

Oracle Corporation
Response to the ACCC's Digital Advertising Services Inquiry
Interim Report December 2020
30 March 2021

A. Introduction

1. Oracle Corporation (**Oracle**) supports the preliminary conclusions that the Australian Competition & Consumer Commission (**ACCC**) has reached from its investigations of Australia's advertising technology (**adtech**) services market,¹ as set out in the Interim Report for the ACCC's Digital Advertising Services Inquiry (**Adtech Inquiry**).
2. The ACCC has found that, in the case of the four key adtech services (advertising ad server, demand side platform (**DSP**), supply side platform (**SSP**) and publisher ad server services), Google's share of revenue and impressions is significant. In fact, the ACCC determined that in 2019, for advertiser ad server and publisher ad server services, Google held an almost 100% market share. There is no reason to expect that this position has changed since 2019.
3. The ACCC has described Google's anti-competitive conduct in the market for adtech services in detail in the Interim Report. This conduct includes the conduct that Oracle outlined in its submission to the ACCC's Issues Paper for the Adtech Inquiry,² including for example requiring the use of Google's own DSP for purchasing YouTube inventory, having the consequence of pushing advertisers to use *only* Google's DSP for all of their digital advertising. The Interim Report also raises a number of other concerns, from the perspective of publishers, which were not the subject of Oracle's earlier submission to the ACCC, but which are equally important – this includes the anti-competitive manner in which Google participates in header bidding as well as the fees that Google charges for its products such as Open Bidding and Google's Unified Pricing rules.
4. As the ACCC has acknowledged, the lack of competition in the adtech supply chain caused by Google's dominant position across all adtech services has economy wide implications, publishers suffer because they receive less for their inventory than they would in a competitive market, which negatively impacts on the volume of quality content (including in the case of media companies, public interest journalism) that publishers are able to produce, to the detriment of Australian consumers. On the other hand, advertisers across the board pay more for digital advertising (including adtech services) than they would in a competitive market, adding to their costs which are passed on to consumers for goods and services across the economy.
5. Oracle's view remains, as set out in its earlier submission to the ACCC, that there are strong grounds to pursue a case against Google under section 46 of the Competition and Consumer Act 2010 (Cth) (**CCA**). Oracle is supportive of the ACCC continuing to assess whether to commence those proceedings. There is also likely a strong case for the ACCC to commence proceedings on the basis that Google's conduct is unconscionable in breach of section 21 of the Australian Consumer Law, and Oracle encourages the ACCC to consider this as well. The focus of this submission is however on the regulatory reform proposals that the ACCC has put forward for consultation and other regulatory reform Oracle respectfully suggests the ACCC should consider supporting.
6. The first point that should be made in relation to these regulatory proposals is that, given Google's dominance of adtech services is a global not simply an Australian problem, it is important for the ACCC to work closely with its international counterparts to ensure that the regulatory solutions the ACCC puts forward to the Australian Government in its final report

¹ In the Interim Report the ACCC has not definitively stated whether it believes there is one adtech services market or multiple markets. Oracle has taken the same approach in this submission, referring to the "adtech services market" but without definitively concluding whether there is one market or multiple markets under the Competition and Consumer Act 2010 (Cth) in Australia.

² That submission is available here

<https://www.accc.gov.au/system/files/Oracle%20%2813%20May%202020%29.pdf>

from the Adtech Inquiry are consistent with solutions that are proposed to be implemented globally. In this regard, data separation (that is, the ACCC's Proposal 2) is a key remedy that would have international support. In part, this would require Google to, in effect, reverse the decision it made in 2016 to combine DoubleClick data (that is, data from adtech services) with data from Google's consumer facing services. That decision significantly enhanced Google's "data moat" and created an insurmountable barrier to competition from third parties in the provision of adtech services. Data separation also requires that Google provides a meaningful option to consumers to withhold their consent to the use of their data that is collected from consumer facing services for targeted advertising. To be meaningful, this must be implemented through an "opt-in" mechanism and consumers must be able to continue to use Google's services in the event that consent is withheld.

7. The ACCC's Proposal 2 is not the only regulatory intervention that is necessary to address Google's anti-competitive behaviour. We have supported, with some recommended modifications, the ACCC's proposed data portability and data interoperability interventions, which are included in Proposal 1. These reforms, collectively, will assist in addressing Google's anti-competitive practices, which will have economy wide benefits. In addition, the ACCC in its final report from the Adtech Inquiry should look to adjacent markets and whether regulation is required to address Google's anti-competitive behaviours in those other markets that contributes to Google's dominance in the provision of adtech services.
 8. As in the case of Oracle's submission to the Issues Paper for the Adtech Inquiry, this submission is provided largely from the perspective of advertisers, rather than publishers.
- B. Need for coordinated global action to address global competition problems**

The competition problems arising from Google's behaviour – highlighted in the Interim Report – have been recognised in many other jurisdictions.

1. The competition concerns the ACCC has highlighted in the Interim Report are not unique to Australia. For example, as the ACCC is aware, the UK's Competition & Markets Authority (**CMA**), in the Final Report from its 2020 Online Platforms and Digital Advertising Market Study (**CMA Report**),³ found amongst other matters that Google has a dominant position in the supply of adtech services in the UK – in 2019, this amounted to a 90 to 100% share of the publisher ad server segment, 80 to 90% of the advertiser ad server segment, 50 to 60% of SSP services and 50 to 60% of DSP services.⁴ The CMA also found that Google's behaviour in relation to the supply of adtech services (those supplied by Google itself as well as those supplied by other providers) and in adjacent markets has had a chilling impact on competition. The CMA Report pointed to Google's use of its market power in search and the wider digital services ecosystem to build its position as a DSP and also to the clear conflicts of interest that arise because of Google's vertical integration, which has led to self-preferencing behaviours that have had a negative impact on competition.
2. As a consequence of concerns similar to those raised by the CMA in relation to the provision of adtech services (and in other digital services markets) the European Commission has

³ The final report from that Market Study is available here: https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf

⁴ As described on page 19 of the final report from the CMA's Market Study.

proposed a new Digital Markets Act which has the aim of promoting competition in online markets, predominantly by prohibiting certain unfair practices.

3. In addition, the anti-competitive practices of Google have been subject to significant scrutiny in the US. On 16 December 2020, ten US States (led by the State of Texas) commenced proceedings against Google regarding its anti-competitive practices related to the provision of adtech services. The alleged anti-competitive conduct extends into many areas, including Google forcing publishers to use Google's ad server and ad exchange following its acquisition of DoubleClick, using its dominant position to foreclose ad exchange competition, taking action to undermine header bidding and entering into anti-competitive agreements with Facebook which include market allocation and price fixing provisions.
4. The following day, that is, 17 December 2020, 38 US States (led by the State of Colorado) commenced proceedings against Google in relation to search and other anti-competitive conduct. The three main forms of anti-competitive conduct alleged in this second case are Google's arrangements with third parties to ensure access by consumers to competitor services is limited, the use of Search Ads 360 to direct advertisers to Google's search advertising services and away from competitors and Google limiting the ability of consumers to bypass Google search and go directly to websites of third party specialised vertical providers of search services. Although not directly concerned with the adtech services that are being considered in the Adtech Inquiry, the allegations in this case demonstrate how Google has acted in an anti-competitive manner to amass the first party consumer data that it has used to entrench its position as the dominant provider of adtech services and also the pattern of anti-competitive conduct by Google in relation to a broad range of digital platform services.
5. Google has been the subject of scrutiny by the US's Subcommittee on Antitrust, Commercial and Administrative Law of the Committee of the Judiciary in its Investigation of Competition in Digital Markets.⁵ The majority staff report from that Investigation, released in early October 2020, reached similar conclusions to those of the ACCC. Although the Investigation did not focus on adtech services, the report did point to the lack of transparency regarding these services, noting that for example Google does not disclose to publishers what their inventory is sold for and how much of the purchase price is retained by Google.⁶ The report pointed to evidence it received that Google's vertical integration had led to conflicts of interest that enable Google to favour its own services and create significant information asymmetries.⁷ The report summed up in relation to adtech services by noting the following concerns about Google's anti-competitive practices raised by market participants:
 - (a) Depriving advertisers and publishers of key market and pricing information and maintaining market opacity.
 - (b) Leveraging market power in search advertising to compel advertisers to use Google's products in the display advertising market.
 - (c) Leveraging control over YouTube to foreclose competition in digital video ad serving in part by excluding rival ad servers from accessing YouTube.
 - (d) Inhibiting interoperability between Google's ad platforms and non-Google ad platforms.

⁵ The Majority Staff Report and Recommendations from that Investigation are available here: https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf

⁶ As discussed at, for example, pages 129 and 130 of that report.

⁷ As discussed at pages 207 and 208 of that report.

