Unique

The Great Advertising Reset: Navigating The Future Of Media With Explore And Exploit Optimization

Saqib Mausoof
Unique

Table of Contents

Executive Summary

The global advertising industry is going through a great reset. This change is driven by awareness of data privacy implications by consumers which have led to regulations like GDPR and CCPA. Key among this awareness is that their behavior data along with big data platforms have been the fuel that has driven multi-billion-dollar valuations for tech companies and their shareholders. Advertising today is a two trillion-dollar business, and the digital portion is directly affected by regulations that impact third-party data exchange systems built around bits of tracking code called cookies.

Led by the European Union's GDPR initiative, consumer privacy, not big data computing, is now the driving force in the marketplace. Ubiquitous tracking mechanisms like cookies, IP addresses and mobile IDs that use personal identifiers are being discarded. This drastically affects the relevant $225 billion US advertising industry which has been historically dependent on theses IDs for behavioral advertising. This reset (we prefer not to call it the "cookie apocalypse") is going to cause a shuffling of the ad tech stack and further empower dominant players (walled gardens) while also bringing them under increased scrutiny. The independent incumbents(stalwarts) that have developed business models over the last decade using cookie syncing technologies for audiences, ID linkages and look-alike models are going to be challenged by tech savvy brands' data clean rooms and nimble up comers providing innovative solutions.

Google Chrome cookies have not yet been deprecated, but they will be as the more potent CPRA (California Privacy Rights Acts) goes into effect on Jan 1st, 2023. Apple has already disabled its IDFA IDs disabling cross-app tracking that undermines ad retargeting and measurement, and Google has announced that Android mobile ID's will be nulled to zero on return. Browser fingerprinting is already blocked by browsers, and we expect IP address usage, a key signal for trading television advertising, to be curtailed in the future. This could derail the rapid shift of TV advertising towards OTT and CTV as these channels have enabled advertisers to use digital tactics historically unavailable in an age/gender dominated TV industry. As a result, the $70B US television business and the technology that underpins it will face similar changes due to privacy implications of using personal identifiers and resort back to Zip+4 DMA targeting.

These changes will leave brand marketers and publishers virtually helpless when it comes to behavioral targeting using personal identifiers like cookies, mobile ID's and IP addresses across both TV and digital. McKinsey suggests that up to $10 billion in revenue is at risk for US-based data brokers and publishers. Furthermore, programmatic advertising tactics like retargeting, browser-based tracking will be diminished specifically for intermediaries like agencies and ad tech platforms who do not have access to first-party data in their media usage contract agreements. According to McKinsey, "Companies that do not figure out a strategy to maintain access to data may have to spend 10 to 20% more on marketing and sales to generate the same returns."

The ad tech industry response has been to work on replacement solutions like Trade Desk's Unified ID 2.0 that utilizes logged-in users to establish identity tokens in the form of hashed emails. These identifier-based solutions work well with ID-centric data models built to sync and aggregate individual ad impressions. These expensive

compute infrastructures provided the industry the ability to do count queries against neatly categorized datasets as they had access to billions of data points in the ad eco-system. A decade ago, Google Research Director Peter Norvig, the purveyor of mapReduce big data computing was famously quoted as saying that "[Google] does not have better algorithms, just more data." While the truth is nuanced, the industry relied primarily on deterministic arithmetic to the extent that probabilistic was considered a "dirty word" in ad tech (Dr. Richard P. Feynman would have been devastated). However, as these data points are retracted by the regulators amid general mistrust of big tech, personal identifier-based solutions might not be able to pass the muster of privacy regulations. Both Google and Apple have already outlined cohort-based solutions like FLOCs and SKAd Network, respectively, for transacting in the advertising eco-system. This means if universal IDs falter, brands will be forced to use either (a) proprietary targeting inside walled gardens, (b) broad contextual targeting or (c) cohort-based optimization. Thus, the big reset is not just about privacy, but it is also about applying a probabilistic approach towards solving advertising's Sisyphean challenges around targeting and measurement. This reset represents a major economic opportunity for the business that correctly builds an alternative solution.

This white paper presents an elegant solution that is deductive rather than inductive. We use probabilistic models to continuously optimize spend against walled gardens and the open web. Specifically, we use the Bayesian multi-armed bandit algorithm to calculate the probability of a favorable outcome from media platforms with vastly different embedded targeting models. This concept is encapsulated as Explore and Exploit Cohort Optimization (EECO) which is our intellectual property and filed as a provisional patent with the USPTO. We don't claim that this solution is better than a deterministic personal identifier-based solution, but we believe that EECO is more aligned with cohort-centric digital advertising realities as it is non-intrusive and privacy compliant. In fact, it can be complimentary like pairing psychology with physiology.

To summarize, the great advertising reset will challenge the industry to find an alternate, privacy compliant solution; however, it also presents a major economic opportunity for the company that builds a viable alternative solution. Unique believes that EECO's rigorous probabilistic approach using multi-armed bandits is a solution that can provide brands with the ability to optimize their campaign spend across an unknown set of technology platforms. This provides advertising effectiveness rather than pure efficiency in a privacy compliant manner. This white paper outlines our approach in detail.

"Both Google and Apple have already outlined cohort-based solutions like FLoCs and SKAd Network, respectively, for transacting in the advertising eco-system."

State of the Industry

It's a 2 trillion dollar market.

Source: WPP, eMarketer, IDC and WARC

Media services in the US have had phenomenal growth in last decade fueled by programmatic advertising, behavioral targeting, cookie-based tracking and data brokerage services. The addressable market for media services is more than US $2trn in terms of client spend (Source: WPP, eMarketer, IDC and WARC) with nearly US$600bn in spend on display advertising driven by cookie technology.

However, ad tech's phenomenal growth has now been curtailed by the enforcement of GDPR and CCPA that have led the big eco-system players like Google and Apple to deprecate the third-party cookies and Apple to introduce App Tracking Transparency (ATT) measures in iOS14.5 respectively.

This changes everything, the great advertising reset (we prefer not to call it cookie-apocalypse) is fast approaching. Our belief is that this reset will not diminish the power of online advertising. In fact, the Covid-19 pandemic has seen media spend increase globally; however, it will readjust the spend across the media and technology. This is what we refer to as the **ad tech stack reshuffle** and will contribute to several trends that include:

- Laser focus on first-party data for marketers and media owners
- The race to create first-party data and a rise of data clean rooms and self-service walled gardens
- The breaking of tracking and attribution as cookies and IDFA's go away, imposing great difficulty in measurement, fraud prevention and other ad verification, attribution and mechanisms, as well as Return on Ad Spend (ROAS)
- Retargeting as a tactic which can be estimated at a commerce impact of 30x ad spend will dwindle
- FLoC and SKAdNetwork implementation of cohort level data sets will raise the size of the walled garden's walls without a solution for the rest of the marketplace
- The recognition (and scrutiny) of identity solutions, linkages and graphs at the center of the advertising and media technology stack
- Increased number of app-driven streaming media and other addressable devices at the individual and household level
- A closer scrutiny at look-alike models and other algorithms that increase the size of first-party seed audiences to a larger targetable pool with respect to privacy and ethical perspectives

Ad Tech & Programmatic

What about retargeting?

