



# *Building a digital marketing roadmap to the post-cookie era*

**Part 1:** *Where do we stand?*

# Summary

© fifty-five - September 2021

**3** Why you should read this guidebook

**4** About fifty-five

**5** About the authors

**6** A new countdown to the privacy-safe world

1. *Where and why it all started*
2. *A new privacy-safe digital landscape*
3. *What does it mean for brands?*
4. *What are these new buzzwords about?*

**18** How to identify the impacts on all the data value chain

1. *Why does it matter and where to start?*
2. *What are the impacts on my activities and use cases?*
3. *Which part of my audiences and media strategy is at risk?*
4. *Is my organization ready?*

**30** Conclusion

**31** Case Studies

**34** Glossary

*Over the past few years, digital marketing has relied on first and third-party cookies. However, cookies and other existing trackers usage is facing growing limitations from regulators, tech players, and users themselves. This has made it mandatory to redefine online data collection, activations, and measurement while answering users' expectations for more privacy.*

At fifty-five we help brands answer the numerous questions this new post cookie era poses, and prepare them for a smooth transition. Despite Google's recent postponement of its phase out of third-party cookies support in Chrome, we believe that now is the time to define and roll out a transition strategy. The plan will have to be relevant to your marketing context and ready to tackle the existing privacy challenges.

**To help you solve those complex issues, we've gathered our analysis and experience in this two-part guide:**

### **Part 1: Where do we stand?**

- **Understand** what this post-cookie and privacy-safe world is about

- **Identify** how this new marketing world being shaped will impact the deployment and performance of your current digital marketing use cases

### **Part 2: Take over the roadmap**

- **Identify and understand** what the new solutions on the market are for and how they can help overcome new data collection, activations and measurement limitations
- **Kick off** your transition into the post-cookie era and identify the key steps and best practices depending on your specific context



We help brands leverage data and technology to craft superior brand experiences.

fifty-five is a new breed of data company that helps brands leverage data and technology to improve marketing, advertising, and customer experience, through a combination of specialized consultancy and technology services. fifty-five was founded in 2010 by former Google executives and is now a proud member of You & Mr Jones, the world's first Brandtech group. Headquartered in Paris, fifty-five is a global partner to its blue-chip clients, with offices in New York, London, Geneva, Hong Kong, Shanghai, Shenzhen, and Taipei.

---

Learn more on [fifty-five.com](https://fifty-five.com)

Or contact us: [contact@fifty-five.com](mailto:contact@fifty-five.com)



Strategy Consulting



Data Architecture



Media Consulting



Customer Experience



**Jean-François  
WASSONG**

*Partner, Chief Innovation  
& Technology Officer*  
[jean-francois@fifty-five.com](mailto:jean-francois@fifty-five.com)



**Charles  
DUENAS**

*Expertise  
& Innovation Manager*  
[charles.duenas@fifty-five.com](mailto:charles.duenas@fifty-five.com)



**Guillaume  
TOLLET**

*Executive Director  
& Privacy Specialist*  
[guillaume.tollet@fifty-five.com](mailto:guillaume.tollet@fifty-five.com)



**Sarah  
SOUFFLET**

*Data Project Lead*  
[sarah.soufflet@fifty-five.com](mailto:sarah.soufflet@fifty-five.com)

[contact@fifty-five.com](mailto:contact@fifty-five.com)



# *A new countdown to the privacy-safe world*

1. *Where and why it all started*
2. *A new privacy-safe digital landscape*
3. *What does it mean for brands?*
4. *What are these new buzzwords about?*

## Where and why it all started

Google, Apple and other big tech players are largely setting the pace of the marketing industry today and moving towards a world where individuals' privacy should be better respected. One should look in the rear-view mirror to understand where this started.

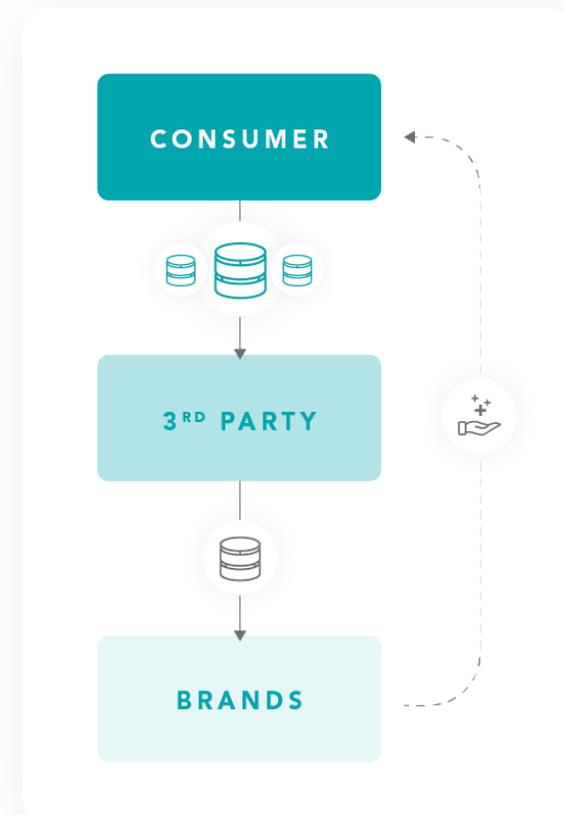
Measurement, activation, and other marketing practices require efficient data sharing among different parties:

- **Users** browse the internet looking for information, content, and products, and in doing so provide rich information on their profile
- **Third parties** (such as advertising

players) collect, aggregate, and analyze user-related data, and market its use

- **Brands** leverage data and marketing services offered by third parties to create digital content and to support their activities

**Cookies** have long been the technical underliers to enable these data-sharing mechanisms, but without full acknowledgment or consciousness from the users, resulting in a perceived unbalanced value exchange. In their most intrusive form, when used as a third party, cookies no longer fit new standards in terms of user control, browser security,



or regulatory compliance. As a result, they are now living their twilight years.

**Is it the end of digital marketing? No. Digital Marketing existed before cookies were so widely used.** We believe a privacy-safe environment can be created with dedicated technical advertising solutions while cookies should, in the future, serve only functional purposes.

## Cookie

A cookie is a small file of letters and numbers that is downloaded onto your computer when you visit a website. This token is then reused for any subsequent visit to help the server keep track of the user. Cookies make it possible to gather and store data about users' browsing behaviour, which can later be reused during these users' subsequent visits (user logins, for instance).

> [See glossary page 34](#)

## A new privacy-safe digital landscape

A new privacy-safe digital landscape has formed slowly over time, thanks to regulators and systemic digital players piling up restrictions. This new frontier is being shaped to try to adjust the unbalanced data exchange.