- (e) Using its search dominance to impose standards like Accelerated Mobile Pages (AMP) that, as a result of depriving publishers of user data, benefit Google's ad business.⁸

Australia's recent experience with the news Media Bargaining Code highlights that Australia is well placed to take a leading role in developing innovative and effective global solutions for the global competition problems in relation to adtech that the ACCC has highlighted in its Interim Report.

6. There is a clear need to coordinate global solutions to these global problems. This has been recognised not only in Australia, but in other jurisdictions that have been closely examining the actions of digital platforms. For example, in the CMA Report, after noting that consultation and engagement had occurred with many other jurisdictions, including Australia, concluded:⁹

We believe these forms of international engagement are vital in seeking to develop a consensus on the issues and the potential solutions to the global challenges posed by digital platforms.

7. The CMA made many other comments in the CMA Report that acknowledged the need for a coordinated approach to these issues globally.¹⁰
8. Australia has taken a global lead in other areas of digital platforms regulation, most recently in relation to the proposed Media Bargaining Code, which has resulted in the dominant platforms, Google and Facebook, for the first time, agreeing to pay compensation to Australian media companies for the use of their content. This is a world first. As Rod Sims has said on the question of whether international regulators are collaborating in relation to digital platform regulation:

We certainly talk to each other and try to learn from each other ...¹¹

9. By implementing much needed regulation in the area of adtech services, in a manner that is consistent with proposals that are being considered elsewhere, Australia will again be able to lead the way as it has for the Media Bargaining Code.
10. Certain of the new regulation that the ACCC has proposed in its Interim Report would be able to be coordinated with other jurisdictions and rolled out in a globally consistent manner to ensure that it is effective in not only addressing the issues that have been identified in the Interim Report but also in ensuring that such competition problems do not re-emerge in the future. This regulation is primarily:
- (a) Proposal 2, which deals with data separation.
 - (b) Proposal 1, dealing with:
 - (i) data portability; and

⁸ As discussed at page 211 of that report.

⁹ As set out at page 33 of the CMA Report.

¹⁰ Including for example at pages 359, 418 and 437.

¹¹ Standing Committee on Economics, House of Representatives, public hearing, 24 February 2021. The official transcript is available here (see page 16):

https://www.aph.gov.au/Parliamentary_Business/Committees/House/Economics/ACCCAnnualReport2019/Public_Hearings

- (ii) data interoperability.

C. Data separation

Appropriate forms of data separation regulation

1. The ACCC's Proposal 2 is to consider data separation mechanisms to level the playing field between large platforms with a significant data advantage and competing adtech services providers. There is only one platform with such a significant data advantage, which is Google. This Proposal 2 regulatory solution should be limited to entities that are dominant adtech services providers in Australia. At the current time there is only one such provider, which is Google. By limiting the class of entities to which the proposed regulation applies, this will mean that regulation is appropriately targeted, that an inappropriate regulatory burden is not imposed on other firms and also that regulatory uncertainty is not created.
2. The proposals that the ACCC has put forward for comment are:
 - (a) direct regulation of the internal sharing of data within a single company by prohibiting the combination of certain types of datasets;
 - (b) rules prohibiting the use of certain types of data, such as related to health or medical conditions, for ad targeting purposes; or
 - (c) imposing limitations on the use of data collected from user-facing services for targeted advertising purposes except with user consent.

To achieve the intended pro-competitive outcomes, direct regulation that prohibits the combination of specific data types as well as restrictions on the use of data are required.

3. The different data separation options that have been put forward should not be considered as mutually exclusive. Oracle's perspective is that the first option, that is, prohibiting the combination of different data sets, is an important component of a viable and effective response to the competition problems that have been created by Google's vast data advantage. The only logical separation would be to require that Google is obliged to separate the data that it collects from its consumer facing services, including Android OS and Google search, from the data that it collects through its adtech services.
4. This would, in a practical sense, reverse the action that Google took in 2016 to combine data from its consumer facing services with DoubleClick data. Google was only able to take that action in 2016 as, at that time, its dominant position in relation to the provision of consumer facing services allowed it to do so. By that time, Google's dominance meant that it no longer needed to offer services that were privacy protective for consumers by keeping those different types of data separate, as it had previously assured consumers it would do.
5. As ACCC Chair, Rod Sims commented when announcing in 2020 that the ACCC had launched a misleading and deceptive conduct case against Google in relation to its actions in combining DoubleClick data with other consumer data held by Google:¹²

Google significantly increased the scope of information it collected about consumers on a personally identifiable basis. This included potentially very sensitive and private information about their activities on third party websites. It then used this information

¹² The ACCC's media release is available here: <https://www.accc.gov.au/media-release/correction-accc-alleges-google-misled-consumers-about-expanded-use-of-personal-data>

to serve up highly targeted advertisements without consumers' express informed consent.

and:

The use of this new combined information allowed Google to increase significantly the value of its advertising products, from which it generated much higher profits.

6. In other words, the ACCC is well aware that it is the combination of these two different types of user data that creates the most significant benefits for Google.
7. The second option, which is restrictions on the use of certain sensitive types of data for advertising related purposes, should be separately considered in the Australian Privacy Act review which is currently being undertaken by the Australian Government, as it is a remedy appropriately suited to address privacy concerns. It is not a remedy that could hope to address the significant barriers to entry and expansion (and consequent antitrust problems) in the market for adtech services arising from Google's data collection practices.
8. The third option, which requires user consent for the use of that user's data for targeted advertising, should be implemented together with option one. Again, it should be limited in its application to dominant adtech services providers, which would initially be Google. At the current time digital services providers, such as Google, require consumers to agree to the collection of extensive, highly personal data as a condition of using the provider's services. When faced with a "take it or leave it" choice by Google, consumers have no real choice but to provide consent, because a consumer may not use any of Google's services unless she does so. This third option, when implemented, must change this current position by providing real choice to consumers. Consumers must be required to positively opt-in to provide consent, that is, the default settings for a consumer must provide that such data collection will not occur – only if the default setting is changed by the consumer to positively agree for her data to be used for targeted advertising would this be permitted. A consumer who does not agree to allow her data to be used for ad targeting must be able to continue to use all of Google's consumer facing services, in the same manner as if she had opted-in to ad targeting.

Balancing efficiency benefits and competitive harms

9. The ACCC raised in the Interim Report the prospect that mandating data separation may create short term reductions in efficiency in Google's adtech services which would need to be offset by longer term competition gains. The true position is that there would be significant short term and long term competition gains from mandating data separation in relation to Google which will vastly outweigh any short term efficiency losses to Google. The immediate benefit would be that the data separation would limit the scope for Google to engage in a broad range of the anti-competitive conduct that the ACCC has identified in the Interim Report. Other service providers will then be able to compete more effectively with Google's adtech services not only because of a levelling of the playing field between Google and those other providers but because Google's ability to engage in other anti-competitive conduct is diminished.
10. Mandating data separation would also address some of the other competition and consumer harms that arise from Google's ability to combine the data that it collects from its consumer facing services, including Android OS and Google search, with the data that it collects through its adtech services. Specifically:
 - (a) The ACCC has suggested in the Interim Report that data separation may be appropriate where data collected through conduct involving a misuse of market power within a market is used to adversely affect competition in other markets. This is exactly what has occurred here. Google, which is the dominant provider of consumer facing services

such as search services, is able to misuse that market power to require consumers to provide consent to the collection of much larger volumes of data than are required to provide those services. It then uses that data – together with the data that it accumulates through its provision of adtech services (which we would also argue Google misuses its market power to collect) – to adversely affect competition in relation to the supply of adtech services. This, in Oracle’s view, is a clear breach of section 46 of the CCA. A data separation requirement would go some way towards addressing this breach.

- (b) As Oracle has pointed out in other submissions to the ACCC,¹³ the provisions of Google’s privacy policy that allow it to combine data collected through adtech services with other data are unfair contract terms for the purposes of section 23 of the Australian Consumer Law. In particular:
- (i) these terms create a significant imbalance between the rights and obligations of the parties (Google obtains the ability to create a super profile of the consumer which it is able to monetise but the consumer receives a benefit of a lesser value, being the right to use Google’s services and suffers detriment because she loses the ability to control her online privacy);
 - (ii) the ability to combine this data is not necessary to protect Google’s legitimate interests;
 - (iii) significant detriment to a consumer occurs as a result of her loss of control of privacy; and
 - (iv) finally, there is a lack of transparency in the terms of Google’s privacy policy and its general terms and conditions which significantly impedes the exercise by consumers of the limited rights that they do have to opt out of targeted advertising and the combination of their personal information in connection with such targeted advertising (which are only available to those Australian consumers with a Google Account in any event).

11. In addition to addressing these issues, if a data separation regulation is imposed, in the longer term innovation will be enhanced as well as efficiency, which will (as the ACCC has acknowledged) itself contribute to improving competition leading to better outcomes for publishers and advertisers across the economy, and therefore better outcomes for Australian consumers.

