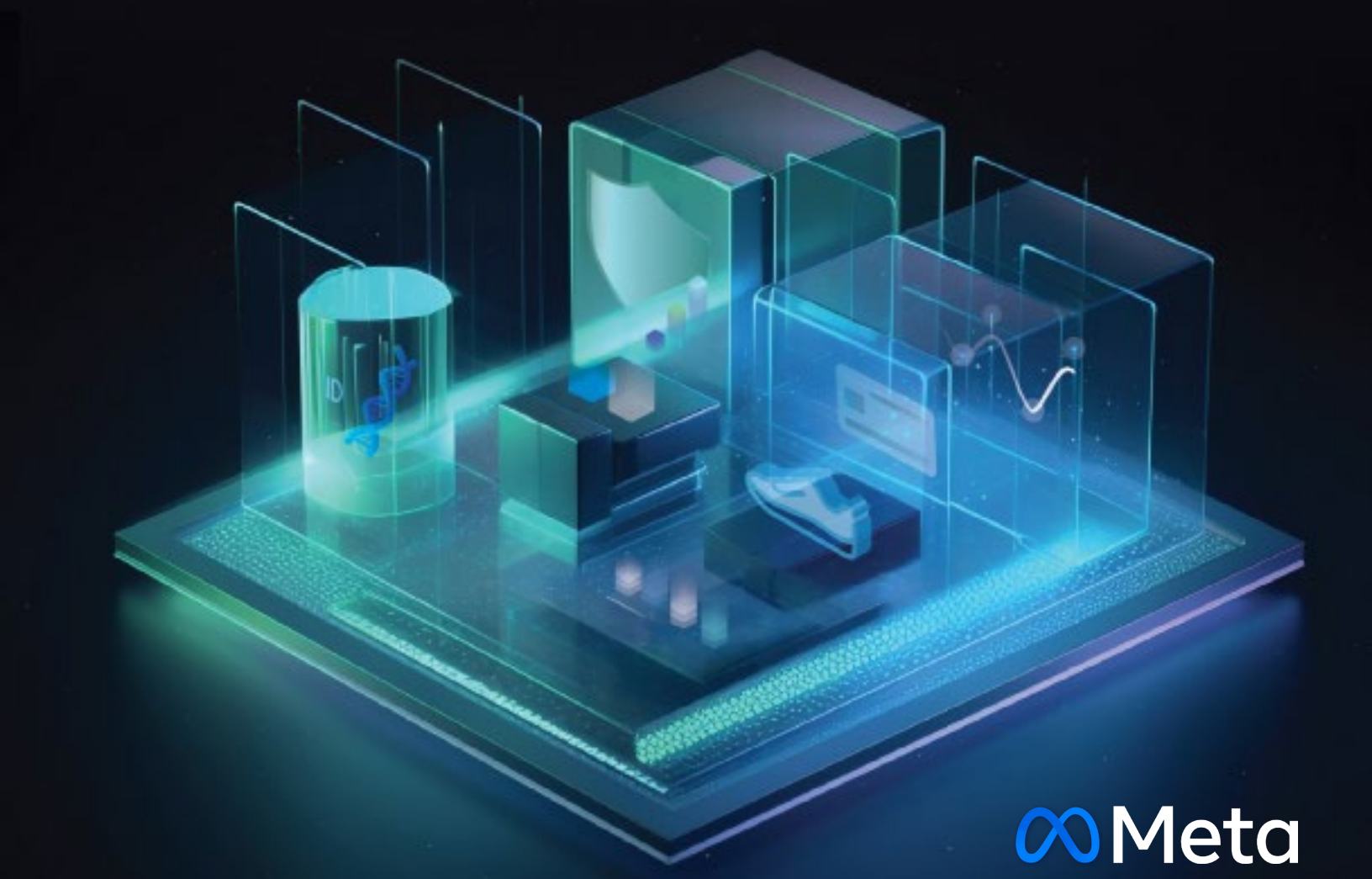
Deloitte Digital

A Marketer's Guide to Privacy-Enhancing Technologies



Meta

Contents

Introduction 03

Why is the digital advertising ecosystem adopting PETs? 04

What are privacy-enhancing technologies? 05

Which PETS are currently being explored within the digital advertising ecosystem? 06

Understanding the current marketing use cases of PETs 07

How do clean rooms fit within the ecosystems? 11

How is the ecosystem likely to evolve? 12

PET Maturity Curve 13

Top 5 recommendations for Marketers 14

Appendix 16

Introduction

The digital advertising ecosystem is shifting. As data use across devices rises and people become more aware of how their data is being used, they are demanding more protections and more control of their data. Technology platforms and regulators have responded to these demands with platform policy changes (e.g., iOS14 update, third-party cookie deprecation, etc.) and privacy regulations (e.g. European Union General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), etc.) that have a real impact on digital advertising. Data used to optimize, deliver, and report on mobile and web conversion events – tactics upon which the ecosystem is built – are being upended to reimagine digital advertising. The vision is a more responsible digital advertising ecosystem that respects users' privacy and engenders trust. Some in the industry are focused on restricting data sharing, while others are looking to rebuild systems with privacy-centric safeguards. Now, marketers, AdTech firms, and platforms have the opportunity to leverage technical solutions that deliver user protections AND advertising performance – privacy-enhancing technologies (PETs).