Cookies and other available trackers are indeed attacked by the well-known “triple cookie restriction”: **legal** (GDPR, CCPA, upcoming e-Privacy); **technical** (browsers and operating systems); and **behavioral** (use of ad blockers and cookie notice blockers). In parallel, the large logged-in environments — Google, Apple, Facebook, and Amazon — take advantage of these privacy restrictions to further enclose their environments,

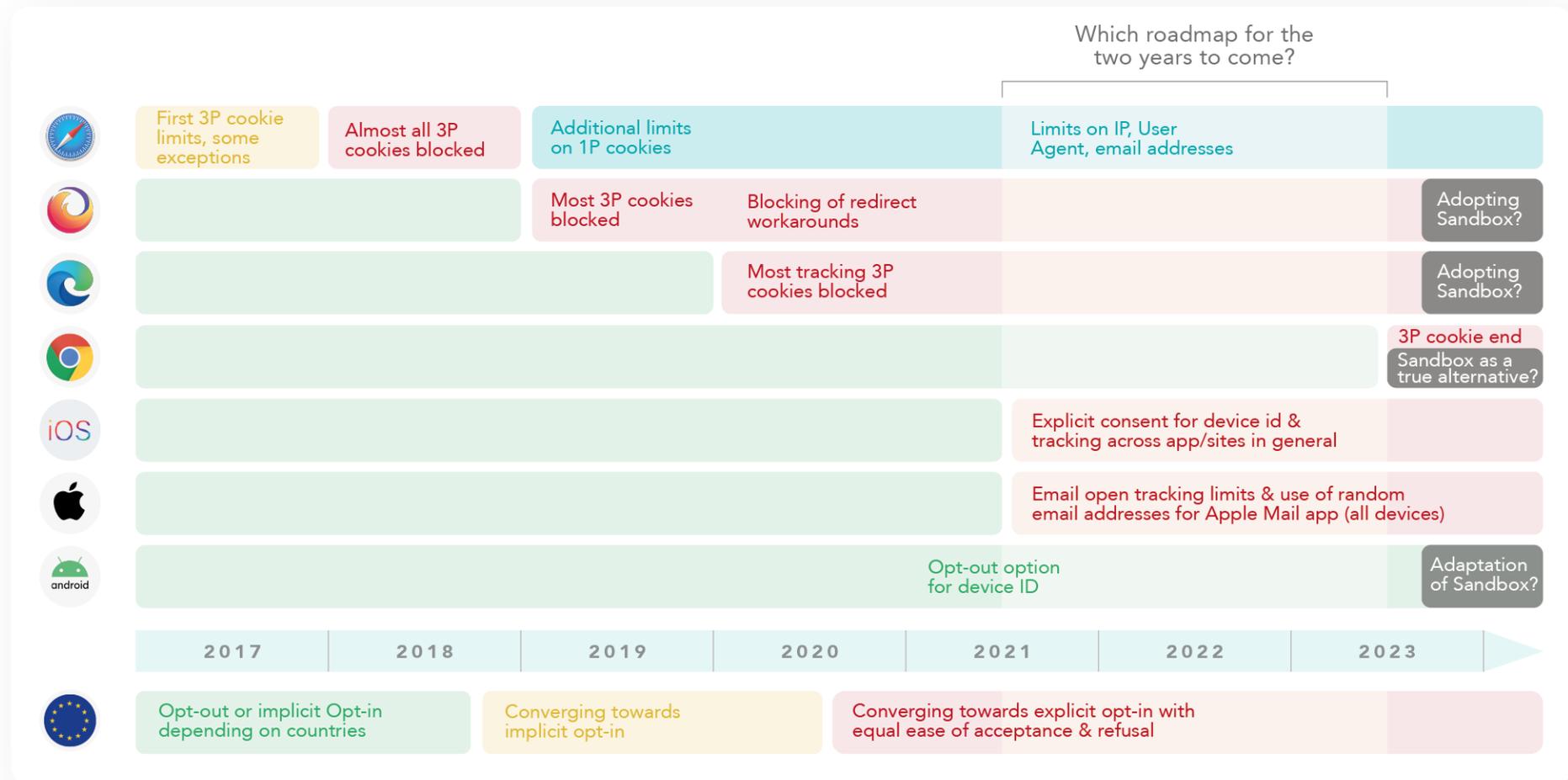
**no longer enabling marketers to track users across platforms** (e.g., measuring Facebook on Apple devices).

### GDPR

The General Data Protection Regulation is the latest European regulation on personal data protection, which was enacted in 2016 and came into force in 2018. It aims at unifying legislation across the EU, and especially at giving power back to European citizens regarding the use of their personal data while making holders of such data accountable.

> [See glossary page 34](#)

## Apple started its race for privacy 5 years ago: most browsers have followed suit, with Google lagging behind but bound to align slowly



Looking at this historically, what is notable is the **“domino” effect** of privacy-leading players such as Apple on others. For instance: Firefox and EDGE followed Apple for third-party cookies, and Android followed iOS for mobile device identifiers — although in a less impactful way for now, only subjecting it to an opt-out and not an opt-in.

**2021** has been a milestone year, with **big impacts on a large perimeter of data** thanks to almost-simultaneous new regulations and Apple’s moves. Many countries in the GDPR zone have started to make it compulsory to have explicit consent for cookies, and **to display a “refuse” button on the first layer of the cookie banner**, decreasing **consent rates** from close to 99% to around 60%, and concerning all trackers, all browsers, and all devices. **Apple also acted as a regulator**, adding its

own **App Tracking Transparency (ATT)** consent pop-in to iPhones to restrict the **IDFA** even more harshly, which can be seen as the equivalent to third-party cookies for Apple mobile apps. And only a few months later, considering itself now “done” with cookies and IDFA, **Apple started looking into and restricting what are emerging as alternatives to cookies** for some players: IP addresses used in digital **fingerprinting** techniques, and email addresses collected online and matched with people-data pools.

Aside from all this, Google lags behind. Its two-year plan to phase out third-party cookie support on Chrome and replace them with the **Privacy Sandbox**, a solution supposed to be on par in terms of performance, but promising to be more preserving of user privacy, is being delayed by several factors. In the past months, it became clear the

technical solution, but also its **perceived image by the market, would not be widely enough adopted**. Browsers (Firefox), websites (WordPress, Amazon) and regulators (European Commission, United Kingdom’s Competition and Markets Authority) were vocal about how it would not at all increase privacy, and bore a real risk of competition bias. So what to do now? Find new sophisticated trackers not blocked by Apple and Firefox? Keep business as usual on Chrome and postpone investments in privacy projects? Despite being somewhat delayed, **this privacy trend has impacts today and is not to be stopped**. There is no time to procrastinate nor to keep bad, outdated data habits.