Privacy implications: not required to be of general application

12. The ACCC suggests in the Interim Report that implementation of Proposal 2 could require close consultation with the Office of the Australian Information Commissioner. This is not necessary as the data separation arrangements would only be imposed on dominant adtech services providers, initially only Google, to address its insurmountable data advantage for the purposes of improving competition in the supply of adtech services. The Privacy Act should not be the vehicle used to enact this regulation. The data separation obligation should be implemented under the CCA reflecting that the primary intention is to address a competition concern. There is no need to impose the regulation on all entities that are subject to the Privacy Act. No other provider of adtech services collects the vast quantities of personal

¹³ See for example this submission made in relation the ACCC’s Digital Platforms Inquiry at page 15: <https://www.accc.gov.au/system/files/Oracle%20Corporation%20%28March%202019%29.PDF>

information that are collected by Google and therefore there is no policy rationale – from either a competition or a privacy perspective – to impose this regulation on any other entity.

Consistent with international precedent

13. Pursuing this option of data separation would also be consistent with international precedent and allow for the international harmonisation that Oracle has argued in this submission is required. As the ACCC has acknowledged in the Interim Report, recommendation 4 of the CMA Report is that the new Digital Markets Unit of the CMA be given powers to introduce pro-competitive interventions, including data separation. Unsurprisingly, the reasons for the CMA putting forward this proposal mirror the reasons advanced by the ACCC. The CMA concluded that Google's¹⁴ vast quantities of consumer data, amassed across their extensive user-facing services, analytics services and devices that use Android OS, creates a virtually impenetrable barrier to entry and expansion in adtech services. Data separation would be one way to address this. However, as acknowledged in the CMA Report and also the Interim Report, this of itself will not be the only regulatory intervention required to address Google's anti-competitive behaviour.

Implementation of this regulation

14. As both the ACCC and the CMA (in relation to its similar proposals) have acknowledged, the regulation will be straight forward to implement. But compliance must be monitored and audited to ensure the regulation achieves its intended aims. Enforcement action will be necessary in the event of breach.
15. The ACCC's existing powers under the CCA, as well as the European Commission's proposed Digital Markets Act, provide an appropriate model for the investigatory powers that the ACCC would need to properly monitor the proposed data separation regulation.
16. The Digital Markets Act provides for an audit process in relation to particular digital markets practices.¹⁵ This could be adapted for use in relation to the mandated data separation arrangements. Specifically, the CCA could be amended to require Google to undertake, and provide to the ACCC, an independent audit of the processes it has implemented to comply with its data separation obligation within 6 months of the commencement of the regulation. In addition, an independent audit could be required to be undertaken annually, or every 2 years, to determine if Google is continuing to comply with this obligation.
17. Given it will be difficult to determine whether or not Google is in compliance with this regulation simply from independent observation of Google's market behaviour, the ACCC's powers under section 155 of the CCA should be expanded so that the ACCC has a specific right to issue a section 155 notice to obtain information, documents or evidence to determine whether or not Google is in compliance with this data separation obligation. This should be supplemented by a specific power, similar to that in the proposed Digital Markets Act,¹⁶ for the ACCC to undertake inspections of Google's systems (and appoint its own auditor to do so) to ensure effective monitoring of compliance. This specific power is necessary as it will not be possible otherwise for the ACCC to independently observe whether Google is in compliance.
18. The CCA provides for remedies for non-compliance which should apply to a breach of the data separation regulation. Those remedies should also apply to a breach of the provisions for monitoring compliance.

¹⁴ The same comments applied to Facebook, though in the context of other digital services.

¹⁵ As described in Article 13.

¹⁶ As described in Article 21.

D. Data portability

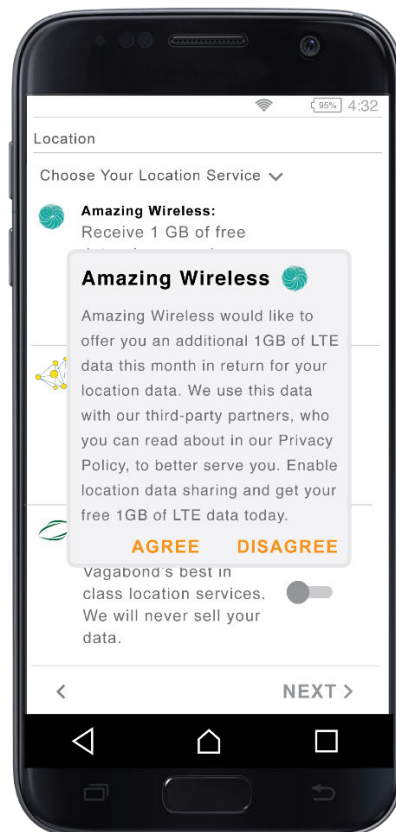
Data portability is an important regulatory option to ensure that competition is enhanced and consumers are empowered.

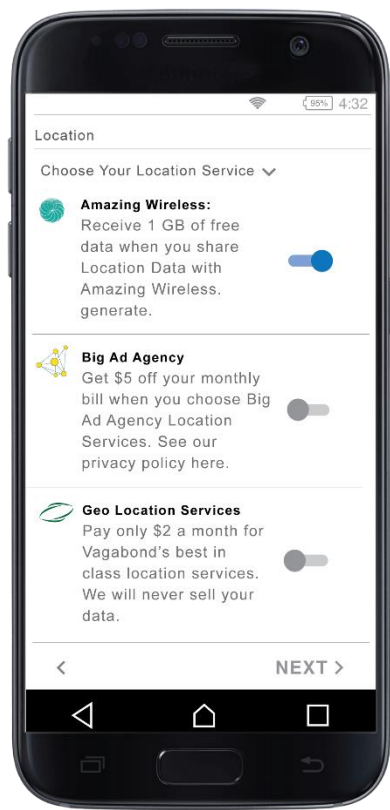
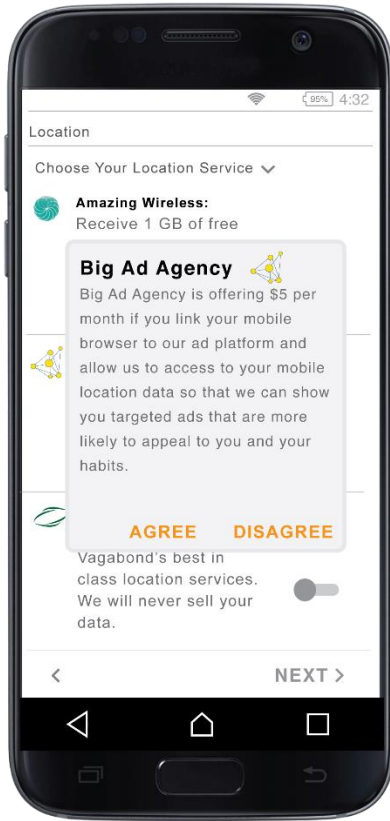
1. The ACCC has suggested as part of Proposal 1 that measures could be implemented to increase data portability provided safeguards are implemented to ensure that consumers have sufficient control over the sharing and processing of their data.
2. In mid-2020, Oracle lodged a submission to the Treasury's Inquiry into Future Directions for the Consumer Data Right, a copy of which is at **Attachment A**, which recommended the extension of Australia's world leading consumer data right (**CDR**) regime to location data collected through smart devices.
3. Location data, such as GPS coordinates, altitude, Wi-Fi scans, cell tower readings and other information, is collected via smart devices on a continuous, real time basis. Oracle suggested in its Treasury submission that CDR was applied to location data, rather than a broader range of information that is collected from consumers online, as location data is easy to collect (and transfer) and is very valuable.
4. Location data is particularly valuable for targeted advertising purposes. As the ACCC noted in the Final Report from the Digital Platforms Inquiry, the value of that data is indicated by the fact that sales of location targeted advertising reached an estimated US\$21 billion in 2018.¹⁷ Although value is obtained from collecting that data over a long period (including to make inferences), it is particularly valuable when used on a real time basis – for example, to target advertising when a consumer is near a particular retail outlet or to provide information on traffic conditions as consumers travel in vehicles.
5. As set out in Oracle's submission to the Treasury, there are significant benefits to providing consumers with portability rights in relation to location data, which will be achieved whether portability is implemented via CDR or another, simplified regulatory regime:
 - (a) consumer welfare will be enhanced as consumers will for the first time be given control of their location data, which is a very sensitive category of their personal information;
 - (b) consumers will for the first time be able to fairly harvest the value of their location data;
 - (c) adtech services providers, advertisers and others will have the ability to compete to acquire this data in a way that is not currently possible;
 - (d) there will be direct and indirect benefits across the economy from increased competition and innovation in the adtech services sector, including (but not limited to) in Australia's media sector as media companies will be able to derive more value from their inventory; and
 - (e) data-driven innovation will potentially also be enabled in other sectors, through other uses of location data expressly permitted by Australian consumers.
6. The value to consumers of this data portability right will be enhanced if the consumer also has the right to request that any person who holds that consumer's location data is required to delete it. For example, if a consumer exercises her portability rights by requiring her location data to be transferred to her internet service provider, she should have the right to require

¹⁷ As referred to on page 385 of the Final Report.

that Google (or any other digital services provider) does not separately hold that location data and deletes any previously collected and stored location data.