PETs are a range of techniques and technologies that help protect valuable data (including personal data) while enabling new insights and actions to be taken based on the data. PETs are playing an increasingly important role in keeping the digital advertising ecosystem functioning. As the sun is slowly setting on third-party cookies on Chromium-based browsers, PETs are being explored to solve for alternative privacy-enabled activation, measurement and targeting. There are also consortium-led proposals, collaborations among different parties in the AdTech industry, to find industry solutions that can deliver private cross-platform, customer matching and measurement between advertisers and publishers.

With PETs being actively explored and applied to key digital advertising use cases by AdTech and consortiums, now is the time for marketers to lean in, get educated and bring their voice to the discussion. Standards and frameworks are currently in development, which will ultimately lead to the solutions adopted at scale; your input as a marketer is critical in forums such as World Wide Web Consortium (W3C), IAB Tech Lab and World Federation of Advertisers (WFA). But first, marketers must learn more about PETs, take stock of the data their business needs to unlock value, and experiment with PETs to drive marketing utility and privacy protections.

This paper was developed to educate and prepare marketers for a privacy-aware digital advertising future. As such, this paper will:

1. demystify what PETs are by providing an easily digestible overview of the technologies;
2. clarify use cases being proposed within the digital ad ecosystem; and
3. provide advice on how to embrace the opportunities they present.

Why is the digital advertising ecosystem adopting PETs?

The societal benefit of an ad-supported internet is enormous. The internet has been praised as a liberator of information and a connector of people. Advertising has been essential in extending the benefits of a connected world; it underwrites the internet. Personalized ad experiences, fueled by data, help businesses reach relevant customers, and help people discover content, products and services that interest them. However, the digital advertising ecosystem evolved faster than privacy expectations and regulations.

As methods to capture data expanded, businesses created new opportunities to commercialize that data, further fueling data capture and monetization – creating a multiplier effect. For example, first-party cookies were designed to give websites memory and better functionality for people. The concept was repurposed to allow third-parties to place cookies as users visited websites, enabling advertisers to reach users and measure the effectiveness of digital advertising across multiple publishers without user consent. Pressure on the industry to mature its privacy safeguards heightened as data use grew exponentially and people and regulators demanded greater protections.

The ecosystem has already begun to transition. In addition to the shift from regulations, impactful changes are being driven through policy developments by the major internet browsers and mobile operating systems. These changes reflect customer sentiment that people are having more awareness of and control over how their data is used by businesses is a necessity for the future of the internet.

Initial responses include different approaches and have had varying success. One popular approach in regulations and platform policies is the use of consent mechanisms. While obtaining consent can enable a trusted customer experience, it also creates friction in the customer journey. Furthermore, it can be a challenge for businesses to determine the granularity, language and technology stack needed if they do not have the adequate data governance, protection technologies and privacy capabilities in place to manage first-party data in order to maintain that trust.

PETs allow businesses to increase customer data protections without creating friction. With PETs, there are opportunities to build always-on privacy-preserving solutions. Interest in PETs within the advertising industry has grown because they provide additional data protection and privacy capability while enabling key marketing use cases.

PETs alone are not a silver bullet for privacy or signal loss. PETs provide robust protections when combined with good data governance. However, PETs can and should eventually be part of a portfolio of every marketer's privacy-first marketing strategies.

> PETs allow businesses to increase customer data protections **without creating friction.**

What are Privacy-Enhancing Technologies?

While PETs are a relatively new topic in AdTech, they have been in development since the 1980s and deployed in academia, the public sector, healthcare and financial services since the 2000s. Researchers have used them to anonymize sensitive research data, while financial services companies have used them to create better models to detect credit card fraud. These highly regulated industries welcomed a set of tools that enabled them to use big data while minimizing privacy risks. PETs fall within a broader spectrum of data privacy protection approaches, from organizational to technological:

Data Privacy Protection Spectrum

ORGANIZATIONAL
Reliant on contractual and operational protections

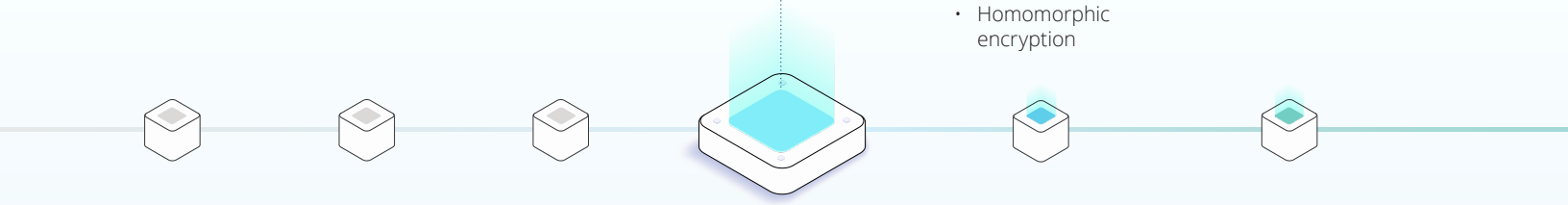
- Consented First-Party Data
- Data Governance
- Purpose Limitation
- Data Minimization
- Time Delayed Reporting
- Pseudonymization

TECHNOLOGICAL
Reliant on technological protections

PETs

TECHNIQUES
- Differential privacy
- K-anonymity
- Synthetic data
- Zero Knowledge Proofs
- Homomorphic encryption

TECHNOLOGIES
- Federated Analytics
- Multi-party computation
- Trusted Execution Environment



On one end of the spectrum, organizational protections are process and governance oriented, which can be rooted in contracts and operational processes. On the other end, technical protections, such as PETs, minimize unauthorized access and/or use (including analysis) of consumer data sets using a mix of cryptography, hardware and statistical techniques. In between, protections use a mix of permissions, statistics, and lighter cryptography to make it more difficult to process data in unauthorized ways.