**This paper explains what to do now to generate value and prepare for the future of data.**

## *What does it mean for brands?*

### How is tracking impacted?

**To simplify, we'll talk about "cookies" broadly in the rest of this paper, but all kinds of trackers are impacted by these new regulations and technical restrictions.** The "cheat sheet" on the next page shows considerable heterogeneity of situations depending on the device and browser. But overall, these limitations translate into **decreased availability of user-related information.**

Amongst all restrictions, what Apple brought in 2021 with its new policy called "**App Tracking Transparency**" is often misunderstood. It has falsely been seen as only limiting the use of IDFA, iOS device

identifiers, which impact brands that want to drive traffic to their mobile app such as e-retailers. But brands advertising on iOS apps to drive traffic to their website in Safari are also strongly impacted. In a statement to app developers, Apple said "you'll be required to ask users for their permission to track them across apps and websites owned by other companies". For instance, an **ad** on the Facebook app **that redirects to a website** to generate engagement will no longer be able to track users with identifiers unless Facebook obtained in-app consent.

### IDFA

The Identifier for Advertisers (IDFA) is a unique identifier linked to an Apple mobile device, whose purpose is to target a unique user in order to follow their online behavior and display personalized content. The IDFA was used, for example, to retarget a user according to certain actions he or she may have had on a mobile app.

[> See glossary page 34](#)

## Cheat sheet: Cookies & other trackers crumble *(September 2021)*

	COOKIES 3 <sup>RD</sup> PARTY	COOKIES 1 <sup>ST</sup> PARTY	OTHER TRACKERS
Web	 All known trackers blocked	Limited restriction (45 days)	NA
	 All known trackers blocked	No restriction	NA
	 Fully blocked	- Normal cookies > 7d renewable - Cookie w/ click ids > 24h	Limits on IP & email addresses for Fall '21
	 No restriction <span style="color: red;">▶ Phase out in 2023</span>	No restriction	No restriction
	 Inherits Safari restrictions	Inherits Safari restrictions	Limits on IP & email addresses for Fall '21
App-to-App & App-to-Web	DEVICE ID (IDFA/AAID)	CLICK IDs IN URLS	OTHER TRACKERS
	 No impactful restriction, so far, only opt-out option	No restriction	NA
	 Subject to ATT consent, low rates expected	Subject to ATT consent, low rates expected	Limits on email addresses for Fall '21

## What does it mean for marketing data?

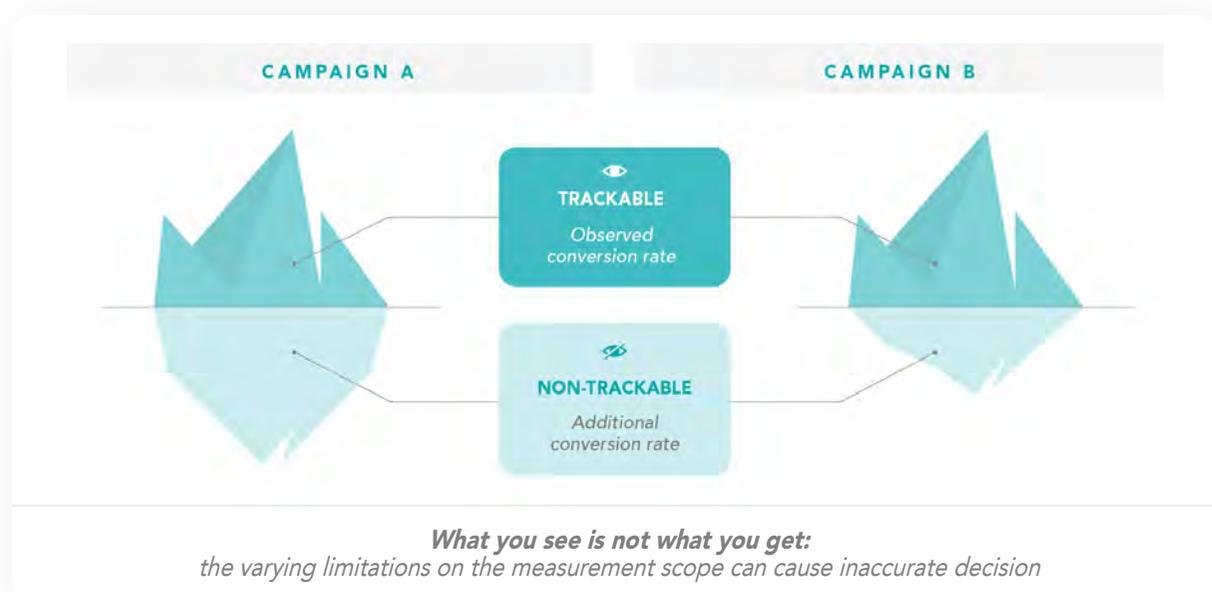
Until recently, measurement aimed for **high data granularity** and the ability to track users and all their interactions **everywhere**. Cookies and other tracker restrictions, as well as increasingly-enclosed walled gardens, make it more difficult to get global, consistent, and reliable online marketing measurement, instead resulting in **data gaps and biases**.

- **Volume.** Direct audiences and data volume reduction by each of the three cookie restrictions. The cuts may come very quickly, for instance in direct losses in retargeting audience volumes for all users that do not consent to cookies on your website, or to Apple ATT pop-in on your app.

- **Trust.** Even more importantly than volume losses, the variety of situations impacted lead to an **unknown and almost random quality, significance, and depth** of the collected data. This may lead to questions such as: Is this campaign performing poorly because its message is inefficient, or because it targeted users more likely

to have cookies blocked? It is already difficult enough to know what we measure, and whether the final data is representative or not.

- **Precision.** Less granular data, more aggregates. Not being able to precisely tie an action to a user leads to **less granularity** and fewer