7. The ability of consumers to control the transfer of location data can be enabled by choice screens presenting various options to the consumer via their smart devices during the set-up process. For example, intermediaries seeking consumer data could develop an offering, presented as a settings configuration during the set-up process, and consumers could pick from a selection of entities (including Google) depending on their interests and preference. After initial set-up, consumers could re-configure their choice if their preferences change over time by revisiting their settings— providing entities wishing to acquire location data from a consumer for value with an easy way to reach consumers with their competing offers.
8. A practical example of how this could work is shown in the different screenshots below.





9. As demonstrated by these screenshots, a user-configurable setting can enable an individual to transfer her location data in exchange for benefits offered by different entities, as potential data recipients. Entities wishing to receive location data could offer individuals, through their devices, a wide range of different benefits in exchange for location data, including free data, coupons, cash rewards, discounts, or even something less tangible such as the opportunity to contribute location data for projects that would benefit the community.
10. The screenshots above demonstrate that, in addition, individuals could be given choice as to what types of location data can be collected, how often that collection would occur and by what means (for example, only via Wi-Fi so the consumer's data plan was not used for the collection). Again, this gives individuals a greater level of control than currently exists in relation to this valuable data set.
11. Although CDR could be used to implement this type of location data portability regime, a simpler regulatory framework could be implemented. This is the case as location data is already widely collected from Australians. This collection is permitted provided the Privacy Act (where applicable) is complied with in relation to that collection. As noted in the ACCC's Final Report from the Digital Platforms Inquiry, OECD research from 2013 found that 29% of the top rated paid apps and 60% of free apps in the Google Play Store sought permission to collect a user's location (and presumably therefore did collect it, even if it was not required for the delivery of the services offered by the app).¹⁸ At the current time, it is likely that an even greater proportion of apps collect location data.
12. Under a simplified model of data portability, the only necessary regulation would in fact be to enable consumers to *restrict* the collection, retention and use of location data by Google and other operating system owners and/or digital services providers that were subject to the regime.¹⁹ Enabling individuals to impose such restrictions will ensure that the entities (if any) to whom the consumer agrees to "sell" their location data will be able to obtain value from the use of that data. Specifically:
 - (a) Google facilitates the collection of location data by app providers. If an app uses Google Android application programming interfaces (**APIs**) to collect location data, Google receives a copy of this location data. As a result, Google has the largest pool of location data collected from consumers, and app providers have a subset that is non-unique. Regulation should prohibit Google from collecting this data or using it for any purpose unless a consumer has provided express opt-in consent to Google doing so. Further, Google should not be able to restrict use of any of its services (including Android OS) by a consumer if that consumer does not provide that consent.
 - (b) Regulation should require that smart devices are configured so that consumers have more direct control over the collection and use of their location data, that is, to facilitate the use of apps such as the app described above so that individuals are able to directly select who may receive their location data (and who is not authorised to receive it).
 - (c) A simplified data portability regulatory regime would work in tandem with the data separation proposal that Oracle has outlined above. Digital services that require location data (such as for example Google in relation to Google Maps) should be required to comply with directions from users that the location data may only be used for the provision of the relevant service, and not for any other purpose (including but

¹⁸ Final Report, at page 385.

¹⁹ As set out in the submission at Attachment A, Oracle suggests that the data portability regime applies only to a limited category of entities, potentially initially operating system providers and then on a delayed basis a category of digital services providers that meet particular size thresholds.

not limited to for the delivery of targeted advertising). As would apply where a consumer did not agree to allow Google to use her data for targeted advertising, entities subject to the regime should be required to allow a consumer to use that provider's digital services even if the consumer does not allow that provider to use their location data for purposes other than the direct use of the relevant digital service.

E. Data interoperability

Data interoperability, by whatever technical means it is achieved, will enhance competition by providing other adtech services providers with the information required to compete with Google and by enhancing transparency.

1. The Interim Report's Proposal 1 also includes a recommendation in relation to data interoperability. Data interoperability refers to businesses sharing data without a direct request from a consumer. As the ACCC has noted, because consent from individuals is not obtained, data interoperability typically only occurs for non-personal, aggregated or anonymised data.
2. This part of Proposal 1 specifically links to the common transaction ID and the common user ID that the ACCC has recommended in Proposals 5 and 6. Use of common transaction IDs (Proposal 5), would allow data interoperability in relation to information about individual transactions. This is useful from the perspective of an advertiser for both measurement and attribution purposes (as discussed below). Proposal 6, for a common user ID, would allow tracking of all ads that a user viewed. This would assist not only in attribution, as the ACCC has mentioned in the Interim Report, but also with frequency capping (that is, with ensuring that the same user is not served the same ad too many times). Although the ACCC has suggested the use of these common IDs, in this submission, Oracle is not endorsing any particular form of technology to achieve interoperability. The key issue is to ensure that interoperability is achieved, as it is necessary for a properly functioning adtech services market.
3. As Oracle explained in its submission to the ACCC's Issues Paper for the Digital Platforms Inquiry, data interoperability is key to the operation of adtech services market from the perspective of advertisers. Advertisers rely on a data pipeline to ensure that their digital advertising campaigns are effective. Data interoperability is key at three specific points in a campaign process:²⁰
 - (a) *Bidding*: An advertiser needs to determine what price to bid for the purchase of digital inventory, and what inventory to bid for, so that it does not pay too much for its advertising, to assist in bidding for the right inventory to reach its target audience and to ensure that it is not advertising too many times to the same user (frequency capping).
 - (b) *Measurement*: An advertiser needs to determine the value that it obtains from its advertising campaign, that is, how many consumers actually saw (and if relevant heard) the advertisement in a brand safe environment. This allows the advertiser to compare

²⁰ Data is also important at the initial stage of an advertising campaign, which is the point at which an advertiser determines its target audience, however the data needed for targeting is not obtained through the interoperability mechanisms discussed in this section of the submission.

ad quality across publishers and determine which publishers it wishes to continue to purchase inventory from.

- (c) *Attribution*: Where advertising converts to a sale, an advertiser needs to know what ad or ads contributed to that sale so that the advertiser can optimise future advertising budget allocations.
4. As demonstrated in Oracle's earlier submission, and also set out in the ACCC's Interim Report, Google inhibits data interoperability at every level in relation to the supply of adtech services. This is also detailed in **Attachment B**, Oracle's presentation on Adtech Essentials Digital Demand and Supply. In summary:
- (a) *Bidding*:
 - (i) In 2018, Google announced that it would limit access to Google's UserIDs. This impacted bidding as it became more difficult for advertisers that did not use Google's adtech services to bid on inventory. A separate "cookie syncing" process²¹ is required to be undertaken by non-Google adtech services providers, including DSPs and ad exchanges, to identify users and therefore to determine whether a user falls within the target audience for the advertiser (and also how many ads the relevant user has seen for that advertiser's products or services – that is, to undertake frequency capping). This cookie syncing process is only approximately 60% accurate, creating significant inefficiencies.
 - (ii) Google's proposal to remove all cross domain cookies in Chrome by 2022 and replace these with Google controlled "Privacy Sandbox" private APIs would mean that advertisers will lose the ability to independently undertake targeting or frequency capping.
 - (b) *Measurement*:
 - (i) In Google's premium display DSP, Display & Video 360 (**DV360**), YouTube and non-YouTube video ad performance appear on separate reports and are measured on different metrics. This means that advertisers are unable to make direct comparisons between YouTube ad performance and non-YouTube ad performance.
 - (ii) From May 2019, Google restricted the use of non-Google monitoring tools on YouTube. Adtech services providers that measure ad fraud (that is, whether an ad was seen by a human or a bot) and viewability (that is, whether the ad was displayed or whether it was blocked or only partially visible to the user) are now only provided with aggregated data curated by Google. In addition Google does not provide any data on the specific YouTube video on which an ad appears, meaning it is impossible to measure brand safety for YouTube advertising.
 - (iii) It is possible to undertake independent ad measurement on the Google Display Network,²² but the reports provided cannot be integrated with the metrics of any independent viewability vendors and therefore those reports cannot be used for algorithmic optimisation.