While PETs provide strong technical protections, privacy approaches are not mutually exclusive. Privacy protections from multiple points on the spectrum can and should be combined to create protections that balance privacy with marketing utility. For example, when building for purpose limitation, meaning that data is processed only for a limited, clearly stated purpose, technical protections, such as the use of secure hardware like trusted execution environments, can provide attestation it's working as expected.

Which PETS are currently being explored within the digital advertising ecosystem?

To gain a greater appreciation of how PETs help minimize privacy risks and drive commercial value, it's critical to understand the two categories of PETs, **techniques** and **technologies**, and where in the digital advertising ecosystem they are being explored. Techniques use software and cryptographic protections to protect data, while technologies also use hardware aspects of the processing environment to increase protections.

TECHINIQUES

Category 1	How does it work?	How could it be used?	How is privacy protected?
Differential Privacy	Add noise to input data sets	Outsourcing analysis of advertiser customer data from a CRM / CDP to a third-party to perform analysis to help the advertiser understand how to improve customer engagement	Additional data is added to the core data set before sharing to reduce the risk of an ML model memorizing user data or individual users being identified or singled out
K-anonymity	Group and summarize data to hide individuals	Customized measurement. An advertiser could share first-party data with an AdTech platform, which could connect event level ad campaign data, perform measurement analysis, and provide summary results in return	Data sets are grouped and layered together so no individual data set or point is distinguishable to the advertiser
Homomorphic Encryption	Allows analysis on encrypted data without having to first decrypt it	A brand could analyze a platform partner's data without accessing unencrypted data	Only the owner of the encryption key can see the original data