Of the billions of dollars generated through ad tech, at least 50% (assumption made on managing programmatic media spend where campaigns were classified as prospecting, retargeting or data-driven) of media spend can be attributed to retargeting and look-alike modeling. With the increased scrutiny on such tactics, the efficiency of programmatic advertising will be reduced. In addition, following on the last few years of increased transparency in the industry, clients are increasingly taking media activities in-house and most brands will experiment with direct purchase with walled gardens and publishers. Facebook, Google and Amazon already make their platforms and tools available for advertisers by honing self-service models, the ability to bring first-party data inside their eco-system and with service level teams that can support brands marketing

initiatives. The elimination of third-party cookies on the Chrome browser (Chrome accounts for over 60% of all browser traffic) will further cement power and knowledge in the hands of walled garden tech platforms and increase the importance of first-party data.

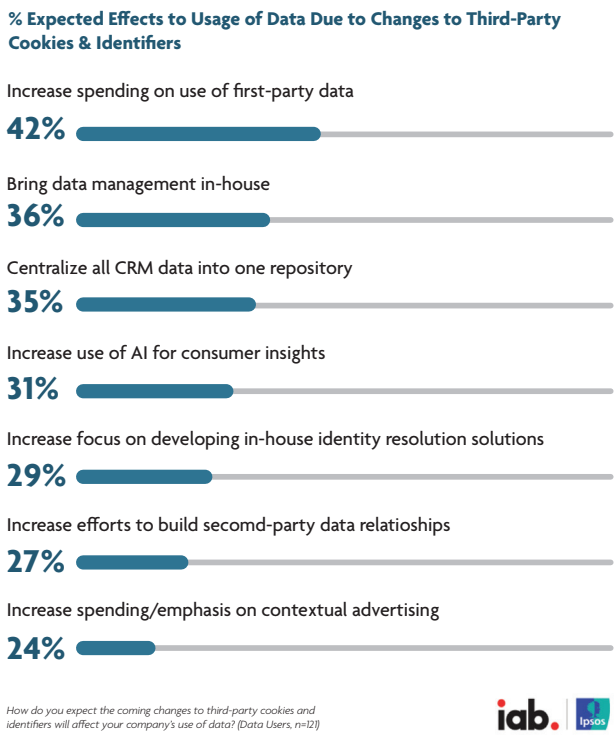
This will have major effects on programmatic business at large resulting from:

- In-house programmatic spend going directly to walled gardens at an even greater scale
- Lack of media spend in tactics like retargeting in display and mobile channels
- Lack of tracking and thus drop in measurement, reporting and attribution services by agencies and intermediaries

IAB Report 2021

The effects on data use will lead to more resource investment while lowering company profit margins

Additional Insight: in a spearate question, 34% of data leaders expressed concerns about potential walled garden CPM increases - another increase in investment as a result of changes to third-party cookies and identifiers.



How do you expect the coming changes to third-party cookies and identifiers will affect your company's use of data? (Data Users, n=121)

The industry at large has developed frameworks (FLoC and SKAd) in the form of cohort models that are based on edge computing methods, i.e. cohorts are created on the browser/device based on consumption of similar content sets for supporting programmatic. It is very likely that this alternative will not be as good as the user data controlled by the walled gardens primarily Apple, Google and Facebook. Thus walled gardens will always have an insider advantage. Lastly, true optimization is also about reducing spend, and historically, spend reduction does not work well in the ad tech world as their growth comes as a percentage of media spend. All these options leave programmatic trading desks and platforms in a conundrum as media spend shifts away from lucrative third-party, data-driven behavioral advertising. As mentioned before, McKinsey suggests that up to $10 billion in revenue is at risk for US-based data brokers and publishers.

Perils of Privacy And Consent

GDPR, CCPA and the approaching *Winter of Disconnect*

Cookies are bits of java script code that websites drop on consumer's browsers and devices. The industry has been using them for the last 25 years to track users' online behavior by piling data collected without implicit consent through the user's journey on the web. The enhancement/ collection of data on top of the cookie gave birth to behavioral targeting, retargeting and the rise of ad tech open marketplaces for bidding. It was a simple way for all players to track and optimize ads across digital advertising. Said another way, the cookie followed the actual user's journey and did not require a mechanism to consider where the consumer may go next.

Since tech platforms found cookies easy to create, share and monetize, this allowed for fueling programmatic growth. Armed with cookie technology, platforms,

technology businesses and smart marketers built a massive data ecosystem and infrastructure around the cookie to connect brands and customers. As a result, data about individuals is shared billions of times a day, not just with advertisers but with hundreds of thousands of intermediaries. Estimates from Wunderman Thompson claim that consumers' personal data is shared between the third-party cookie ecosystem over 500 billion times a day!

In fact, cookies and IDFA are just the tip of the iceberg when it comes to privacy regulation. We foresee Android ID's and IP addresses also heading towards a privacy-centric approach as all aspects of behavioral targeting like technographic based ID linkages come under scrutiny. This trend is evident as more and more browsers reject fingerprinting. This along with the deprecation of third-party cookies, has caused browsers to take a principle-based approach to safeguarding the privacy of users. As most direct to consumer-based technology companies reject ID based tracking including IP addresses, the world of personal identifier based behavioral targeting is dismantling in front of our eyes primarily driven by CPRA enforcement by Jan 1st, 2023.

The Right Side Of History

Are Google and Apple on the right side of history?

After announcing the phasing out of third party cookies in 2022, on 6/24/21 Google extended their support for third-party cookies till sometime in 2023. However, Google is still committed to deprecating third party cookies and is not currently planning to build alternate identifiers to replicate the behavior of the cookie to track individuals as they browse across the web, nor will they use them in their ad products. They stated that they are aware of alternate identifiers, which are being created in the market and they will not be supporting those across Google's ad stack. Instead, Google's stack will be powered by its own internal solutions.

Unique's interpretation is (and there are many):

- We believe that Google does not feel the current alternative ID solutions are ones they believe check the boxes from a privacy and compliance perspective, so they are keeping their distance.
- Restating that a company can do business with Google for targeting if a partner follows their rules.
- Companies will need a gateway to leverage the Google toolkit to get this done (privacy sandbox, FLoC)

Opportunity

We at Unique believe that utilizing first-party customer data and an elegant mathematical model as the foundation for our product roadmap will prove to be effective as a long-term, privacy compliant targeting strategy.

