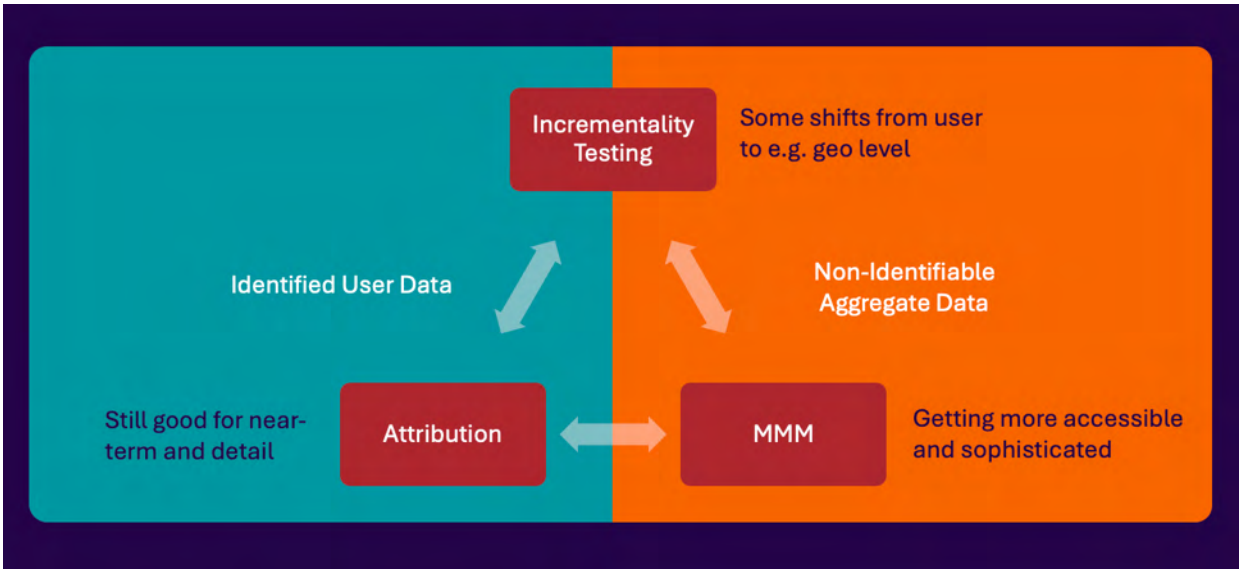


Figure 7: Data visibility and measurement techniques – their roles within a balanced approach

[21] Robyn (facebookexperimental.github.io)

Summary

While regulators juggle the demands of privacy vs competition and freedom vs free content, the trends are all towards increasing transparency and more granular consent for users.

New technologies such as server-side tagging, advanced consent modes and advanced customer matching have the scope to either enable or mask that transparency depending on how they are deployed, meaning some quite subtle technical choices can lead to very different privacy (and hence compliance) outcomes.

Digital measurement needs to be seen both through the lens of what can and cannot be directly measured in a consented world and the increasing divergence between the Apple and Google (and other) worlds of measurement.

And the balance of techniques required to assess and optimise marketing effectiveness will for many need to tip more towards things like MMM and testing to avoid an increasing bias towards the bottom of the funnel.

Practical Tips

1. Start with the context of your own measurement universe – what's your mix of Safari/iOS vs Google/Android vs Other, app vs website, online vs offline marketing channels.
2. Get your own first-party measurement data in order: consented, complete in terms of campaign tracking parameters, enhanced with other stronger user identifiers where relevant.
3. Irrespective of the background regulation or the mode of transfer, be transparent with users about how and when you're sharing that first-party data with other vendors, publishers and networks.
4. Keep an eye on how vendors and networks are evolving their technologies to take advantage of things like privacy sandboxes as they emerge, but also be conscious that ultimately privacy should be going up (less sharing) and granularity going down (less visibility of individual behaviours) as a result of this shift.
5. Consider what the right blend of multi-touch attribution, incrementality testing and MMM might be for your marketing mix, and how that balance might be shifting as top of funnel direct digital measurement becomes less accessible.

Need support with any of the issues raised in this paper?

Speak to a subject matter expert from our Leadership team today

info@lynchpin.com

0345 838 1136

LYNCHPIN