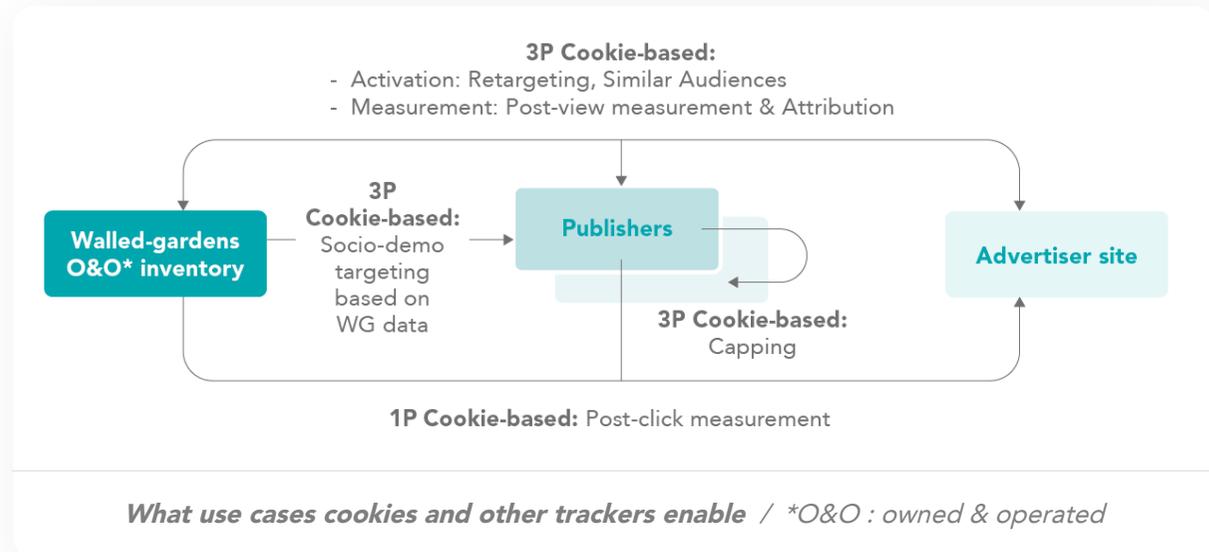
dimensions available. You might still know that 2,000 users purchased on your site, but you don't know which campaign influenced the purchase, and you'll have less socio-demographic information. Instead, both the regulators and privacy-aware developers such as Apple and Google **Privacy Sandbox** see, in the concept of **data aggregation**, a way to de-identify data.

- **Extent.** Scattering and risk of overlaps. Dealing with several walled-gardens inventories was already driving advertisers mad when trying to avoid overlaps and obtain holistic, consistent measurement. Adding other factors to the equation that make data even more heterogeneous and irreconcilable (devices, browsers, different consent rates depending on the sites/app) further increases

the risk of **scattering and overlaps**. For instance, Facebook media could already no longer be tracked with a Google ad server such as Campaign Manager, but now distinct **attribution** rules and embedded modelling in each platform make for additional layers of complexity.

### What does it mean for your activities?

At an operational level, this means many added-value media tactics such as frequency capping or retargeting will experience strong perturbations because the cookie-based data on which these tactics rely is no longer available — or at least not in the same volumes as before.



At a more high-level view, measurement and activation of all marketing initiatives will be impacted, with risks on ad efficiency and less data to optimize online journeys. User experience also bears the risk of being disturbed; not only will content personalization be more difficult, but asking for consent everywhere in quite invasive ways is already perceived as harassment by users.

### Consent Rate

The consent rate is the number of consents given (clicks on “accept” on the CMP banner) divided by the number of CMP banner impressions.

> [See glossary page 34](#)

## What are these new buzzwords about?

**CONCEPTS & TRENDS**

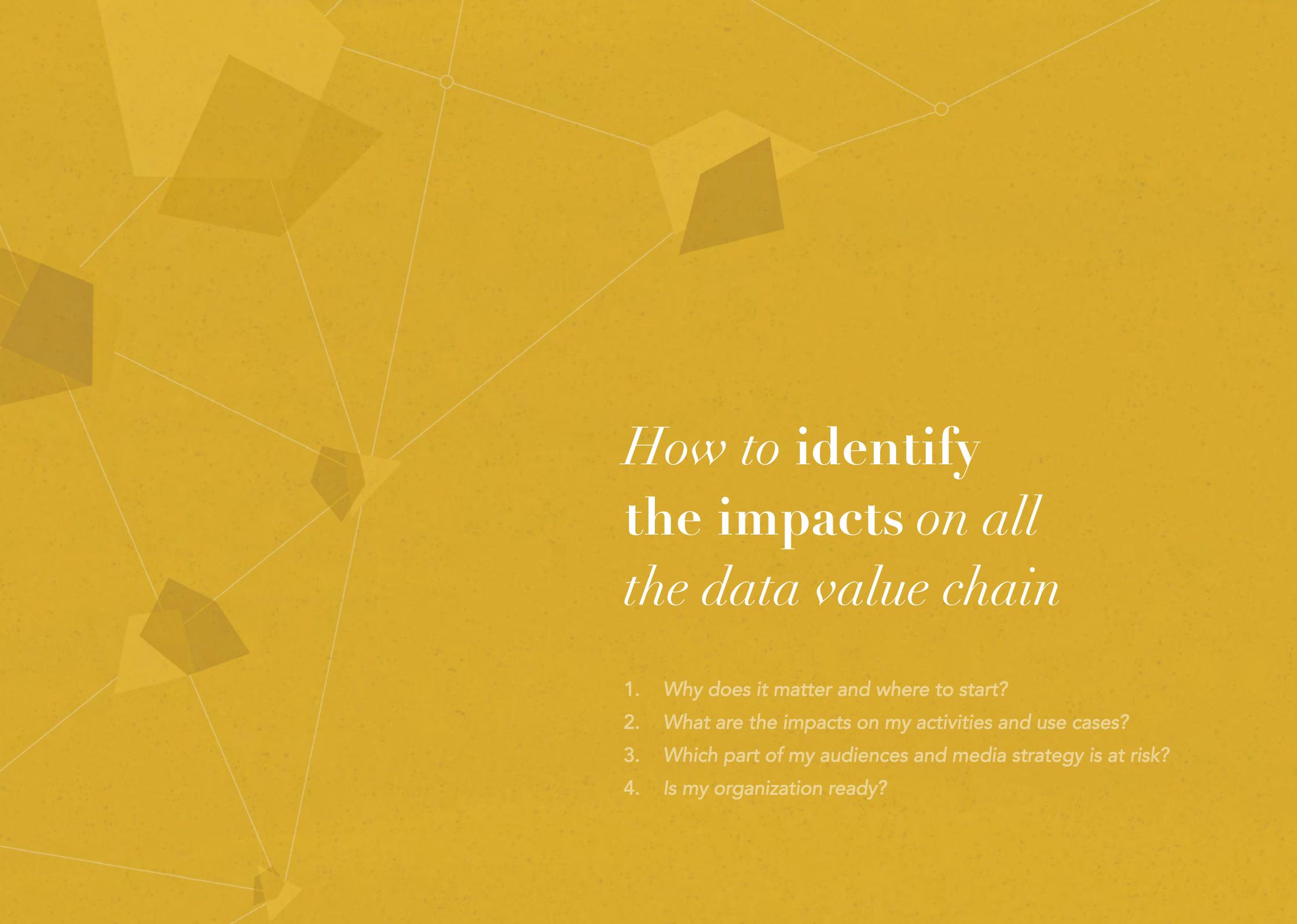
- Server-side
- Clean room
- Universal IDs
- PII tracking
- Cohorts
- Contextual targeting
- Conversion modelling
- Zero party data

**PLAYERS & TECHNOS**

- Google Privacy Sandbox FLoC
- GTM server-side
- ZEOTAP
- Facebook Conversion API
- ID5
- Apple SKAdNetwork
- adform
- LiveRamp
- INFOSUM