> Our goal over time is to show "efficacy," based on cohort modeling that replaces id based tracking signal **using an optimization model with a 75% to 80% effective rate.**

A privacy compliant solution is the key to achieving success in the cookieless future, because any solution built to replicate the cookie and offer 1:1 matching will not be well received in today's regulatory marketplace. We expect the ad tech stack to reshuffle and that provides an opportunity for our approach to be successful and to solve most advertising use cases.

Essentially, many of the tools available today have been built, in a privacy non-compliant manner (in lieu of newer privacy regulations) and we believe Google feels the same way. Our product will be built in a manner that is custom, unique, and owned by the Marketer as a SaaS platform but is least vulnerable to CCPA/GDPR and Google's stance of working with cohorts rather than personal identifiers. Specifically, we seek to build an "engine" that allows us to navigate the walled gardens and open web without using personal identifiers through the use of AI and ML models deployed in EECO (Explore and Exploit Cohort Optimization).

The Age Of The Cohorts

Historically, Google has been the biggest pursuer of big data processing, brought to market map-reduced data sets, and has had their research director Peter Norvig claim that **"We don't have better algorithms. We just have more data."** While the truth is highly nuanced, the fact was that Google pursued big data and thus believed that a full spectrum of data will give better insights, learning and targeting of consumers.

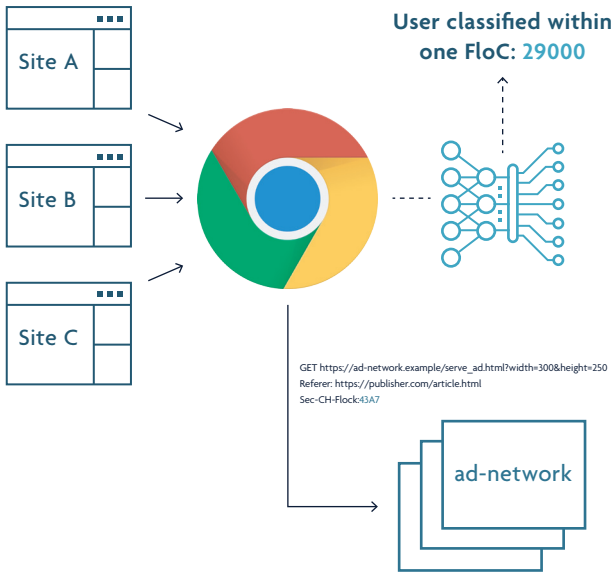
However, facing GDPR and CCPA, the stance has changed, and Google has publicly pulled back the use of personal identifiers in the biggest buy side platform, DV360. Now Google has created the concept of FLoC (Federated Learning of Cohorts) and a place to gather insights from FLoCs with the privacy sandbox. These cohorts created on the consumer browser end the personalized tracking of third-party data pixels, thus a lot of processing is done on the consumer device.

FLoC, FLEDGE and TURTLEDOVE

FloC is Google's privacy-led solution to replacing third-party cookies. The ad tech and ad giant claim is that Cohorts are a privacy-safe alternative to targeting a group of users, instead of profiling and targeting individual users. Google has also reiterated that they will not use personalized identifiers in their ad eco-system (DV360) and will also not build a back-door into their privacy sandbox.

From what Google has shared on their website, the FLoC proposal, users belong to one single cohort that is built in the browser and grouped based on browsing behavior. The cohort must be sizeable enough to prevent micro-targeting and comply with CCPA and GDPR like regulations. Adding to the privacy-first approach, user data such as web history

is stored and processed on the edge (on-device), so only the cohort id is exposed and not personal identifiers. The way a FLoC works is illustrated below:



While in the FLoC proposal the browser determines the cohort membership of a user, FLEDGE enables advertisers, publishers and ad tech to add a user to cohorts they define. Similar to FLoC, with FLEDGE targeting is cohort-based, but cohort membership is based on specific events for those users and can be defined freely. Most importantly, FLoC is used for prospecting tactics (finding new customers). There is also TURTLEDOVE which is an initiative to support retargeting tactics. It does this by retargeting in a privacy-preserving way by grouping users into "cohorts" of hundreds (or thousands) of users, so no single user can ever be individually identified.

Google Privacy Sandbox

Again, according to our understanding from Google, and this is sparse, the mission of the Google Privacy Sandbox is to "Create a thriving web ecosystem that is respectful of users and private by default." It is a group of proposals about how advertising can be rebuilt without third-party cookies. It covers ad targeting, ad delivery, ad reporting, and user privacy. Google privacy Sandbox is putting the wider ad tech industry on notice before it is implemented in time to meet full CPRA regulations enforcement on Jan 1st, 2023.

The Privacy Sandbox is a revolving set of initiatives aimed at protecting user privacy whilst enabling the advertising industry to take advantage of some information, insights and tools. Some key initiatives include:

- all data being held at the device—not server-level—enhancing privacy and negating server-side matching, this is called edge computing
- the provision of a Chrome "conversion management API" for attribution
- privacy budget API to restrict data extracted via the browser
- the Federated Learning of Cohorts (FLoC) API that uses machine learning to cluster similar behaviors
- the Two Uncorrelated Requests, Then Locally-Executed Decision On Victory (TURTLEDOVE), a technique for tracking browser interests, i.e. retargeting
- FLEDGE exhibits elements of behaviors that browsers are trying to eliminate, namely the tracking of users across the internet and can enable tech publishers to extend their network across the open web

Competitive Solutions

There are four key initiatives (aside from cohorts optimization) that the industry is working towards. These include:

- Unified identity solutions based on Single Sign On (SSO)
- Contextual advertising
- CTV and OTT addressable TV
- Data clean rooms and walled gardens

Why Hashed Email (HEM) Based Solutions Are Partial Solves

HEM based solutions like TTD Unified 2.0 and LiveRamp ATS are authenticated login solutions dependent on Single Sign On (SSO) or logged in users. Programmatic advertising in its current form, and indeed its future form can work well with these solutions using the RTB frameworks of connecting advertisers to publishers. However, while logged-in users are highly lucrative, they will not serve the long tail and/or the final consumer experience as logged-in users represent < 30% of the internet.