²¹ Cookie syncing is necessary as different adtech services providers (including DSPs and ad exchanges) use their own IDs to store information they have collected about a user. Under the syncing process, the companies work together to match IDs to enable the use of their own data – only the IDs, not stored information, is shared and therefore cookie syncing does not breach privacy laws.

²² Google Display Network sites reach over 90% of internet users worldwide.

- (iv) The limitations on access to Google’s UserIDs in 2018 also impacted the provision of independent verification services.
- (c) *Attribution:*
- (i) Google’s decision in 2018 to block access to its UserIDs had a significant negative impact on the ability of independent attribution services providers to access the information that is required to properly assess the ads that contributed to conversion.
 - (ii) The data collected by advertiser ad servers is critical to determining attribution. Google’s advertiser ad server, Google Campaign Manager, has no API to export ad interaction data. This makes it impossible for third party attribution services providers to access raw data from that advertiser ad server to measure attribution.
 - (iii) Google’s proposal to remove all cross domain cookies in Chrome by 2022 and replace these with Google controlled “Privacy Sandbox” private APIs would mean that advertisers will entirely lose the ability to independently undertake conversion tracking.
5. Oracle supports greater data interoperability to assist in relation to bidding, measurement and attribution, by whichever technical means is most appropriate to achieve this. Data interoperability should not be limited only to the data that is linked to the common transaction IDs and user IDs that the ACCC has suggested. As outlined above (and in more detail in Oracle’s submission to the ACCC’s Issues Paper for the Adtech Inquiry) Google has limited the access to vital information needed for bidding, measurement and attribution. Providing for data interoperability only in relation to impression tracking and the number of ads that a user has seen is insufficient to address the competition impacts of Google’s behaviour.
 6. The data interoperability requirements should also encompass the requirements that the ACCC has included in Proposal 4 as part of a proposed industry standard. Specifically, monitoring tools that meet agreed criteria should be able to be used across all websites to enable necessary information to be collected to allow for independent assessment of viewability, ad fraud and brand safety. It is neither necessary nor appropriate for this to occur under a voluntary industry standard. It should be independently developed and appropriately monitored and enforced. These are roles that the ACCC should undertake.
 7. It would be a straight forward process for the ACCC to develop a regulation which specified the criteria that the monitoring tools must meet. If those criteria were met, any blocking of the tools by Google (or any similarly dominant provider) in respect of its own adtech services or other digital services should then be directly prohibited under the CCA. This would be a mechanism that was very straight forward in its application and also straight forward to monitor and enforce. As it would apply only to clearly defined dominant providers, it would also avoid any regulatory uncertainty.
 8. Allowing for data interoperability, as outlined above, will not create privacy issues. The types of information that would be accessed and used would be aggregated and anonymised data. In the event that there were any concerns as to privacy, it would be possible to impose a generally applicable regulatory obligation that restricted adtech services providers for seeking to use the relevant data categories to identify specific individuals.

F. Proposal 3: Industry rules

1. The remaining proposal from the Interim Report to be considered in this submission is Proposal 3. This proposal is for the implementation of industry rules (that is, a self-regulatory

industry code regime) for the management of conflicts of interest and self-preferencing in the supply of adtech services.

2. The ACCC has suggested these industry rules would encompass:
 - (a) the implementation of rules to manage conflicts of interest, such as preventing the sharing of information or “best interests” obligations;
 - (b) requirements to provide equal access to adtech services to limit the scope for self-preferencing; and
 - (c) increased requirements for transparency, which it is hoped would reduce both the ability and incentive of vertically integrated adtech services providers to engage in self-preferencing conduct.
3. Oracle is not supportive of a self-regulatory code or industry rules in the market for adtech services for a number of reasons. First, there is the question of the appropriate body to develop such a code given that, in the first instance, as the dominant adtech services provider, Google should be the only entity that would be subject to the regime. Google should not be given the task of developing the code itself. Recent history in Australia has shown that this will not achieve the intended outcome, noting that the ACCC’s proposal for voluntary bargaining codes between the dominant digital platforms (including Google) and media companies was unsuccessful. It was not until a mandatory code was developed and close to being passed by the Australian Parliament that Google agreed to negotiate with Australia’s media companies.
4. There is then also the question of who would have the role of ensuring compliance with such a code. It would seem unlikely that any non-government entity would be sufficiently resourced to appropriately monitor compliance with such a code and to resolve disputes. The ACCC is the only appropriately resourced (and knowledgeable) agency in Australia who could perform such a role.
5. The proposed industry rules themselves are not sufficiently robust. For example, the ACCC has suggested it is hoped that increased transparency requirements would reduce both the ability and incentive of vertically integrated adtech services providers to engage in self-preferencing conduct. Instead of imposing increased transparency requirements, regulation should simply be introduced that had the direct effect of prohibiting this self-preferencing conduct by dominant adtech services providers.
6. Again, as in the case of other proposals put forward in this submission, such regulation would be clear and straightforward to enforce. This would remove regulatory uncertainty, as would ensuring that the regulation applied only dominant adtech services providers (currently only Google). The regulation could directly specify requirements to provide equal access to adtech services such as by requiring that the dominant provider’s services (for example, ad servers) make ad interaction data necessary for attribution services available to third parties who provide those adtech services.

G. Other proposals should be considered by the ACCC

The ACCC in its Final Report should not limit its recommended regulatory proposals to those directly relating to the adtech services market. The ACCC needs to consider also the anti-competitive actions of Google in adjacent markets, as those actions have contributed to Google’s adtech services dominance, and propose appropriate regulatory interventions in those markets.

1. The ACCC should not limit its final recommended regulatory proposals to those that are outlined in the Interim Report. In addition to directly addressing Google’s anti-competitive

actions in relation to adtech services as provided for in the regulatory proposals in the Interim Report, the ACCC should consider proposing regulation to address Google's anti-competitive actions in adjacent markets which contribute to Google's dominance in the adtech services market.

2. The ACCC is aware of the US Department of Justice's (**DoJ**) case²³ against Google in relation to Google search. That case focusses on the anti-competitive agreements that Google has entered into with Apple, original equipment manufacturers (**OEMs**) and others to maintain its dominant position in search. As mentioned earlier in this submission, on 17 December 2020 38 US States commenced proceedings against Google which contain a similar complaint to that contained in the DoJ case.
3. The US States allege in their case that Google enters into arrangements with third parties to ensure that access by consumers to competitor search services is limited. Those arrangements provide not only that Google is the default search option but also, in many cases, that it is the *exclusive* search option. For example, Google pays Apple between US\$8 billion and US\$12 billion per annum to ensure that it is the default search engine on Apple devices. It also uses restrictive contracts to limit general search competition on Android devices.
4. The US States case correctly argues these agreements are anti-competitive because users rarely change defaults therefore meaning that Google obtains an unfair advantage in the supply of this consumer facing service. In the US, such arrangements have resulted in Google being the default search engine on 80% of web browsers. It is also the default search option on most smart devices. The US States case argues that Google's anti-competitive behaviour is also evident in relation to voice assistants, IoT devices and connected cars. The DoJ case contains similar allegations and makes clear that Google's anti-competitive tying practices extend to other consumer facing products beyond search.²⁴
5. These anti-competitive agreements, because they are a large factor in Google's dominance in consumer facing services markets, assist Google to collect the vast quantities of consumer data that create the insurmountable barriers to entry and expansion in the adtech services market. These anti-competitive agreements are a form of exclusive dealing. Agreements that provide for Google search to be the exclusive search option as a condition of providing that app, or any other apps or services, fall squarely within the exclusive dealing provisions of the CCA. In addition, agreements of the type discussed in the DoJ case that require Android OEMs that take particular Google apps to also take a bundle of other apps, make certain of Google's apps undeletable and provide that these must appear on the home screen are also in a practical sense exclusive dealing agreements. Given the restrictions imposed by Google under such arrangements, in a practical sense, OEMs have no ability to enter into agreements with other app providers for the pre-installation of other equivalent apps.

²³ A number of US States are also party to this case.

²⁴ For example, paragraph 55 of the DoJ complaint (available here: <https://www.justice.gov/opa/press-release/file/1328941/download>) states: *Next, for Android device manufacturers that sign an anti-forking agreement, Google provides access to its vital proprietary apps and application program interfaces (APIs) for preinstallation, but only if the manufacturers contractually agree to (1) take a bundle of other Google apps, (2) make certain apps undeletable, and (3) give Google the most valuable and important real estate on the default home screen.*

6. These types of exclusive dealing should be expressly prohibited under section 47 of the CCA, as these agreements clearly have the purpose (as well as the effect) of substantially lessening competition not only in the relevant consumer facing digital services markets but also in the adtech services market. The notification process that applies generally to exclusive dealing should not apply to this type of conduct.