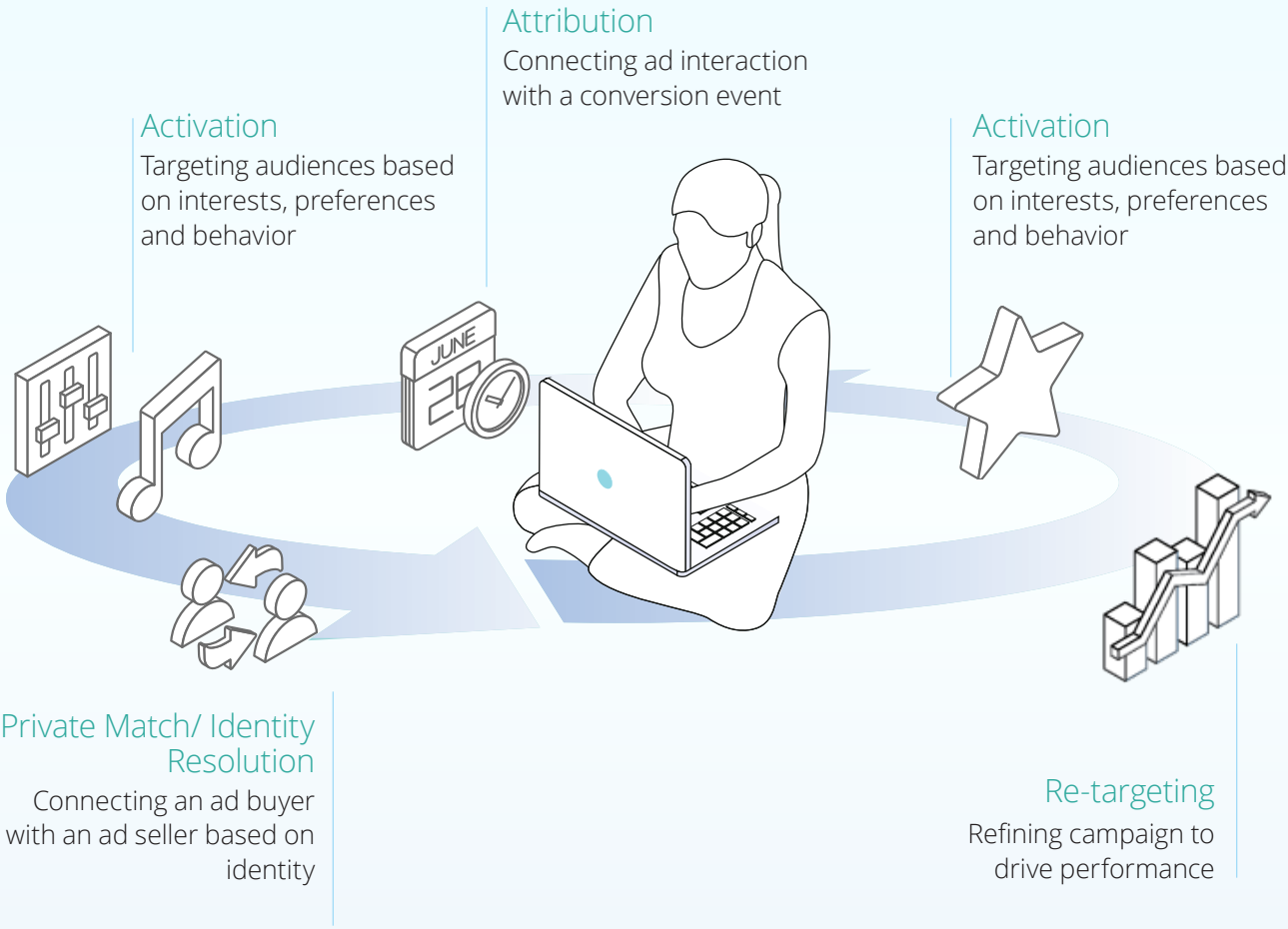
TECHNOLOGIES

Category 2	How does it work?	How could it be used?	How is privacy protected?
Multi Party Computation (MPC)	Compute information jointly without either party learning anything new about individuals	An advertiser could share online, offline or mobile conversion data with a platform to understand the incremental impact delivered from ads	Data is encrypted (converted into data which you can't decipher without a key) end-to-end, while in transit, in storage and in use, resulting in neither party seeing the other's data and computations processed within trusted servers
Federated Analytics	Analyze code run where the data is stored	Attributing ad interactions with conversion data for an individual on their cell phone operating system or browser	User level data remains on the individuals cell phone, only aggregated results shared with operating system or browser to protect identity
Trusted* Execution Environments (TEEs)	Isolated compute environments to protect and securely process data and code	Creating aggregated attribution reports. Conversion event reports may contain cross site information which needs to be kept private. Processing aggregate reports in a TEE, ensures no other entity will gain access to individual, unencrypted conversion reports	Prevents unauthorized entities from outside the TEE from altering data, while code integrity prevents code in the TEE from being replaced or modified by unauthorized entities

*The top three cloud service providers each offer TEEs / private computing capabilities

Understanding the current marketing use cases of PETs

Marketers' goals have not changed, they will continue to want to reach new and existing customers and measure the impact of those engagements. Customers will still want to learn and engage with businesses. With less data, PETs are enabling the evolution from precisive to aggregated and predictive models to avoid user-level identification and protect people's privacy while enabling advertising performance.



However, there is no one perfect solution that solves for all use cases across the different parts of the ecosystem. Different solutions offer different levels of user data protection and user experience personalization, with each applying multiple PETs at multiple points to create different layers of protection. In addition to PETs, there are a number of other techniques that also provide some additional privacy, but can have offsetting vulnerabilities or disadvantages. The combinations of PETs and other techniques being explored are summarized below.

	PRIVATE MATCH/ IDENTITY RESOLUTION Connecting an ad buyer with an ad seller based on identity	**ACTIVATION** Targeting audiences based on interests, preferences and behavior	**ATTRIBUTION** Connecting ad interaction with a conversion event	**INCREMENTABILITY MEASUREMENT** Understanding the true value of ads to drive conversions	**RE-TARGETING** Refining campaign to drive performance
Browser based	Multi Party Computation K-anonymity 1	Federated Analytics K-anonymity 3	Differential Privacy K-anonymity Federated Analytics TEEs 4		Federated Analytics K-anonymity TEEs 7
Mobile OS			Federated Analytics K-anonymity 5		
Collaborations	Multi Party Computation Federated Learning K-anonymity TEEs 2				
Selected Social Media				Multi Party Computation K-anonymity 6	

PRIVATE MATCH / IDENTITY RESOLUTION

1 **Publisher Advertiser Identity Resolution (Chrome)**

2 **Cross Media Attribution (World Federation of Advertisers)**

2 **Open Private Join (IAB Tech Lab)**

2 **Interoperable Private Attribution (Meta, Mozilla, World Wide Web Consortium)**

These solutions are focused on cross-platform matching and identity resolution. However, this use case is at an early stage of development. Most solutions in development are primarily focused on enabling measurement use cases for now, but there is potential for them to enable other cross-platform use cases in the future. Most of these solutions rely on **Multiparty Computation**, the ability to jointly compute information without either party being able to see the other's data, in addition to forms of private matching keys or identity keys to enable multi-platform connections. This is important because it can allow for ads measurement across platforms without the need for any party to have full control over all the data or to share an individual's data with another party. These matching key solutions all require further discussion, development and buy-in across the ecosystem before they are widely available. However, this means that marketers have an opportunity to evaluate these solutions and lean in to support the development of those that best suit their needs.

ACTIVATION

3 Topics (Chrome Privacy Sandbox)

This proposed solution solves for activation, the ability to target audiences based on interests, preferences or behavior through a combination of **K-anonymity,** grouping data to hide individuals, with **Federated Analytics**, keeping individual data on a user's device. The combination of on-device browser-based ad auctions using the users' website history with aggregation of user data into set interest groups protects data privacy. Although this solution will allow advertisers to target audiences by interests, those audience groupings are fixed within the browser environment and won't necessarily support cross-platform applications or retargeting.