Open ID solutions like Unified 2.0 offers solutions that support:

- A replacement for cookies with an HEM/token based on a Single Sign On
- Single-click once authenticated (like Google/Facebook) with controls on consent
- A framework for publishers to connect with advertisers through programmatic pathways
- Momentum of the ad agencies and ad tech behind the initiative

The problems with such approaches include:

- Only Google and Facebook have established a universal SSO
- A global SSO is expensive, callbacks across the eco-system
- Consumers don't know TTD/LiveRamp, so need brand recognition
- Many privacy concerns being exposed as these personal identifiers are being deployed

Therefore, Universal ID (UID)-like solutions can be seen as fundamentally incompatible with Google's no personal identifier-based targeting, and according to a growing opinion among the privacy savvy, the usage of hashed emails can be even more privacy invasive than cookies. As bad as cookies have been made out to be by the Electronic Frontier Foundation (EFF) and other privacy bodies, all browsers ultimately gave users complete control to delete cookies, but hashed email (HEM) are forever floating in UID environments. The consent then given by a consumer is packaged into multiple relationships to increase portability across devices and environments like publishers, SSPs, and registration walls.

This is probably the reason why New York Times's SVP of Product, Allison Murphy, said the publication does not plan to use identity technologies, including Unified ID 2.0.

Rise Of Contextual and Associative Advertising

Contextual targeting is not new but, in recent years, has become a secondary approach for targeting as third-party cookie solutions ascended. There are two

approaches commonly used in contextual targeting. Keyword contextual targeting matches keywords on a page to determine suitability for ad placement. Semantic contextual targeting refers to showing ads that capture the "meaning" of a page.

However, the gap lives in the application of contextual solutions. It is one point to know how a page's context can be organized but its still another to make the decision on which parts of a contextual landscape to target. The cookie was the glue that connected first-party data and the contextual targets on the pages or videos. That connective tissue disappears without today's technology solution - the cookie.

As third-party cookies have continued to be restricted, contextual targeting solutions are increasingly substituted for audience-based solutions. Contextual targeting, although not strictly "identity," has re-emerged as a complementary in cases where there is limited first-party data. Contextual targeting does leverage first-party data, rather than third-party data, allowing users to maintain data privacy on data collection. Also, contextual does in most cases match browser's real time intent (looking for shoes now) rather than looking for shoes 30 days back in time.

We do expect contextual to rise in prominence; however, it will need a connection between intent and first-party data. Otherwise, we foresee it as a fairly limited advertising tactic.

Industry Spend Is Going to Shift to CTV/TV

CTV is a growing market and the amount of inventory entering the marketplace is exponential. Media technology platforms like the Trade Desk and Criteo are very optimistic about the CTV/OTT platforms and the ability to provide cross media measurement. However, we must be careful how the tracking mechanism of CTV, i.e. the IP address fairs under further scrutiny as it is already considered personal information under GDPR. Along with Google Gnatcatcher that deploys universal measures of IP address protection and other privacy initiatives, IP addresses are also under scrutiny. Therefore, we believe that even CTV advertising will eventually be targeted, optimized and measured by cohorts within 2 years. Therefore, Zip+4 level cohorts will be put to use, and this plays well with our product pathway of cohort optimization, i.e. EECO.

Clean Rooms and other data platforms

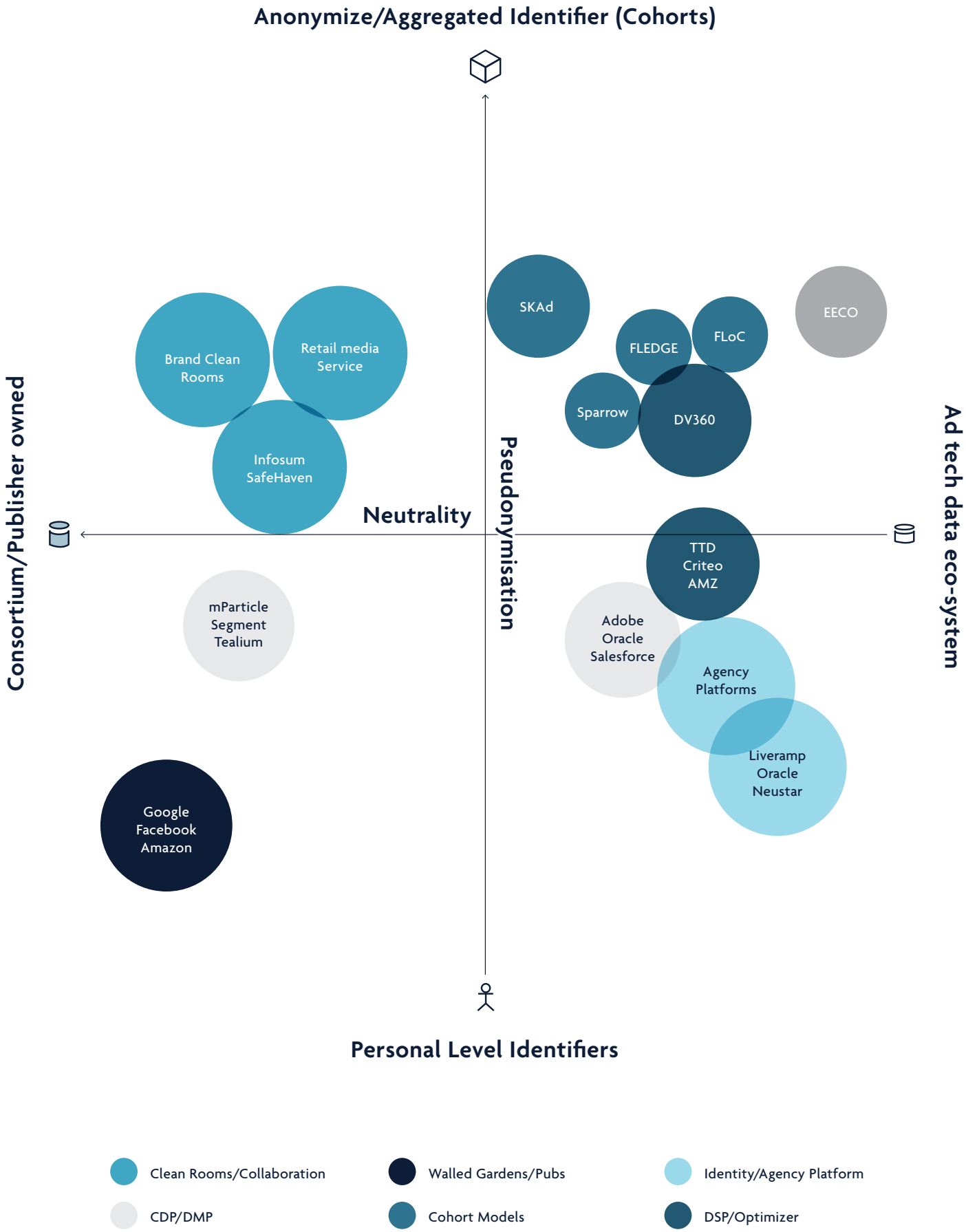
The need for a privacy and identity management solution has led to the formation of data clean rooms that allowed "walled gardens" like Google, Facebook or Amazon to match their audience data with brands' first-party data while maintaining strict controls for privacy and protection. However, the concept is now being explored by brands, publishers and even advertisers.