Plenty of new trendy buzzwords are currently popping up around the post-cookie era and associated solutions. Above all, the main question is who should we believe and what will be the next reliable and future-proof solutions. There are several keys to successfully wading through this influx of technological concepts and large-scale communication initiatives:

- **Draft your own** strong convictions when possible to distinguish the level of uncertainty of each solution
- **Prioritize** topics and review your testing and deployment roadmap frequently
- **Keep calm and take the time** to analyze the different offers and opportunities they could deliver
- Methodologically **process** each solution



# *How to identify the impacts on all the data value chain*

1. *Why does it matter and where to start?*
2. *What are the impacts on my activities and use cases?*
3. *Which part of my audiences and media strategy is at risk?*
4. *Is my organization ready?*

## *Why does it matter and where to start?*

The progressive end of the third-party cookie has had a few short-term impacts, including the deterioration of retargeting and display capping. But beyond immediate marketing capabilities, there is still a real shift to be assessed. The exercise of impact assessment provides insights on the business **perturbations** and adaptation efforts that advertisers will face in the coming months and years. Note, however, that the **forecasted state of digital marketing is still uncertain**, with some players releasing unexpected policies or having unclear or changing roadmaps. Regulations may also cause instability, particularly when their enforcement requires additional precedents and standards. The ongoing

complaints from privacy association “NYOB”, based on **GDPR** and somewhat anticipating what e-Privacy aims to standardize in two to three years, are a perfect example of this.

When analyzing privacy impacts, do not stop your analysis after examining your online marketing. Not all use cases are impacted equally, and you may have a very specific exposure depending on your strategy and media mix. **Post-click measurement** for performance-oriented businesses, for example, will not be disrupted in the same way as **post-view** effects for branding-oriented ones. Retargeting will largely suffer, while other targeting techniques may better resist.

And finally, a simple media mix relying mostly on Search will not undergo the same thing as an advertiser with a broad spectrum of channels will.

So, in our view, it is vital to follow a thorough process to assess current impacts and upcoming perturbations.

- First, **understand the impact for each type of activity**, whether global (media, analytics) or detailed (retargeting, onboarding) and estimate your exposure
- **Break down impacts depending on your media mix and type of audiences**, to understand how much

is somewhat secured and how much is at risk

- Finally, given the transversality of the transition to a privacy-proof world, your **organization** should proactively track and solve complex issues. **Assessing your organization's readiness** level will let you prepare better.

### Post-click conversion

A post-click conversion occurs when the user is exposed to an ad, clicks on it and then makes a conversion. [...]

### Post-view conversion

A post-view conversion occurs when a user is exposed to an ad impression and makes a conversion without interacting with the ad (clicking on it).

> **See glossary** page 34

# What are the impacts on my activities and use cases?

## Macro **impact assessment** on marketing activities

		DESCRIPTION	IMPACTS - TO DATE (excluding emerging solutions' potential)
Activate & optimize	Onsite/App Measurement	Measure the website/app <b>performance</b> (engagement, conversion) by analyzing the <b>website interactions</b> done by the <b>users during a visit</b> .	<ul style="list-style-type: none"> <li>▶ <b>LOW IMPACT</b> If the consent rate is low and no exemption has been set up:                             <ul style="list-style-type: none"> <li>- Less visibility on sites/apps performance</li> <li>- Partial data conducting to suboptimal UX choices</li> </ul> </li> </ul>
	Media Measurement	Evaluate the <b>performance of my media investments</b> on website visits, interactions and lead forms so as to <b>understand the impact</b> of each <b>media</b> on the generated conversion	<ul style="list-style-type: none"> <li>▶ <b>HIGH IMPACT</b> Strong limits on campaign performance overview:                             <ul style="list-style-type: none"> <li>- Possible media cost increases or lack of visibility on the generated business</li> </ul> </li> </ul>
Collect & measure	Onsite/App Activation	<b>Personalize the user experience</b> based on his previous website visits	<ul style="list-style-type: none"> <li>▶ <b>MEDIUM IMPACT</b> Scenarios to reprioritize taking into account the 2 main consequences: 1) Longer &amp; less representative AB-test impacting UX decision making / 2) Onsite personalization on reduced volumes</li> </ul>
	Media Activation	Address users with <b>relevant media</b> based on <b>profile, interest, behavior</b> and previous websites visits	<ul style="list-style-type: none"> <li>▶ <b>HIGH IMPACT</b> - Audiences quality deterioration (less business generated through retargeting, higher average media costs)</li> </ul>
	CRM & ON/OFF	Address your client data base and <b>target specific clients with relevant communications</b> based on their <b>on- and off- line actions</b>	<ul style="list-style-type: none"> <li>▶ <b>MEDIUM IMPACT</b> - Less qualitative audiences (based on offline data) - Less end-to-end performance view</li> </ul>

Privacy is not only a matter for online media targeting. It is key in our goal of mapping the full user journey, analyzing impact at each moment and marketing activity, and coordinating accordingly with respective teams.

Doing so, we see discrepancies in impacts. Onsite/Mobile App activities and CRM/On-off ones stand out better than media because they largely rely on **first-party data** and assets. Onsite measurement resists better than onsite activations, which reflects that consent regulation strikes harder on targeting in general than statistics.

Despite being useful to communicate internally and know where to focus your efforts, this summarized view is not sufficient to understand your exposure. Indeed, there are many ways and techniques to conduct advertising,

and you may have particular metrics or scenarios when it comes to Onsite/App measurement or activation.

The table on the following page shows fifty-five's pick of the impact on each detailed use case.

What is striking here, again, is the variety in levels of resilience. Some notes to help you navigate the table:

- The **consent rate** varies depending on each site or app, hence **does not have equal impact on all use cases**. Walled gardens have so far made it very hard to deny cookies and have almost-100% consent rates. So do many large publishers asking to pay to block tracking. But advertisers, for whom data is not an asset at the core of their business, will tend to provide a more unbiased choice to users and

have lower consented audiences.

- Always **distinguish between environments owned by walled gardens** (Facebook, Google Search, Youtube) **and other inventories**. The former benefit from both high consent rates and rich first-party data, hence are much less impacted.
- Identify **what is cookie-based and what isn't**. Some ad-centric measurement types (impressions, viewability), site-centric ones (landings), and ad-centric targeting (**contextual**) can be cookie-less, hence not impacted by either regulation or technical constraints, if the tools have been set up properly.
- Finally, **remind yourself of first-party cookies**, which so far are less impacted than third-party cookies.

This results in some cases resisting better, such as analytics and media **post-click measurement**.

Equipped with this more detailed knowledge about use cases, you can better assess the resilience of the strategy proposed by your media and digital teams, and be able to better prioritize the solutions described in the next part of this paper.