ATTRIBUTION

4 Attribution Reporting API (Chrome Privacy Sandbox)

Google's Sandbox has a number of proposed solutions currently open for development and testing within the ecosystem. Attribution is being split into two use cases, detail reports and summary reports. Summary reports use **K-anonymity** and **TEEs,** a secure compute environment to protect and process data and code. To provide protection when delivering more granular data level insights for the detail reports, the browser has chosen to deploy **Differential Privacy, a secure compute environment to protect and process data and code.** While this delivers strong individual privacy protections, there are differing perspectives on the necessary level of differential privacy which needs to be applied to adequately protect data. Future data modeling and applications need to be built with these protections in mind to maximize data insights.

4 Browser-based Private Measurement

An attribution solution for the web, has already been implemented, deploying **Federated Analytics** and **K-anonymity.** Time delays are also used as a method of further aggregation.

5 Mobile Operating Systems Private Measurement

A similar solution to example 4's Browser-based Private Measurement is in development or already deployed across mobile operating systems, using **Federated Analytics** and **K-anonymity.**

INCREMENTALITY MEASUREMENT

6 Private Lift (Meta)

Meta is testing Private Lift, their solution which allows advertisers to perform incrementality measurement without the need for either party to see the other's data sets. The solution leverages **Multiparty Computation** and **K-anonymity**, providing data privacy protection while also delivering data utility.

RE-TARGETING

7 Fledge (Google's Privacy Sandbox for the Web)

Fledge in many ways is similar to Topics (3) but extends the use case for other AdTech organizations to set their own audience interest groups. **Federated Analytics** retains individual data on a users device and **K-anonymity** is layered in with **TEEs** to enable trusted analysis across this potential re-targeting use case.

The above discussion of seven current solutions and use cases was based on publicly available information at the time of publication. Other solutions are currently in development, and other use cases for PETs in AdTech are possible.

Each of the five main use cases for advertisers has some solutions available and are undergoing testing/ research; however, the maturity of solutions varies across use cases. The use cases with the most developed solutions in the PET space are attribution and incrementality measurement – both of which have privacy upsides and some utility downsides. We can expect further developments within each of the use cases within the next two to three years. Advertisers' input will be critical during this period.

How do clean rooms fit within the ecosystems?

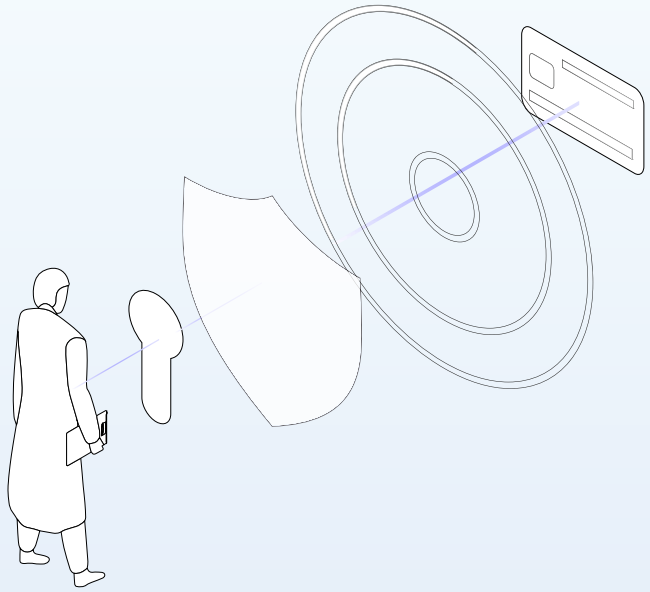
Data clean rooms are increasingly being discussed and tested within the digital ad ecosystem as cloud technology solutions that provide brands, agencies, and ad sellers a secure and neutral environment to plan, share data, and drive insights. These independent data environments emphasize the benefit that no entity has to share data directly with another. Clean rooms seek to provide a secure and compliant infrastructure to mix information and run analyses that enable private measurement and in some cases enrich audience targeting and activation. However, clean rooms are still currently in the process of being defined by industry trade bodies. While the IAB Tech Lab recently published a set of standards for clean rooms, implementation and adoption of these standards is ongoing.

The level of privacy protections, which depend on the combination of data protection methods and PETs deployed, varies greatly across different clean room solutions. While clean rooms are not a PET, many clean rooms leverage PETs as part of their data protections. Some clean rooms are independently operated by third-parties and provide infrastructure; others are a joint partnership where the clean room provider also contributes significant first-party data and insights. When considering working with clean rooms, it is important to understand what privacy measures are being used and if these measures meet your own enterprise data ethics and stewardship values.

Enterprises with large amounts of first-party data are beginning to leverage clean room solutions to create new commercial opportunities around data, partnering directly to provide brands with new solutions as insights from traditional identifiers decline. The growth of retail media networks is a good example, along with solutions from two of the main TV networks. Many companies are already using retail media networks, with 74% of brands already reserving budgets.[1] As the number of clean room partnerships grows, the challenge for advertisers and their agencies will likely be the interoperability of outputs. With industry guidelines still in the early stages of development, a test and learn strategy can help companies identify which clean room has the combination of data protection methods, PETs, and identifiers that is right for them.