Clean rooms deploy a range of associated privacy-enhancing matching techniques and have evolved using the ability to link data via pseudonymised data whilst maintaining the security and privacy of that data from both partners. This ability to activate first-party data in another environment without sharing actual personal identifiers is also an extension of the clean room with use cases around insights, activation, media attribution and data modelling with consumer privacy and AI ethical oversight. This will become a key method that first-party brand owners like big retailers will engage with brand media spends particularly with data poor brands like CPGs without compromising their customers data rights.

Reshuffling Of The Ad Tech Stack

Below is our interpretation in a table format that showcases how the shift in advertising spend moves away from the programmatic eco-systems tied to cookie-based behavioral targeting, tracking and optimization.

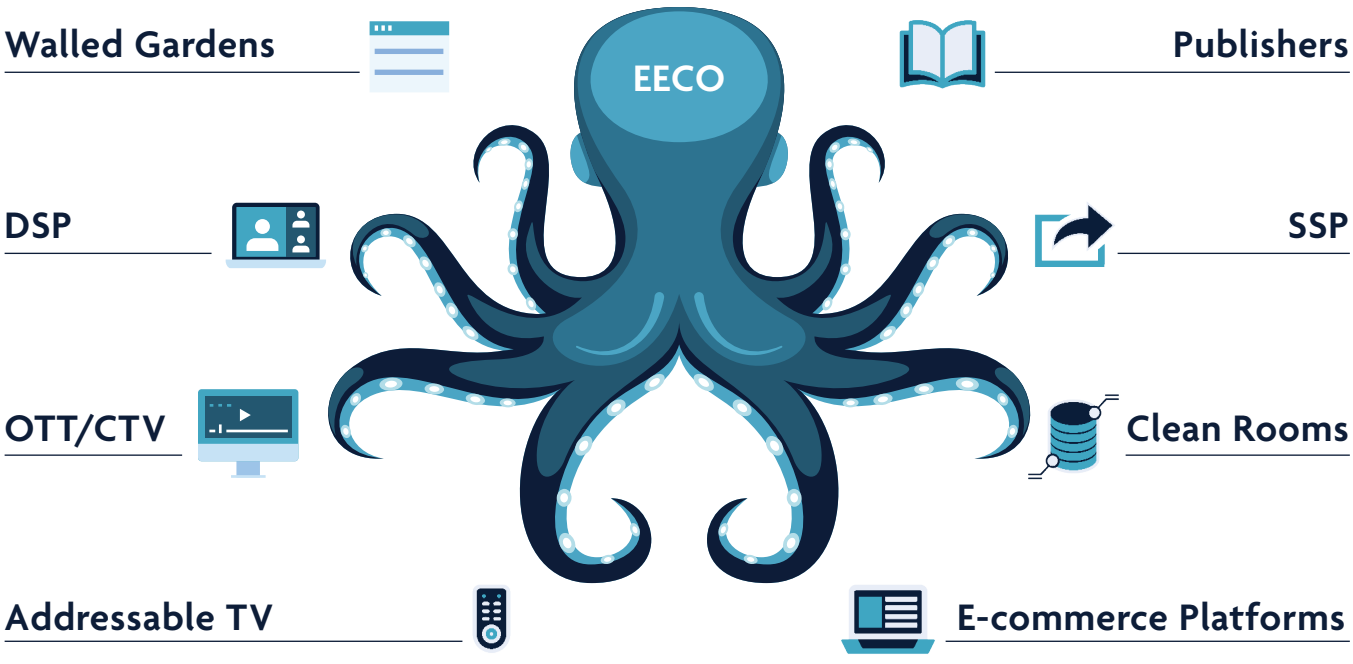
Targeting/Optimization Approach	Associated Regulatory Risk
The Big Brand Way: Proprietary ID based on authenticated first-party data matching (WarnerMedia, Roku, Walmart, Target)	Limited risk given use of first-party, consented data Requires higher focus on privacy and security of the use and storage of consumers' Personally identifiable information (PII), but holds limited risk in terms of potential future regulations
A common ID based on a first-party data match to a third-party, PII-based reference data set (Tradedesk Unified ID 2.0, LiveRamp ATS, Britepool, ID5)	Has browser risk if the browsers decide that the common ID has created a third-party identity workaround Based on HEM which is harder to delete and opt out than cookies
Common pseudonymous ID token based on cookies and older tech (LiveRamp IDL, Neustar, Oracle)	Further restrictions around the use of some types of browser or IP signals may limit the ability to target
Second-party data environment based on multiple clean room with anonymous ID linking (Infosum, LiveRamp Safe Haven)	Limited browser and policy risk but efficacy could be low, and the integration of end point id activation is complicated
Household ID based on IP address and geographic match (Acxiom, Experian, Merkel)	Potential new regulation that could put more scrutiny on data aggregators and collection of offline PII based data There is longer term risk in the U.S. that regulatory action may make IP addresses PII, reducing the ability to leverage it as a non-consented identifier
Contextual targeting (Vibrant Media, AdRoll, Nativo, TripleLift)	Limited risk at the browser and policy level because this approach leverages contextual information
Cohort based targeting and optimization based on first- or third-party data (FLoC, FLEDGE, SKAD, EECO)	Limited risk at the browser and policy level because this approach leverages cohorts constructed from our first-party data or at the browser level.


Anonymize/Aggregated Identifier (Cohorts)
Consortium/Publisher owned
Neutrality
Pseudonymisation
Ad tech data eco-system
Personal Level Identifiers
Brand Clean Rooms
Retail media Service
Infosum SafeHaven
SKAd
FLEDGE
FLoC
EECO
Sparrow
DV360
TTD
Criteo
AMZ
mParticle
Segment
Tealium
Adobe
Oracle
Salesforce
Agency Platforms
Liveramp
Oracle
Neustar
Google
Facebook
Amazon
Clean Rooms/Collaboration
Walled Gardens/Pubs
Identity/Agency Platform
CDP/DMP
Cohort Models
DSP/Optimizer

Introducing EECO

EECO is a cohort based, privacy-first, zero PII data approach, based on efficiency vs effectiveness, stochastic scheduling using Bayesian probability commonly known as the multi-armed bandit. It is an ethical and sustainable first-party data strategy that has customer privacy at its core. We believe creating, targeting, optimizing and measuring based on Cohort creation is the right approach. Instead of using big data and number crunching algorithms we are taking a step back and looking at this problem of cohort manipulation through a mathematical model. Our lead data scientist, Dimitri Vaynblat (PhD in Applied mathematics from MiT) describes it as "a contextual Bayesian model that can create a continuous cohort creation based on linkages and features that can learn more from walled gardens."