### **Contextual targeting**

Contextual targeting is a type of advertising which allows advertisers to target prospects based on their online navigation context such as the type of content displayed on the web page the user is exposed to. The ad displayed is defined by the environment where it will appear (page content, time of day, etc.)

**> See glossary page 34**

## Detailed impacts per use case (1/2): Measurement

### LOW IMPACT ON MEASUREMENT

#### Onsite/App Measurement

**Basic data counter** (cookie-less events or pageviews)

#### Media Measurement

**Ad-centric non-cookie-based:** Brand safety, fraud detection, viewability, impressions, clicks

#### CRM & On-Off

**On-to-off measurement:** from media exposure to sales - through Walled gardens

### MEDIUM IMPACT ON MEASUREMENT

#### Onsite/App Measurement

**Classic analytics KPIs** (cookie based Users, Session, Funnel, Conversion, Media attribution...)

#### Media Measurement

**Media Post Click Attribution** (ad server or analytics)

#### CRM & On-Off

- **On-to-off measurement:** from media to the site (lead/call/login) to sales
- **CRM activations** (emailing/SMS) based on onsite data

### HIGH IMPACT ON MEASUREMENT

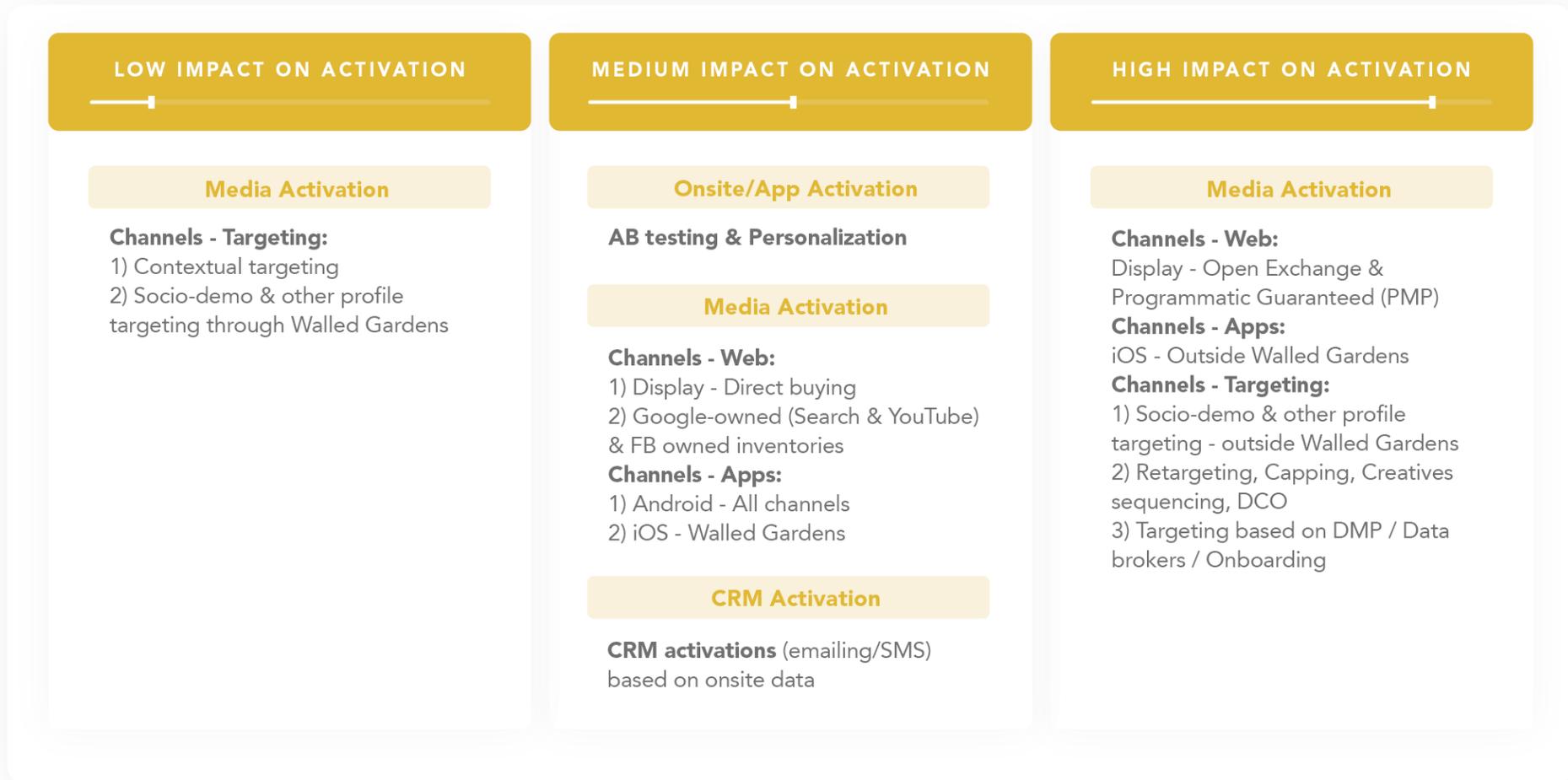
#### Media Measurement

- **Media Post View Attribution** (ad server or analytics)
- **Ad-centric cookie-based** – Reach measurement

#### CRM & On-Off

**On-to-off measurement:** from media exposure to sales - outside of Walled gardens

## Detailed impacts per use case (2/2): **Activation**



## *Which part of my audience and media strategy is at risk?*

The technical way we try to reach users for targeting or measurement highly impacts the resilience of different use cases.

But the type of users themselves (e.g., device, location), where we try to reach them (e.g., site, app), and which media strategy (e.g., branding, performance) are also key factors.

- The tracking restrictions are currently focused on well-known **browsers and devices** (Safari, Firefox, Edge, iOS), and consent can be considered impactful in countries that make it **compulsory to have refusal of cookies as simple as acceptance**

- As seen above, **sites with little first-party data** such as publishers of the “open-web” will struggle much more than large-scale publishers or walled gardens
- The objective of marketing actions in the funnel also changes your data needs and their stability. If you’re working at the **Awareness** phase, your targeting will struggle outside walled gardens, but your measurement, based instead on deliverability and viewability, will be less impacted. If you’re trying to build **Engagement and Conversion**, you will likely need to reconcile your site/app and your media, relying strongly

on third- and first-party cookies, and you will be strongly impacted.

By quantifying these effects with simple KPIs, you may easily assess your current and future exposure. The **scorecard** on the next page can be filled out by teams to complete this assessment—but nothing replaces real-life data. Some advertisers conduct **AB test** campaigns, comparing targeting **with and without cookies**, not only to estimate **performance losses** if they do not find replacements for cookies and other trackers, but also to **understand which cookie-less techniques work best**.