[1] Deloitte Perspectives: Future retail trends Q4 2022

When considering working with clean rooms, it is important to **understand what privacy measures are being used** and if these **measures meet your own enterprise data ethics and stewardship values.**



How is the ecosystem likely to evolve?

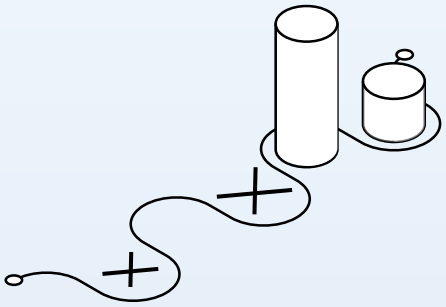
PET-based solutions that will enable a privacy-first digital advertising ecosystem are still in their infancy, but some trends have begun to emerge. Brands will continue to invest in and scale first-party customer data because people expect to have a deeper understanding of, and input into how brands use their data. This will ultimately create deeper connections between brands and consumers. However, it does require brands to invest in determining strategies to enhance touchpoints and loyalty in the customer journey and support data capture through maturing privacy-enabled data systems architecture and data governance. Brands have the opportunity to create a value exchange by providing a clear benefit in return for shared data.

While brands focus more on first-party data, the AdTech ecosystem will continue to evolve and experiment with PET solutions to solve for marketing use cases that are under threat. However, there is a choice to be made about how these solutions can be developed. Platforms and measurement partners could splinter, each evolving separate, frequently incompatible solutions. This segmentation across the ecosystem could increase switching costs and result in a fragmented view of their marketing activities. However, if marketers and advertisers lean into the discussion, and if platforms and measurement partners can join forces to develop broad industry guidelines, mutually beneficial and compatible solutions can develop.

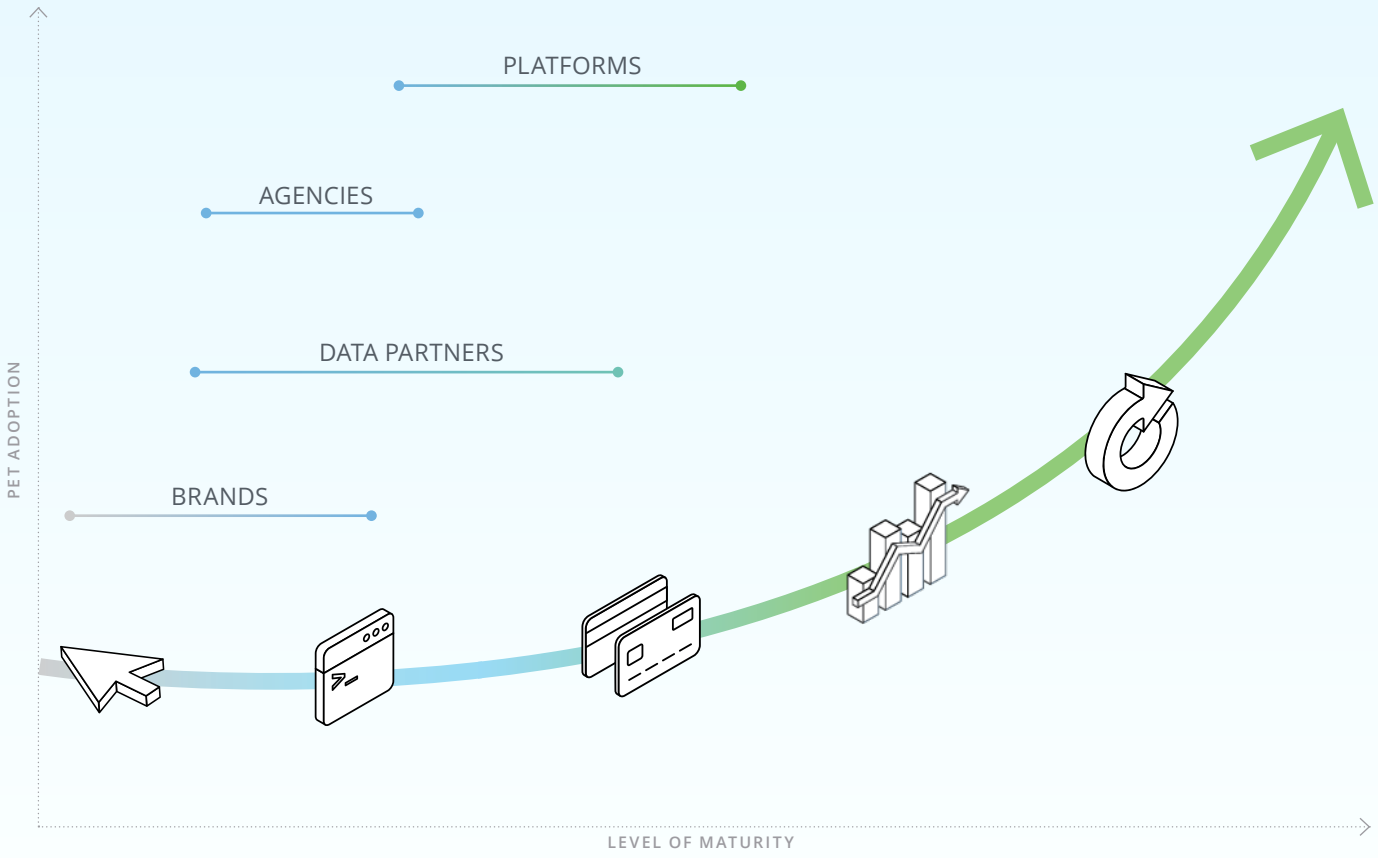
Data privacy can be seen within brand organizations as a barrier rather than an enabler. This perception can prevent brands from buying into and contributing to privacy solutions. This narrative can only change through education. However, during a time of economic uncertainty and enhanced focus on ROI, there will be more inertia around testing new marketing solutions when existing tactics still work. Therefore, adoption will take time with technology platforms seeking to attract advertisers through minimal implementation barriers, plug-and-play solutions and API's which help migrate media investment to support the overall development.