Cohort optimization is not segment optimization. It is not a new version of retargeting. Neiter is it a A/B testing framework. It is exposing probability on a group based on continuously segmented lift tests, control cells, marketing-mix models and intelligent feature-based optimization. This approach is far more privacy safe in theory than third-party tracking like HEM, MAID and cookies.



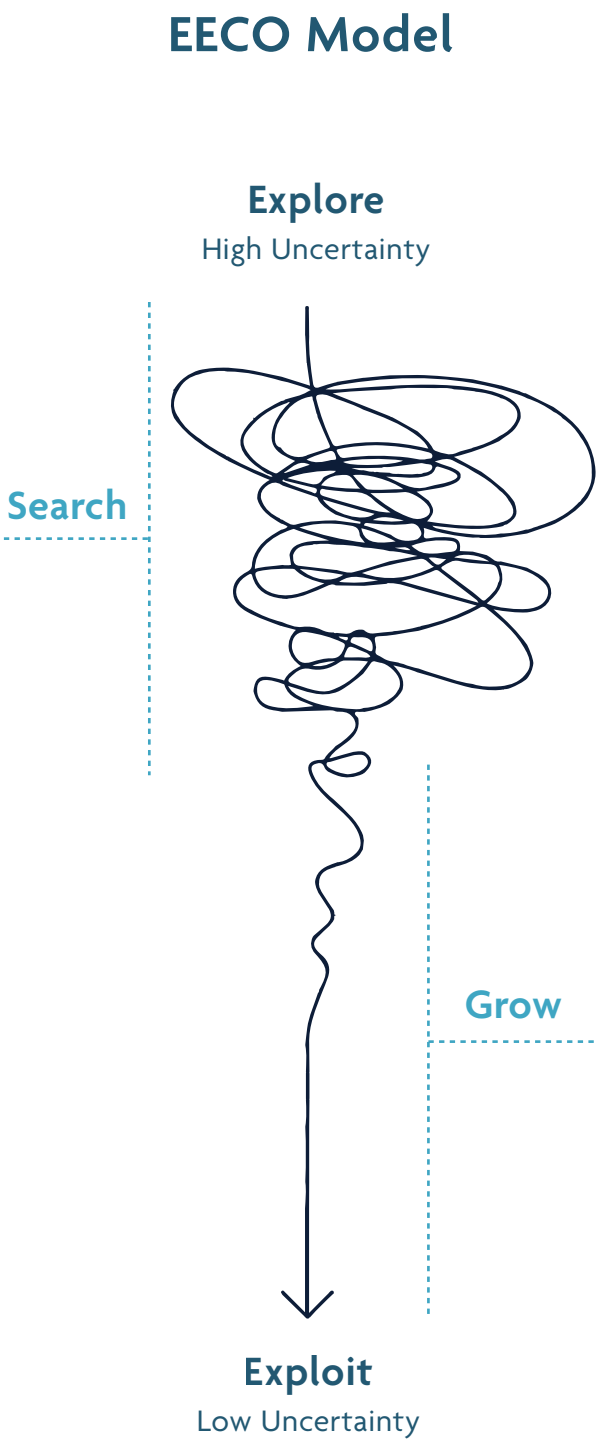
Proprietary Algorithm Based on Bayesian Multi-Armed Bandits

The Explore and Exploit Cohort Optimization Engine (EECO) empowers advertisers to optimize performance of their cohort-targeting campaigns in a privacy-safe manner using Bayesian multi-armed bandits.

At the heart of EECO lies deep reinforcement-based learning algorithms specifically tailored for probabilistic cohort-centric campaign optimization. They belong to the same family of algorithms that were behind Google's DeepMind' defeat of the world's best Go players, and today, enable robots to learn from their own experiences and behaviors.

By mastering exploration vs. exploitation trade-offs, the EECO algorithms maximize campaign performance through exploiting targeting strategies that have delivered the best results in the past while constantly exploring new strategies that might perform even better. The prescribed strategy is to start with a period of exploration, where you push structured campaigns at random and gather results. As you learn about which channel works and which do not, you shift spend towards the best performer (exploitation), while you keep exploring.

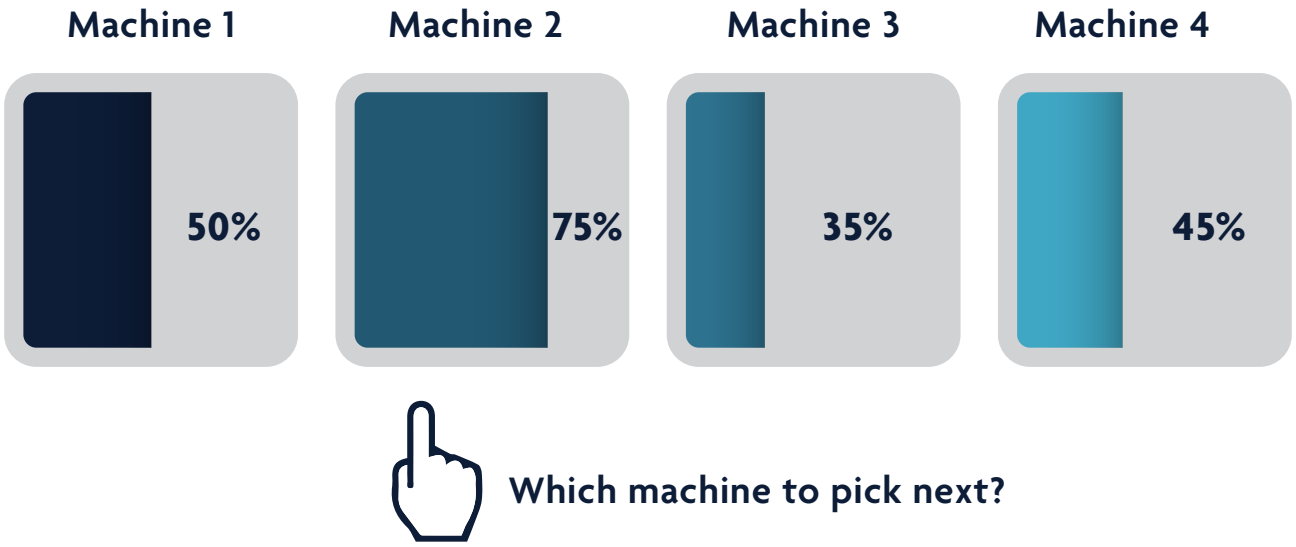
In short, explore when there is time to use the learnings and exploit when you are ready to harvest the learnings. The interval between is the strategy and thus the algorithm. These models are also classified as the 'multi-armed bandit' problem and their applications range from Hollywood sequels to choosing a restaurant in our everyday life and center around the latest(explore) vs the greatest(exploit).