H. The case for an unconscionability claim

1. Although not raised in Oracle's previous submission to the ACCC on the Adtech Inquiry, there is also a strong case that Google's behaviour is unconscionable, in breach of section 21 of the Australian Consumer Law. Oracle urges the ACCC to consider this in determining what, if any, further investigations of Google's behaviour in the supply of adtech services it proposes to undertake.
2. Under section 22 of the Australian Consumer Law, in analysing whether a person (in this case Google) has engaged in unconscionable conduct in relation to the supply of goods or services for the purposes of section 21, the courts are required to have regard to a wide range of factors. Looking at some of these factors as these apply to the supply of adtech services by Google:
 - (a) *Relative bargaining strengths:* In the supply of adtech services, whether on the demand (advertiser) or supply (publisher) side, there is a significant imbalance of bargaining power between Google and its customers. This is the case even for the largest publishers and advertisers.
 - (b) *Conditions reasonably necessary for the protection of legitimate interests of the supplier:* Google imposes a range of restrictive terms on its customers in relation to the supply of adtech services that are simply unnecessary for the protection of its legitimate interests. Many of these are listed in the ACCC's Interim Report and referred to elsewhere in this submission, as well as Oracle's submission to the ACCC's Issues Paper for the Adtech Inquiry.

One simple example is the restriction imposed by Google on advertisers using third party data to enhance the targeting of their advertising campaigns. This is an unnecessary restriction, which imposes significant detriments on advertisers. Google does this not to protect any legitimate concern in relation to privacy. Instead it takes this action to ensure that advertisers must instead use only data that is supplied via Google and to increase reliance on Google's adtech services.
 - (c) *Willingness to negotiate contractual terms:* There is no ability to negotiate in any meaningful way with Google in relation to the terms for the supply of its adtech services. Both publishers and advertisers are presented with "take it or leave it" terms, particularly in the case of small and medium sized enterprises.
3. The factors listed above are examples only and Oracle encourages the ACCC to fully investigate whether Google's behaviour is in breach of section 21.

I. A final word on privacy

1. A final comment should be made in relation to privacy. The ACCC in its Interim Report has commented on a perceived "tension" between enhanced competition and the protection of privacy. For example, the Interim Report states:²⁵

... Google often publicly claims that privacy legislation, or consumer expectations of privacy, prevent it from releasing the data sought. But without access to the more detailed information, publishers and advertisers consider that they have to make

²⁵ See page 18 of the Interim Report.

decisions based on trust that the service is operating as claimed, which is unacceptable in a commercial relationship.

Both competition concerns and privacy issues are able to be addressed by appropriate regulatory interventions.

2. While privacy concerns must be addressed in relation to the collection, use and retention of personal information, it should not be forgotten that competition issues arise because personal information, once collected, is an asset in the hands of the holder. The ACCC must not ignore competition problems in the adtech services markets because of erroneous claims that all questions relating to the regulation of dealings with personal information must be considered solely through a privacy lens or cannot be considered at all because privacy concerns take priority.
3. As Oracle set out in its submission to the ACCC's Issues Paper, Google uses privacy concerns as an excuse to disguise the anti-competitive reasons for its actions. There is no reason why privacy should be sacrificed in a competitive adtech services market. In fact Google's actions demonstrate that the reverse applies, that is, privacy rights of individuals are in fact sacrificed in uncompetitive digital markets – a clear example is the fact (as noted earlier and in other Oracle submissions) that Google only took the privacy destroying action of combining DoubleClick data with the data that it collected on individuals in consumer facing digital services markets when it had reached a position of sufficient dominance in those consumer facing digital services markets that individuals had little choice but to agree to such combination occurring.
4. The proposals put forward in the Interim Report are intended to improve competition. However, a consequence of adopting many of these proposals, modified in the manner specified in this submission, would be that Australian privacy protections would be enhanced. In particular:
 - (a) Data portability provides power to individuals to control who has access to their personal information, and how it is used, in a way that is simply not possible under the Australian Privacy Act.
 - (b) Imposing a data separation obligation on Google will go some way towards addressing the concerns that Australians continually express in relation to the collection and combination of extensive amounts of their personal information for targeted advertising purposes. Australians would also, as part of this proposal, be given the right to make a positive decision as to whether or not to allow their personal information to be used for targeted advertising – a significant step forward from the current “take it or leave it” choice users are presented with.
5. Data interoperability is the remaining proposal put forward by the ACCC that would deal with personal information. Data interoperability is currently undertaken without breach of privacy regulation, not only in Australia but in other jurisdictions – including under the European Union's General Data Protection Regulation. There is no reason why data interoperability, however it is technically implemented, cannot be undertaken in a manner that is compliant with Australian privacy laws.
6. In short, it will be possible to implement reforms to promote competition in adtech services while at the same time enhancing the ability of Australians to protect their privacy. Not only for the reasons outlined immediately above but also because a more competitive adtech

services market will facilitate innovation – and it would be expected that this innovation would include the development of adtech services that promote the protection of privacy.

Thank you for considering this submission. Oracle would be very pleased to discuss any of the issues that have been raised with the ACCC.

30 March 2021.

Attachment A: Oracle Corporation Submission to the Inquiry Into Future Directions for the Consumer Data Right

ORACLE CORPORATION

**SUBMISSION TO THE INQUIRY INTO FUTURE DIRECTIONS FOR THE
CONSUMER DATA RIGHT**

10 JUNE 2020

Introduction

1. Thank you very much for providing an opportunity to Oracle Corporation (**Oracle**) to make this submission to The Treasury's Inquiry into Future Directions for the Consumer Data Right Inquiry (**Inquiry**).
2. Oracle is a global technology company with a broad portfolio of solutions for companies of all sizes. Oracle brings a unique perspective to the Inquiry in this submission, as its technology expertise means that it is well placed to comment in relation to the application of Australia's consumer data right (**CDR**) in the digital context.
3. The key intent of the Inquiry is to look at how the CDR could be enhanced to boost innovation and competition, and support the development of a safe and efficient digital economy, benefiting Australians and Australia. As Oracle explains in this submission, a key way to achieve those outcomes is to expand the CDR to enable the regime to be effectively applied to personal information which is collected from consumers when they use digital services, where those digital services are provided by digital platforms, via applications (**apps**) or from the use of a myriad of different internet connected devices, such as smart phones, smart TVs, smart speakers and the like.
4. A key type of information collected online is location data collected via mobile smart devices. Location data encompasses personal location and activity information which is collected from a consumer via her mobile device. That data may be collected from sensors such as GPS, WiFi, Bluetooth, etc. There are significant benefits in applying the CDR to location data, though potentially in future the CDR could be applied to other types of clearly defined digital personal information that is collected from consumers as they use digital services.
5. The location data collected by entities such as Google is very valuable. Consumers create that information and therefore own it. In recognition of this, consumers should have the right to share in the value of their location data and the right to have a greater choice and say in how that information is used. The CDR is able to be applied to grant consumers these rights.

Applying the CDR to location data will provide consumers with control over this type of personal information in a way that has not been possible since mobile devices have become ubiquitous, it will allow Australians to extract value from a valuable asset that it should be recognised is owned by Australians, not by the entities that collect the data, and it will promote efficiency, innovation and competition in the adtech services sector (and other sectors including Australia's media sector), benefiting the Australian economy as a whole.

6. The application of the CDR to location data, as Oracle has suggested in this submission, is an important step in moving forward to address the competition issues that exist in the Australian adtech services sector. However, it is not the only step that needs to be taken. The Australian Competition & Consumer Commission (**ACCC**) is currently undertaking an inquiry into the markets for the supply of digital advertising technology services and digital advertising agency services (**Adtech Inquiry**). Although the Adtech Inquiry is important in ensuring ongoing regulatory attention on the competition issues in the adtech sector, the ACCC should quickly move forward using its existing enforcement powers to address the

market failures that are already apparent in that sector. Regulators globally have recognised the need to take action, and are moving forward quickly.¹

7. To effectively apply the CDR to location data, certain amendments are required to the Competition & Consumer Act 2010 (Cth) (**CCA**) and to the Privacy Act 1988 (Cth) (**Privacy Act**). These changes will provide important protections to Australians, including to limit the circumstances in which this category of personal information may be collected and used without the consent of the individual to whom the data relates.
8. We have explained in this submission the proposals that are being considered in the UK for the expansion of its Open Banking regime to information that is collected by digital platforms from consumers. There is an opportunity to work with the UK to ensure that both jurisdictions adopt a similar approach, reflecting the recommendations set out in this submission, which will be for the benefit of both jurisdictions, and ensure that compliance is easier to achieve for regulated entities. A common approach should act as an incentive for other jurisdictions to adopt similar regimes. However, Australia should not delay in moving forward in expanding the CDR, if the UK adopts a slower pace.