Multiple open web solutions and bespoke platform products are the most likely evolution for the ecosystem, mirroring the existing AdTech environment. However, marketers and advertisers have the opportunity to get in on the ground floor by partnering with platforms, other AdTech partners, and industry trade bodies to build and shape internal and external systems that enable both user privacy and high-value advertising.

Data privacy can be seen within brand organizations as a barrier rather than an enabler. This perception can prevent brands from buying into and contributing to privacy solutions. **This narrative can only change through education.**



PET Maturity Curve



Awareness

Understanding that PETs exist and can help with privacy. Unclear on how or the use cases. No real change to the

Active

PET experimentation with limited use cases, but still largely the same business, operating, and customer models

Operational

PETs in production for point solutions —with more advanced changes to current business, operating, and customer models

Scaled

PETs are integrated into all parts of tech stack for the business and most of the ecosystem. Business, operating, and customer models are optimized for privacy and profoundly different from prior business, operating, and customer models

Transformational

PETs and privacy are part of the foundational architecture of the business and the broader ecosystem and part of the business's DNA

Top 5 recommendations for Marketers

There are a few immediate steps marketers can take to prepare for a privacy-aware digital advertising future.

1

Educate and build awareness

The first step in taking action is to share knowledge internally on PETs for all stakeholders from employees, customers, partners to end users, are aware of your privacy strategy and data ethics that support your brand values and market positioning. Communicate the critical need for adopting PETs as a business imperative that supports privacy protections and customer trust. Get involved with consortium efforts like IAB Tech Lab Privacy-Enhancing Technologies' Initiative, W3C's Privacy Interest Group, and WFA's Digital Governance Exchange to make your organization's voice heard.

2

Understand where your business is today

Understand where your business stands in developing data strategies that balance data privacy and business value. You'll want to consider asking yourself questions like: "Is my business aware of the privacy landscape shifts?"; "What data is my business currently using and what data have we not unlocked value from?"; and "What data is shared or managed by partners and what protections do we have in place?"

Once you have a clear understanding of where you are, you'll be able to determine your next steps more effectively.

3

Make your data strategy as collaborative as your business

The impact of your data strategies is not isolated to any one team. Marketing and analytics teams are major users of customer data and should play a primary role in setting data strategy, but an effective data strategy will also require input and alignment with your IT, Legal and Privacy teams. It's critical to break down internal organizational silos and increase synergy between relevant teams. You'll want to consider things like workflow, cross-training and steering committees.