Algorithm Overview

EECO's learning is considerably more efficient than that of any standard learning approach based on A/B/n testing. Unlike A/B/n testing, EECO is "earning while learning", taking advantage of what the engine has already learned, and not waiting until learning is fully completed for all options. EECO starts assigning more ad impressions (and budget) to the winning option as soon as it notices the difference in performance, and it increases the volume of ad impressions as the option's relative performance improves. EECO dramatically reduces the opportunity cost of learning by automatically steering to better performing options: ad impressions that would be wasted on obviously inferior options are assigned to potential winners. As a result, EECO shows improvement much earlier and delivers substantially better overall campaign performance.

In the example below, we showcase a multi-armed bandit model that shows multiple slot machines with some win probability. But we don't know these probability values. The challenge is, if we have to operate these machines one by one, how do you come up with a strategy to maximize your outcome from these slot machines in minimum time?



Functional Components

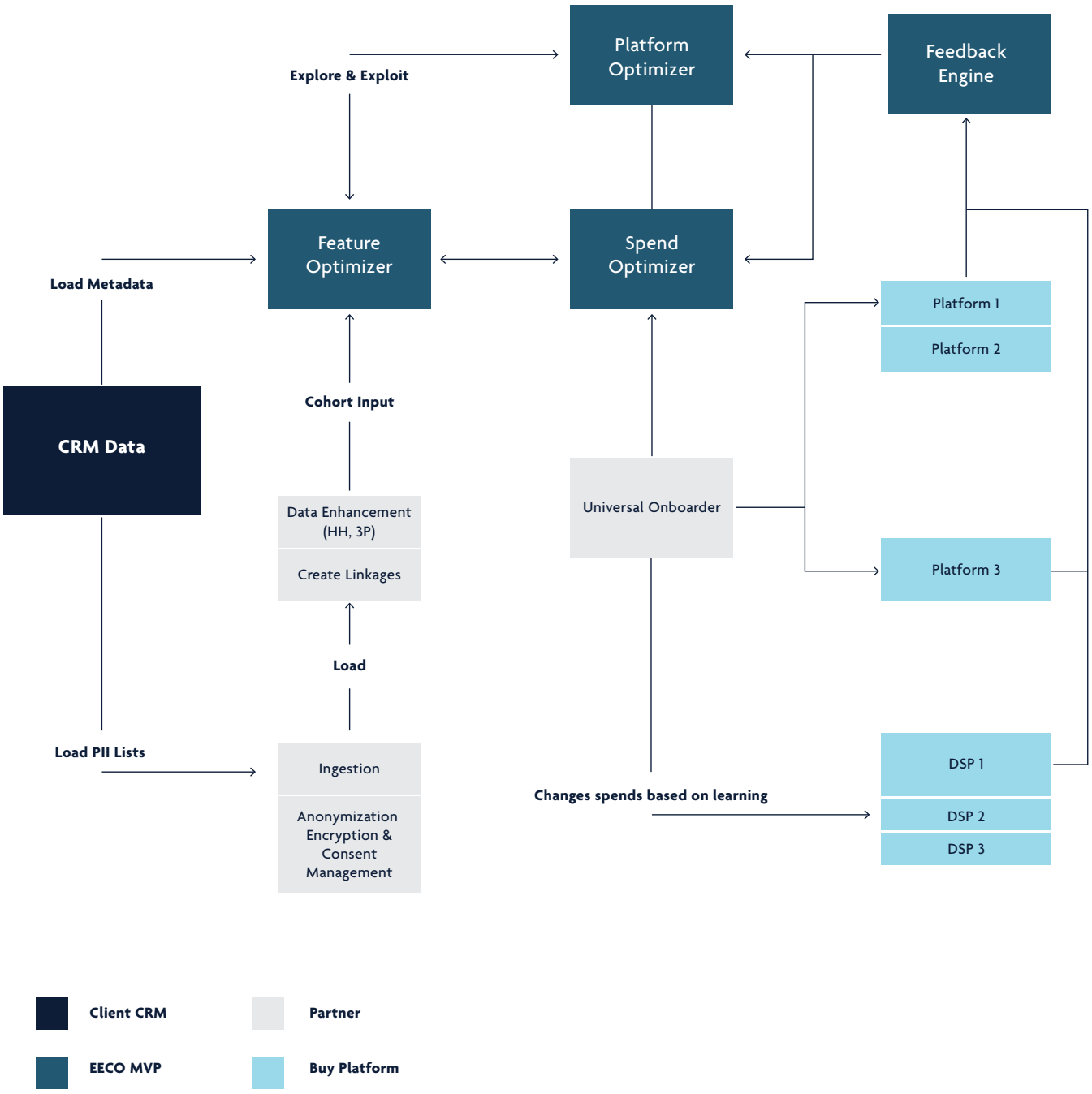
Our provisional patent filed with the USPTO defines in detail our methodology for the use of explore and exploit algorithms in the advertising industry. A high level schematic of the four underlying function component is represented below.

EECO Feature Optimizer takes input data at the PII level (TBD) for creating the cohorts based on ID linking and feature space that define the base data set.

EECO Spend Optimizer works specifically to move the media spend between campaigns and the cohorts that are based on explore and exploit methodology created by the feature optimizer.

EECO Platform Optimizer adds further context by adding different black box platforms optimization. The Feature, Platform and Spend Optimizer will create the algorithm for exploring and exploiting campaigns

EECO Feedback Loop works on building a coherent matrix of responses from all the various platforms and campaign performances. The campaign results from DV360 will be taken into the EECO reporting within the Privacy Sandbox framework and APIs.



Conclusions

All approaches discussed will depend on potential future changes in the regulatory landscape. Clean room, contextual and cohort-based advertising are the least likely to be affected by regulatory or industry-wide changes as they maintain first-party data separately and only use contextual or aggregated data.

The end effect is that as cookies are deprecated and brands and agencies struggle to calculate ROAS, it is important for advertisers to pursue a solution that is neither personal identifier-based, nor at the mercy of walled gardens' internal tracking which is the proverbial fox minding the hen house.

EECO particularly suits the current thinking around always-on, cohort-centric digital advertising realities. It focuses on continuous improvement of campaign outcomes by adopting a probabilistic approach to audience management and targeting. It is contrary to "throwing spaghetti at the wall to see what sticks," by using predetermined A/B testing cells and pushes for overall advertising effectiveness rather than programmatic efficiency with a privacy-first approach.