¹ For example, action is being taken at a Federal and State level in the United States:
<https://www.wsj.com/articles/justice-department-state-attorneys-general-likely-to-bring-antitrust-lawsuits-against-google-11589573622>

Benefits arising from the application of the CDR to location data

Summary

As stated in the Explanatory Memorandum for the CDR legislation:

the CDR aims to increase competition, enable consumers to fairly harvest the value of their data, and enhance consumer welfare.²

For the reasons explained in this submission, implementing the CDR in relation to location data will achieve all of these aims:

- consumer welfare will be enhanced as consumers will *for the first time* be given control of their location data, which is a very sensitive category of their personal information
- consumers will *for the first time* be able to fairly harvest the value of their location data
- if implemented together with other regulatory action which Oracle has called for in its submission to the ACCC's current Adtech Inquiry, innovation will be promoted and competition will be increased in the adtech services sector, leading to improved outcomes for the Australian economy and consumers
- there will be direct benefits across the economy from increased competition and innovation in the adtech services sector, including (but not limited to) in Australia's media sector
- data-driven innovation will be enabled in other sectors, through other uses of location data expressly permitted by Australian consumers.

To ensure appropriate protections are in place for consumers, changes are required to Australia's competition and privacy regulation in conjunction with this expansion of the CDR.

What location data is collected?

General comments

9. A great deal of digital personal information is collected about Australians through their online interactions, including through their use of personal computers, mobile smart devices (and apps on those devices) and the myriad of Internet of Things (IoT) devices that Australians increasingly have in their homes, such as smart TVs. Much of this data is highly personal location data, identifying individuals and the details of their lives.
10. For example, Google is able to collect intensely personal renderings of an individual's online and offline life through the digital services that it offers. The information it collects, some of which is location data, includes:
 - (a) data from every active user input into a Google service (in the form of, for example, watch history on YouTube or directions requests on Google Maps);

² Paragraph 1.3 of the Explanatory Memorandum for the Treasury Laws Amendment (Consumer Data Right) Act 2019.

- (b) details regarding virtually every internet-connected user's private browsing activities on the desktop and mobile internet (whether through browsers or apps, including Google and third-party apps on Android and on other mobile operating systems (**OS**)); and
 - (c) for those Australian consumers with an Android mobile device, precise details about everywhere that individual has been, how they got there, and what they were doing there, which is obtained through the constant stream of granular location and activity data that Google gathers through such mobile devices (whatever privacy settings a consumer adopts).
11. The ACCC's Final Report from the Digital Platforms Inquiry includes an extensive list of data that Google collects about Australians.³ All of this information is combined by Google across services, across devices, and over time, such that Google has a deep historical and highly specific picture of nearly every internet-connected individual's behaviour and interests. As Google's then-CEO said in 2010, "*We know where you are. We know where you've been. We can more or less know what you're thinking about.*"⁴
 12. At the present time, Google primarily uses this personal information (including location data) for advertising purposes. The value of that information can be seen from Google's revenues. In 2019, the revenues of Alphabet Inc. (Google's parent company) were US\$162 billion, almost all of which was generated from digital advertising.

Location data is valuable

13. Location data is one of the most valuable types of digital personal information that is collected by Google (and others).
14. As stated by the ACCC in its Final Report from the Digital Platforms Inquiry:

*The increase in personal mobile devices such as smartphones, and the improvement in location tracking technology, has led to an increase in the location data collected and used. The prevalence of location data was flagged by Google CEO Sundar Pichai in his testimony to the United States Congress in 2018, where he stated that location is 'in the fabric of how people use the internet today'. Likewise the value of location data is indicated by the fact that sales of location targeted advertising reached an estimated US\$21 billion in 2018.*⁵
15. Over time, location data creates a detailed profile about a consumer; where she lives, works, shops, eats, who she socialises with, and many other revealing insights about her pattern of life. The collection of location data over a period of time allows any third party who has access to that location data to infer sensitive and unique information about an individual.
16. For example, figure 1 below shows a small amount of data collected by Google, via an Android device, that initially seems benign (a record listing the Wi-Fi base station that Android device is connected to, along with a timestamp). Yet, if an individual connects to the same Wi-Fi access point at 9:00am Monday to Friday, it is clear the Wi-Fi base station likely represents the individual's place of work. Similarly, if an individual connects to the same Wi-Fi base station every day at 7:00pm and stays connected through the evening, the Wi-Fi base station is likely located in the individual's home.

³ See Table 7.2 on page 380 of the Final Report from the ACCC's Digital Platforms Inquiry.

⁴ Eric Schmidt, *Google CEO: "We Know Where You Are. We Know Where You've Been. We Can More or Less Know What You're Thinking About,"* BUSINESS INSIDER (Oct. 4, 2010), <https://read.bi/2unSd5l>.

⁵ Final Report at page 385.

```

{
  "timestampMs": 1550094845569,
  "wifiConnectivityStatus": {
    "mac": 123597800553519,
    "wifiConnectionStatus": "CONNECTED"
  }
}

```

Figure 1: Test Android Device reporting Wi-Fi connection to Google

17. The following table shows in detail the location data that is collected from Android devices by Google.

Location Data Element	Collected by Google?
GPS Coordinates + Accuracy	YES
Altitude	YES
Wi-Fi Scans	YES
• MAC Address	YES
• Signal Strength + Frequency	YES
Bluetooth Beacon Scans	YES
• MAC Address	YES
• Signal Strength + Frequency	YES
Cell Tower Readings	YES
Barometric Pressure Readings	YES
Activity Readings + Confidence Level	YES
Source of Location Reading (Cell or Wi-Fi)	YES
Connection to Wi-Fi Access Points	YES
IP Address	YES
PlaceIDs	YES
Rate + Change in Rate of Collection	YES

Table 1: Types of location data collected by Google

18. Google is able to collect these types of location data from every Australian who has an Android device, as well as from Australians who use many of Google’s other ubiquitous services, such as Google Maps.
19. As noted in the ACCC’s Final Report from the Digital Platforms Inquiry, OECD research from 2013 found that 29% of the top rated paid apps and 60% of free apps in the Google Play Store sought permission to collect a user’s location (and presumably therefore did collect it, even if it was not required for the delivery of the services offered by the app).⁶ Google facilitates the collection of location data by app providers. If an app uses Google Android APIs to collect location data, Google receives a copy of this location data. As a result, Google has the largest pool of location data collected from consumers, and app providers have a subset that is non-

⁶ Final Report at page 385.

unique. This means that although Google is not the only digital services provider that collects location data, Google has the ability to monetise consumer location data in ways others cannot (since they do not have a unique pool of location data that exceeds Google's).

Designation of location data

20. Under Part IVD of the CCA, location data derived from mobile devices, either collected via the OS itself or collected via apps meeting specific criteria, could be designated in accordance with section 56AC(2) of the CCA as a class of information. In the next few paragraphs, we explain how location data, and the class of data holders, could be described in a designation.
21. The location data covered by the designation made under Part IVD of the CCA will need to be very clearly defined in detail and should include at a minimum the different types of location data that is able to be collected by an OS provider, such as the information specified in Table 1 of this submission.
22. Google (and other service providers) may collect more location data than is strictly required to provide a particular service. For example, Google Maps is able to provide a more accurate and convenient service if it is able to use the location data of an individual while that individual is using Google Maps. However, Google may continue to collect location data from an individual even when that individual is not using Google Maps, that is, in circumstances where the app has no need to collect or store that location data. To avoid regulated entities raising arguments that only the location data collected from individuals which is directly used to provide a consumer facing service should be subject to CDR, the definition must clearly include *all* of the location data collected by a regulated data holder, irrespective of why that data was collected.
23. The designated class of information should not include any information that is *inferred* from location data. As mentioned previously, a great deal of information may be inferred about an individual by tracking their location – where they work, live and many other habits and interests. Applying CDR to such inferred data may stifle future developments whether in artificial intelligence (**AI**) or other areas which seek to transform location data into powerful inferences which can benefit society economically or socially.
24. Although, under Part IVD of the CCA, the class of consumers that may potentially be able to request the transfer of location data is large (including both individuals and entities), it is recommended that in this case the class is restricted to individuals only, given that location data is most relevant to individuals.
25. Location data is collected via smart devices on a continuous, real time basis. Although value is obtained from collecting that data over a long period (including to make inferences, as indicated above), it is particularly valuable when used on a real time basis – for example, to target advertising when a consumer is near a particular retail outlet or to provide information on traffic conditions as consumers travel in vehicles. As this is the case, the designated information should be *real time* location data.
26. The framework established by Part IVD of the CCA requires that businesses in a sector to which CDR applies must not only make consumer data available, as we have discussed in this submission, but must also make information on designated products publicly available. This is intended to facilitate comparisons being made between similar products offered by different providers, allowing informed choices by consumers. There is a diverse range of consumer facing products that are provided by the entities that collect location data (and other types of digital data). The rationale for the application of CDR to location data is not to facilitate comparisons between these existing consumer facing products, but to promote innovation and the provision of new products, as well as competition in associated markets such as in the

adtech sector. Therefore, in the application of CDR to location data, it would not be necessary to specify in the designation instrument particular products.