4

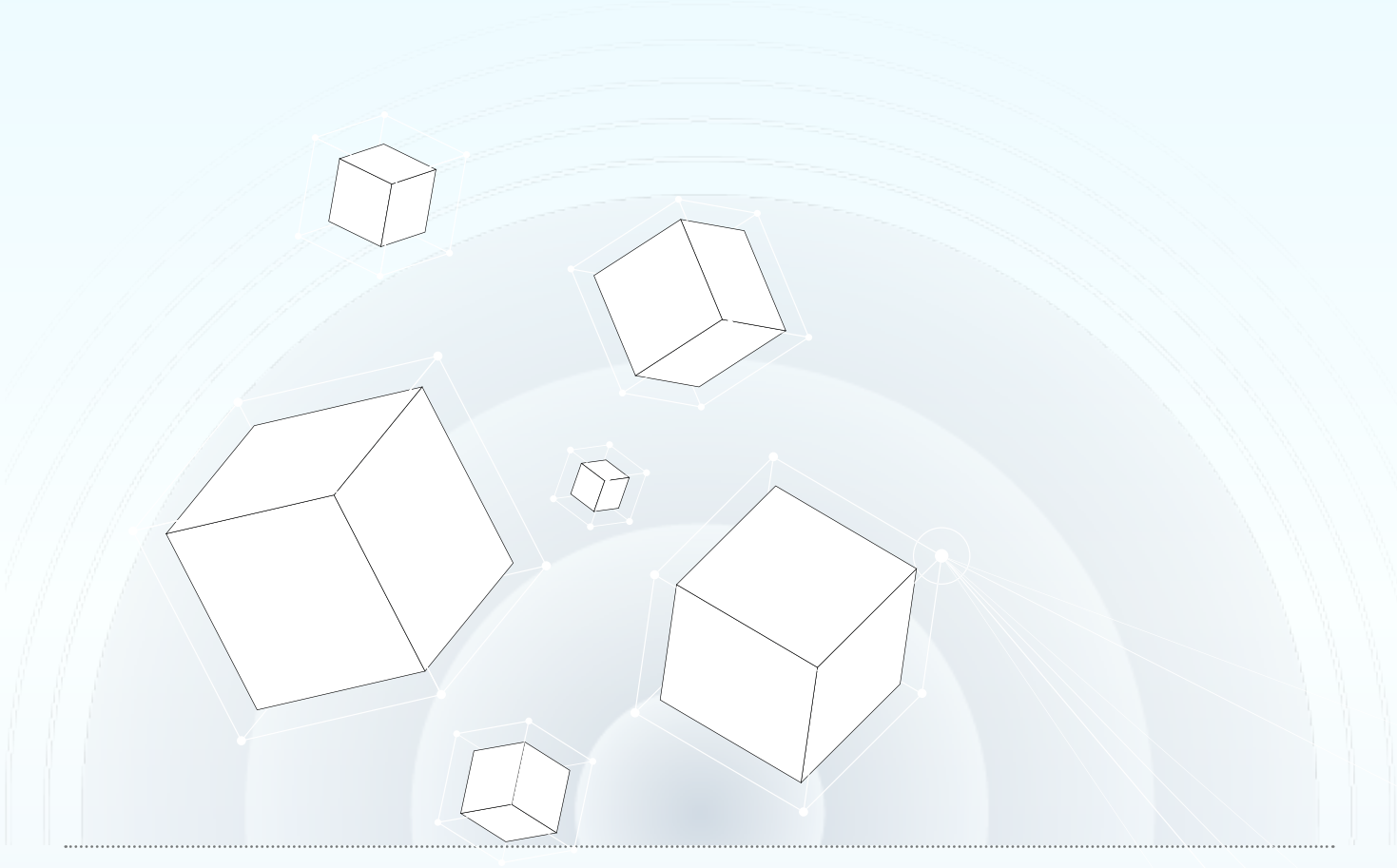
Enhance privacy and consent capabilities

Data privacy is evolving from a regulatory 'check box' exercise to a major driver of business enablement. Your data governance, privacy policies and system architectures need to reflect the increasing complexities of the ecosystem in which you operate. It is essential to have the right data governance frameworks in place before exploring the opportunities PETs can deliver.

5

Partner, experiment, and test

Ask for help from trusted advisors who have the experience to to start your journey leveraging PETs. Build a road map to experiment with PET-enabled solutions being tested by the different AdTech providers. Select organizations who share your approach to data ethics and ask questions such as "How do I protect my data when sharing data?"; "How is my data protected when mixed with partner data?"; "Are my data and computed results deleted, stored or used by the partner once the analysis is completed?"



Appendix

Additional PETs to Know

Category	How does it work?	How could it be used?	How is privacy protected?
Zero Knowledge Proofs	You can share information with a partner to allow for 'truth statements' to be proved	A brand could serve an ad to a user that fits a profile without knowing anything about the user other than the profile match	Information is converted into coded data which can't be deciphered without a key, which is known by just the prover of the information
Federated Learning	ML on distributed localized data sets	Trains local models, on data on user devices, where weights of the resulting models are shared with other user devices, in order for a new global model to be determined	As with federated analytics, key privacy feature is user data never leaves the device, as only model weights are communicated
Synthetic Data	Artificially generated data which mirrors the patterns, balance and composition of the original dataset	A brand could analyze a synthetic data set to develop target marketing profiles	The original data set is not used to perform analysis of the data

Additional Privacy Protection Methods

Category	How does it work?	How could it be used?	How is privacy protected?
Consented First-Party Data	Requires an individual to agree for their data to be collected and used, either explicitly or implicitly	A website could request that users review and confirm what cookies will be placed prior to accessing a website	Companies set internal policies to abide by user preferences in data processing. Protection is as strong as the policy and its compliance mechanism
Purpose Limitation	Limits the use of information to only the purpose stated at the time of collection	A website could use a cookie placed for site functionality only for site functionality, rather than to generate data for targeted advertising	Companies set internal policies to abide by initial stated purpose in data processing. Protection is as strong as the policy and its compliance mechanism
Data Minimization	Limit the collection of information to what is necessary to accomplish a specific purpose.	A company signing up users for a newsletter could collect only an email, rather than also collecting names and other PII	Data that isn't collected can't be hacked or misused; however, data minimization prevents access to historical data and reduces signal
Time Delayed Reporting	Aggregates reporting by collecting data from a certain time period and reporting after a delay	A platform providing reporting on an ad campaign could delay reporting by 24 hours and aggregate hourly	Aggregating data provides some protection; however, k-anonymity is more effective without the signal reduction from delayed reporting
Pseudonymization	Replaces an identifier with a non-sensitive equivalent. Allows the data to be processed and analyzed after pseudonymization. Can be reversible or irreversible.	Replace an email address with a hashed pseudonym and use it to match data from multiple sets (e.g., UID 2.0)	Identifiers are replaced with an equivalent, removing them from the data set; however, loses effectiveness as multiple data sets are combined, as multiple non-sensitive data points can be used to precisely identify an individual regardless of pseudonymization.