Glossary

ATTRIBUTION

The measurement of the value of each user interaction that contributes to a conversion within a campaign. Attribution allows marketers to more accurately measure the success of a campaign.

ANONYMIZATION

The de-identification of data such that it can never be re-identified.

AUTHENTICATED TRAFFIC SOLUTION

Liveramp's ATS connects publisher and brand identity to shape media experiences and measure effectiveness based on authenticated logged in user with transparency and choice.

CLEAN ROOM

Privacy-safe data environments through which platforms, brands and publishers can aggregate 1st party user data to expand audiences, gain insights, conduct measurement and determine ad frequency in a secure and privacy-compliant manner

COHORT

A group of individuals having a statistical factor (such as age or class membership) in common in a demographic study.

COLLABORATION

The process by which two or more parties decide to share data assets.

CONTEXTUAL ADVERTISING

Advertising that uses targeting based on the media content including keywords or whole page topic interpretation through semantic techniques.

CROSS-DEVICE IDENTITY GRAPH

A database of devices that have been deterministically or probabilistically linked based on the available identifiers in order to expand the view of the behaviors of that set of devices, including location. May be linked to an individual or household as part of a thirdor firstparty graph.

CUSTOMER DATA PLATFORM (CDP)

A cloud technology for the hosting, management, analysis and activation of first-party data with or without other data sources

DATA MANAGEMENT PLATFORM

A data management platform is a software platform used for collecting and managing data. They allow businesses to identify audience segments, which can be used to target specific users and contexts in online advertising campaigns.

DATA STORE/DATA EXCHANGE

A third-party data store or data exchange is the repository of third-party data placed for license by compilers of third-party data (data owners and data brokers), onboarded and matched to cookies and/or other linking identifiers made available to the programmatic marketing ecosystem via DMPs, DSPs, marketing clouds.

DETERMINISTIC MATCHING

An approach to matching that requires a definitive or exact match of values in two unique pieces of data or identifiers.

DIFFERENTIAL PRIVACY

An approach to eliminating re-identification of data through the addition of extra "noise" formed of incremental, unrelated data. The approach reduces the accuracy of a data set in the effort to gain privacy protection. Typically works best with larger data sets.

DEMAND SIDE PLATFORM

A company that helps advertisers manage multiple ad and data exchange accounts for media buying purposes.

FINGERPRINTING

The technique used to identify a device based on monitoring and mapping a wide range of device and other settings is recommended [for] parties [that] manage advertising related activities including targeting, frequency capping, fraud detection and reporting.

FIRST- PARTY DATA

First-party data is data that an entity (brand or media owner) has collected with permission from the consumer. The permissions determine the rights of the entity for the use of the data.

FEDERATED LEARNING OF COHORTS (FLoC)

Federated Learning of Cohorts is a type of web tracking through federated learning created by Google. It groups people into "cohorts" based on their browsing history for the purpose of interest-based advertising.

GDPR

According to GDPR: "Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"

GEOLOCATION DATA

Information regarding the physical location emitted from a user's device (mobile, desktop or smart device). The precision of data may vary considerably dependent upon the regulatory regime.

HASHED EMAIL (HEM)

A hashed email is a cryptographic function. Hashing is a way of encrypting a piece of data, like an email address, into a hexadecimal string. Each email has its own unique hexadecimal string that remains consistent no matter where the email is used as a login.

IDENTITY RESOLUTION

A step in the process of collecting and matching identifiers across devices and touchpoints to build a unified view of an individual customer or prospect that can then be used for segmentation and activation purposes.

IDFA

Short for "Identity for Advertising, an IFA is used "to maintain a high-quality audience experience within the Apple mobile eco-system

MAIDS

Mobile Advertising IDs, or MAIDs, are digital identifiers assigned to a specific mobile device that allow marketers to track, target and attribute across domains. The two most used MAIDs include Apple's IDFA and Google's AAID.

MEDIA MIX MODELS (MMM)

Media mix modeling (MMM), sometimes referred to as marketing mix modeling, is an analysis technique that allows marketers to measure the impact of their marketing and advertising campaigns to determine how various elements contribute to their goal, which is often to drive conversions.

MULTI-ARMED BANDIT

A Bayesian algorithm in which a fixed limited set of resources must be allocated between competing (alternative) choices in a way that maximizes their expected gain, when each choice's properties are only partially known at the time of allocation, and may become better understood as time passes or by allocating resources to the choice.

NON PII DATA

Information that does not directly identify an individual (or household, under CCPA).

PERMISSION

The rights given to the controller of data that allow its use for specific purposes.

PERSONAL INFORMATION ("CCPA")

According to CCPA: "Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."

PRIVACY-BY-DESIGN

A proactive and preventative approach to privacy intended to incorporate data protection as a grounding principle in the design of data systems, technologies and business practices.

PRIVACY SANDBOX

A solution designed by Google to replace third-party cookies with a range of APIs that rely on signals within a person's Chrome browser. The five APIs include the trust token API, the conversion measurement API, the privacy budget API (which limits the data a website can access through Google), the Federated Learning of Cohorts API (aggregated, cohort-based insights) and TURTLEDOVE.

PROBABILISTIC MATCHING

An approach to matching that establishes a match between sets of data leveraging inferred, modeled or proxy assumptions.

PSEUDONYMIZATION

The reversible de-identification of data by substituting data points/characters with pseudonyms using an external key. Pseudonymised data can be linked to other data and thus remains "personal information" under CCPA and "personal data" under GDPR.

RTB Exchange

A platform for automated selling and buying of online advertising inventory. On an ad exchange, the buyers are advertisers, media agencies, and retargeting net-works, and the suppliers are networks and publishers.

SSP

A supply-side platform or sell-side platform (SSP) is a technology platform with the single mission of enabling publishers to manage their advertising impression inventory and maximize revenue from digital media.

SECOND PARTY DATA

2nd party data is data shared in a dedicated environment with a clearly defined set of permissions and rights set between each of the parties managing the environment

TAXONOMY:

The practice and science of classification.

THIRD-PARTY DATA

Third-party data is any information or data collected by an entity that does not have a direct relationship with the end user or data subject that the data is being collected upon.

TURTLEDOVE (FLEDGE)

An acronym for Two Uncorrelated Requests, Then Locally Executed Decision On Victory. TURTLEDOVE is a Google-proposed, privacy-safe solution that processes and stores user behaviors locally in their browsers through edge computing (versus the traditional approach of storing these data attributes on servers operated by SSPs, ad exchanges or publishers).

UNIFIED ID 2.0

The Trade Desk Unified ID based on prebid.js and their proprietary SSO solution.

WALLED GARDENS

A walled garden provides an alternative to the cookie-less future that concerns advertisers and marketers. Walled gardens are built on a foundation of logged-in users, which allows them to track each person across device.