## KPIs scorecard to assess **current impacts & resilience**

**Audiences at risk**

**RESILIENT ASSESSMENT KPIs**

**Browsers & devices on media & site**

iOS, Safari, Firefox, EDGE **VS.** Android, Chrome

**Adblockers onsite**

Adblocked users onsite **VS.** Non adblocked users onsite

**Cookies consent rate**

Cookies acceptations **VS.** Cookies refusals

**RATIONALE**

- ▶ Some browsers do not support 3P cookies & device ids and are already strongly impacted
- ▶ Adblocked audiences cannot be served ads on many inventories, nor tracked onsite by media tools
- ▶ Non-consented users prevent an exhaustive measurement and cannot feed media audiences

**Media Mix at risk**

**Online marketing budget**

Online budget **VS.** Connected TV & offline budgets

**Marketing budgets at risk**

Non-GAFA inventories **VS.** GAFA inventories

**Audience targeting at risk**

3P-cookies targeting\* **VS.** 1P-cookies & contextual targeting

**Campaigns objectives at risk**

Post-view conversions **VS.** Post-click conversions

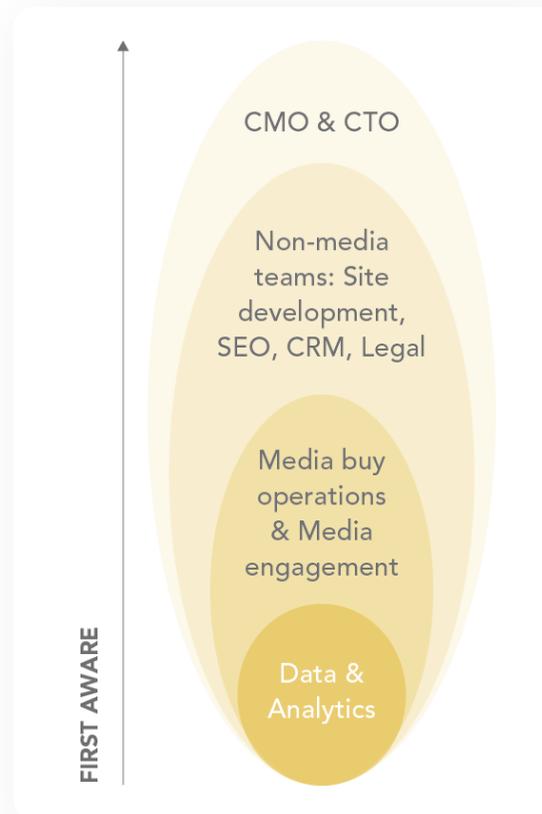
- ▶ Marketing outside web and apps is not or less impacted by new privacy constraints
- ▶ GAFA will be more resilient with their 1P data and the people-data you may share with them
- ▶ A share of your targeting may actually already be resilient as non 3P-cookie-based
- ▶ Post clicks conversions (based on 1P cookies) resist more than post-view (based on 3P cookies)

*\*Covers: socio-demo data outside walled-gardens inventories, and all retargeting or look-alike campaigns with classic tracking methods*

## Is my organization ready?

As you may have realized by now, the transition to a privacy-first ecosystem has widespread implications across your organization. A few questions may help you assess whether your teams and process are ready to rise to the challenge:

- **Who is knowledgeable** about the business and marketing impacts? Data teams and agencies will often be the first to lead the topic, but it is key to bring in all media teams (and non-media teams) that will also be impacted. Topics should be escalated to the C-suite, too, for validation on strategic direction.
- Who leads the impact assessment



and the preparation of privacy-proof solutions? Is it **fully externalized** to a media or data agency? Or do you have a tech privacy owner **internally**?

- **Have you already tackled main compliance challenges** (e.g., implementing a **Consent Management Platform**, auditing your data collection and usages)? Compliance should be your priority before thinking of investigating and developing alternatives to the cookie crumble.
- Do you systematically **examine resilience of any new tool or project**? Again, before upgrading

your current practices to make them future-proof, you will want to avoid launching and spending time and money on use cases already strongly impacted or with short lifetime against privacy constraints.

- It is likely you have started to investigate or even implement resilient technologies relying on new types of data, and need to have their regulatory compliance reviewed. How do you handle **collaboration with your legal team?** Are they aware of the business impacts? Can they analyze solutions with sufficient technical knowledge? Do they try to find a compromise between legal exposure and business benefits?

## CMP

A Consent Management Platform serves as a repository of users' consent. It manages the user's consent from its request through its storage and potential usage, which means publishers can request, receive, store and organize the user consent by vendors and/or categories. It collects and updates the consent given by the users over time. Many CMPs exist on the market with different functional logics and can be tied or not to a TMS.

> See glossary page 34

*What we are witnessing today is a **huge and singular transformation**. No one can say with absolute precision what the future state of digital marketing will be, but constant monitoring and analysis may help you navigate these troubled waters.*

Not everything is uncertain, though. There is no doubt, however, that:

- A large share of your audiences (Apple, Firefox, non-consenting users) is **already impacted and needs reworking**
- First-party data use cases resist better, so **providing services to your users on assets you own** will provide you with premium insights
- **Walled gardens** will provide efficient ways to leverage insights collected on their assets

In short, **this is not the end of online marketing**. Rather, it is an evolution - as we have seen, many alternatives

are emerging. As we move forward, we must keep the root cause in mind and remember one main thing: the post-cookie era is more about **user expectations** than technicalities.

In the next chapter of this paper, we will detail our analysis of the emerging ecosystem, and recommendations to help you build your **privacy-first strategy**.

## Clients who have mastered the new privacy context to prepare the future



Luxury

“How to evangelize around the new privacy restrictions and ways to adapt?”

### CONTEXT

55 has been asked to share to the Group its vision on:

- The impact of new regulations
- New tech solutions
- New marketing best practices

### APPROACH

55 created a Cookie Policy Guidebook for data managers and media representatives of all Maisons in order to :

- Provide updates on the current and futures challenges in the context of changing regulations, technologies and behaviors
- Educate on possible adaptations in a cookieless world
- Raise awareness on the evolution of media buying practices, and impact and need to evolve towards new solutions & business practices

### DELIVERABLES



Privacy Regulation by area



Assessment of existing use cases



Presentation of new use cases involving new technologies



Proposed roadmap

## Clients who have mastered the new privacy context to prepare the future



"How will the post-cookie context impact my media use cases and how can I anticipate it? What use cases should I capitalize on?"

### CONTEXT

With regard to the context leading to a restriction of cookies, the client asked 55 to help them assess existing use cases and define a relevant roadmap

### APPROACH

- Update stakeholders on the latest digital marketing trends
- Understand the business needs, media strategy and media use cases of the client
- Carry out a detailed risk analysis on 10 priority media use cases and their associated KPIs
- Define priority projects (methodology, use cases, tools, new marketing practices) to circumvent the risks identified during the analysis phase

### DELIVERABLES



## Clients who have mastered the new privacy context to prepare the future



“What impact will the end of third-party cookies have on our digital performance?”

### CONTEXT

- In a context of regularisation of the group with a brand separation, each player wants to keep a strong media footprint
- With the announcement of the end of third party cookies by Google in 2022, the group is concerned about the impact on its digital performance

### APPROACH

- 55 identified and defined key resilient projects for the entire marketing value chain:
  - Data collection, resilience/people based (Server Side Tagging & Conversion API) vs. Cookies
  - Onsite and media performance measurement (modeling, opt-out strategy (Google Consent mode))
  - Onsite and media activation (privacy sandbox, API (Facebook API conversion & Facebook Advanced Matching), modeling)
  - Media planning and optimisation (adcentricity, API and media knowledge)
- Prioritisation of the different solutions identified

### DELIVERABLES



Overview of the impacts on the digital marketing value chain



Solution opportunities overview



Presentation of relevant solutions

# Glossary

> brandtech.wtf

## App Tracking Transparency

The App Tracking Transparency framework aims to obtain user authorization to access app-related data for user or device tracking purposes. It should be used if the app in question collects data about end users and shares it with other companies in order to allow cross-app / cross-website tracking

## Attribution

Digital attribution refers to a set of methods whose purpose is to reconstruct the digital journey that has led a client to conversion. This process aims to assess the efficiency of each of the channels used during a marketing campaign.

Starting from the desired outcome (conversion), attribution tools allow marketers to analyse and identify the combination of digital interactions (called “events” or “touchpoints”) that have contributed to the outcome in any way. They then assign a value to each of these touchpoints, thus providing insight into which combination of touchpoints is most successful in influencing individuals to convert. Attribution issues are often related to tracking issues, as well as to matters of conversion deduplication. While there are several attribution models, the most widely used is the last-click model, whereby the conversion is attributed to the user’s last click.

## CMP

A Consent Management Platform serves as a repository of users' consent. It manages the user's consent from its request through its storage and potential usage, which means publishers can request, receive, store and organize the user consent by vendors and/or categories. It collects and updates the consent given by the users over time. Many CMPs exist on the market with different functional logics and can be tied or not to a TMS.

## Cohort

A cohort is a group of users that share a common characteristic, identified by a given dimension

(such as their first visit on a website). This group is tracked in the long term to understand the influence of the characteristic in question.

## Consent rate

The consent rate is the number of consents given (clicks on "accept" on the CMP banner) divided by the number of CMP banner impressions.

## Contextual targeting

Contextual targeting is a type of advertising which allows advertisers to target prospects based on their online navigation context such as the type of content displayed on

the web page the user is exposed to. The ad displayed is defined by the environment where it will appear (page content, time of day, etc.)

## Cookie

A cookie is a small file of letters and numbers that is downloaded onto your computer when you visit a website. This token is then reused for any subsequent visit to help the server keep track of the user. Cookies make it possible to gather and store data about users' browsing behaviour, which can later be reused during these users' subsequent visits (user logins, for instance).

## ePrivacy

The ePrivacy regulation complements GDPR, which became effective in May 2018, when it comes to protecting personal data in the specific context of electronic communications (e.g., cookie legislation). As a reminder, though directives identify objectives for each country as well as a deadline and means to reach this objective, regulations are intended to be immediately enforceable and uniform with the law.

## Fingerprinting

Fingerprinting in digital marketing is a type of algorithm that identifies a given user. Digital “fingerprints” contain information (browser, IP

address, mobile device brand and model) which can be matched with existing data to fully or partially identify users even when cookies or login have been deactivated. However, unlike human fingerprints, digital fingerprints are not always unique and can change over time (new device, different browser, etc.).

Fingerprinting technology can be used for mobile attribution, as it can link ad clicks to app installation or launch. User actions can thus be attributed to ads. More broadly speaking, fingerprinting in the IT world is a way to link extensive data (like a digital file) to a much smaller chain of characters: digital fingerprints. Fingerprinting makes it possible to uniquely identify initial data for various purposes.

## First-party data

First-party data is data collected and owned by a company. Each company thus manages its own first-party data, used to improve customer knowledge and customer experience.

## GDPR

The General Data Protection Regulation is the latest European regulation on personal data protection, which was enacted in 2016 and came into force in 2018. It aims at unifying legislation across the EU, and especially at giving power back to European citizens regarding the use of their personal data while making holders of such data accountable.

## ITP

ITP (Intelligent Tracking Prevention) is a feature integrated into the Safari browser. It was designed by Apple to better protect its users' privacy and prevent ad tech companies from tracking them across the web.

## IDFA

The Identifier for Advertisers (IDFA) is a unique identifier linked to an Apple mobile device, whose purpose is to target a unique user in order to follow their online behavior and display personalized content. The IDFA was used, for example, to retarget a user according to certain actions he or she may have had on a mobile app.

The rollout of iOS 14 in late 2020 made this no longer possible. An example IDFA might look like:EA7583CD-A667-48BC-B806-42ECB2B48606, and is the equivalent of Google's AAID on Android.

## Post-click conversion

A post-click conversion occurs when the user is exposed to an ad, clicks on it and then makes a conversion. A post-click conversion is to distinguish from a post-view conversion, which is a conversion following an ad impression but without any click on the ad.

## Post-view conversion

A post-view conversion occurs when a user is exposed to an ad impression and makes a conversion without interacting with the ad (clicking on it).

## Privacy Sandbox

Google Privacy Sandbox is a program designed to foster open source privacy standards, in order to "create a thriving web ecosystem that is respectful of users and private by default". Third-party cookies will be replaced by five APIs acting as an alternative path to collecting data for advertising purposes, while respecting privacy.

## Private Click Measurement

The goal of Apple's Private Click Measurement is to attribute a conversion to a previous ad click in order to measure online advertising performances, while preserving a user's privacy.

This new measurement method is broken down into 4 steps:

- Limit the number of campaign IDs in order to prevent advertisers from assigning unique tracking codes to each ad click and thus tracking users across the web
- Allow solely the website where the ad was clicked to collect click data and cut out third parties
- Share click data through a dedicated private browsing

window and delay it by a couple of days in order to further hide the user's activity

- Limit the data ad networks and merchants can see at the browser level

## SKAdNetwork

SKAdNetwork is Apple's ad network API designed to help advertisers measure their ad campaigns' performances while ensuring user privacy. This API has three main components:

- Ad networks: sign ads and receive install notifications when the ad leads to a conversion. Ad networks must register with Apple and apps must be configured to work with the ad

networks

- Source apps: display ads provided by the ad networks
- Advertised apps: apps displayed in the signed ads

Az

> Find more definitions on  
**brandtech.wtf**