27. The designation instrument could provide that, initially, the persons that currently hold the designated information (the data holders) would be OS providers, that is, primarily Google (in relation to the Android OS) and Apple (for iOS). Providers of any app that collects location data and associates it with an individual or an account of an individual (i.e., where the data is not collected solely on an anonymised basis) that meet a particular threshold limit could be included on a delayed basis. For example, at a later time, data holders could be extended to include operators of apps with 500,000 or more Australian subscribers (or another appropriate number that does not place undue burden on small businesses or start ups). This would be a similar approach to that adopted for the application of the CDR in open banking, where a phased approach is being adopted, with the 4 major domestic Australian banks being subject to the regime at any earlier point than smaller banks.
28. As a second stage, the CDR could at a future point in time potentially be applied to a broader category of digital personal information that is collected from Australian consumers through their use of digital services, provided that broader category was carefully scoped and clearly defined.

The importance of location data for targeted advertising

Location data collected by service providers such as Google is of great value in delivering targeted online advertising.

29. Taking Google as an example, it is easy to demonstrate the importance of location data for targeted online advertising. Google's ability to collect location data allows Google to claim in its marketing materials to advertisers that it can determine with a "99% certainty" whether a consumer to whom an ad has been displayed subsequently visits a brick-and-mortar store.⁷ Google's store visits conversions are based on matching consumers' Android or iOS location history with "*the exact dimensions of over 200 million stores globally.*"⁸
30. So, for example, after displaying an ad for Nike football shoes, Google is able to verify the effectiveness of the ad by confirming that a consumer checked out the shoes online on his or her mobile device, then walked to a specific shopping mall, that he or she went to the fifth floor of that shopping mall and that he or she visited the Nike store located on that fifth floor. This information allows the advertiser – in this case Nike – to determine whether its ad campaign was successful. As Google itself says, its adtech services allow marketers to "*close the loop between online ads and offline sales.*"⁹
31. Location data, of itself, is also important to advertisers for another reason. Location data enables advertisers to target ads to users in a specific location irrespective of any other characteristics of those users. For example, advertising may be targeted to consumers in a particular country, region, radius around a specific location or near specific business addresses, irrespective of the other characteristics of the individuals.¹⁰ Therefore location

⁷ <https://www.blog.google/products/ads/new-digital-innovations-to-close-the-loop-for-advertisers>

⁸ <https://www.blog.google/products/ads/new-digital-innovations-to-close-the-loop-for-advertisers>

⁹ <https://adwords.googleblog.com/2016/09/New-Digital-Innovations-to-Close-the-Loop-for-Advertisers.html>.

¹⁰ See for example as advertised by Google: https://ads.google.com/intl/en_us/home/how-it-works/: Here it states: "For your ad to perform well, it has to find the right audience. Google Ads lets you choose the location where your ad will appear, including within a certain radius of your store or covering entire regions and countries."

data is very valuable, even where it cannot be combined with other types of personal information in relation to an individual consumer.

32. The importance of location data is also demonstrated by statements Google makes to advertisers regarding this type of data. For example, Google states in the information that it provides to advertisers:

About targeting geographic locations

Target your ads to people in—or who've shown interest in—geographic locations relevant to where you do business. You can select whether you'd like your ad to appear for someone's physical location, locations of interest, or both. Location targeting can help you make sure your ads are relevant to the people who see them—which can help boost your campaign's value.¹¹

33. The importance of all types of digital personal information, not only location data, has recently been recognised by both the Government and the ACCC in the context of the proposed mandatory code of conduct to address bargaining power imbalances between digital platforms and media companies.¹² One of the issues that the mandatory code will address is the provision to media companies of information which the digital platforms have collected in connection with consumers accessing the content of the relevant media company. Media companies and the platforms have not been able to reach agreement on this issue (amongst others), indicating that this information has a significant value in the context of targeted advertising.

The benefits of providing consumers with greater control over their location data and the ability to fairly harvest the value of their location data

Consumers may provide their location data to Google at less than the fair value of that location data because of market failure. The CDR may assist in addressing this market failure.

Market failure: lack of information and bargaining imbalance

34. It is of course true that digital platforms and other service providers that collect location data provide a wide range of digital services to consumers at zero monetary cost in exchange for those consumers providing their location data.
35. Numerous questions arise in this context. First, do consumers actually understand that this is the deal they have made with such service providers and do they truly understand how much information service providers such as Google collect? Are the “free” digital services really adequate compensation for the data that consumers provide? Is the consent a consumer provides to the collection of their location data truly “free” consent?
36. In the Final Report from the Digital Platforms Inquiry, the ACCC concluded that there may exist a market failure. In the ACCC’s view, consumers, in agreeing to provide their location data to digital platforms in return for the provision of services, may not be making informed choices. There is a bargaining power imbalance between the platforms and consumers (i.e., so consumers feel they have no choice but to agree to the data collection), there is a significant

¹¹ <https://support.google.com/google-ads/answer/2453995?hl=en>

¹² <https://ministers.treasury.gov.au/ministers/josh-frydenberg-2018/media-releases/accc-mandatory-code-conduct-govern-commercial>

information asymmetry between the platforms and consumers and consumers also have difficulties in assessing the value of their data once it is in the hands of the platforms.

37. Not only do consumers have difficulty in assessing the costs of providing their information (both in the case of digital platforms and to other providers of digital services) but they have difficulty in assessing the *value* of that information. As a consequence, the ACCC concluded consumers will be better off when they are sufficiently informed and have sufficient control over their user data, so that they actually can make informed choices that align with their privacy and data collection preferences. Applying the CDR to location data, and potentially to other carefully defined categories of digital personal information at a later stage will assist in addressing this market failure.

Significant benefits from initially applying the CDR to location data

38. As is made clear in the Final Report from the ACCC's Digital Platforms Inquiry, one of the most concerning types of data collection from the perspective of Australian consumers is the collection of location data. The ACCC's consumer survey indicated that an overwhelming percentage of Australians who use digital platforms considered the monitoring of offline location and movement without the user's consent to be a misuse of their data.¹³ Implementing the CDR to location data has additional benefits for consumers as it will mean that a key area of concern for most consumers in relation to the collection of digital personal information is addressed quickly.
39. Google has been tracking the physical location of consumers for approximately 15 years, since it first started tracking IP addresses.¹⁴ Notwithstanding the concerns of Australian consumers, at the current time, location data continues to be collected by Google in accordance with its privacy policy, with Australians having only a limited ability to control that location data collection and, in a practical sense, no control over how that location data is used once it is collected. The privacy policies of many apps also allow for broad rights to collect location data (even if such location data is not required for the efficient use of the relevant app).
40. Location data has significant value. Therefore applying the CDR to location data is likely to provide the most immediate benefits to consumers to be able to fairly harvest the value of their digital personal information. Other businesses may be willing to provide consideration that particular consumers value highly, for example, the exchange of location data for a free or subsidised data plan may be one example of what others would be willing to offer consumers for their location data.

Inability to address identified issues through changes to the Privacy Act

41. The ACCC expressed the view in the Final Report from the Digital Platforms Inquiry that Australia's existing regulatory framework for the collection, use and disclosure of user data and personal information, that is, the Privacy Act 1988 (Cth) (**Privacy Act**), does not effectively deter certain data practices that exploit the information asymmetries and bargaining power imbalances between digital platforms and consumers. We agree this is correct and, even when the amendments that the Government has announced it proposes to make to the Privacy Act are implemented, the issues the ACCC has identified will not be fully addressed. This is because the Privacy Act provides only limited rights to Australians; it does not for example allow directions to be given by consumers to those business that collect their location data and other digital personal information and does not address the bargaining power imbalances between consumers and those businesses. Applying the CDR to location data, and in future potentially other types of digital personal information, provides the opportunity to address all of the issues that were identified by the ACCC. To enable this to

¹³ 86% of this category of Australians hold this view, see page 385 of the Final Report.

¹⁴ Final Report, see Table 7.2 on page 380.

occur, the regulatory changes that we have discussed in this submission will also need to be addressed.

Designation of location data would be privacy enhancing

42. Designating location data, and potentially other digital personal information in future, will enhance the privacy protections that Australians have.
43. If location data is designated, it will only be able to be transferred in the manner permitted by the CDR framework. In addition, location data may only be transferred to accredited persons, who must hold the data (and data derived by the relevant accredited person from it) in accordance with the privacy safeguards in Part IVD of the CCA and any additional privacy requirements of the consumer data rules made by the ACCC. The imposition of such additional privacy requirements, together with the monitoring that the ACCC is empowered to carry out, will assist in ensuring that the accredited entities can be trusted to protect the location data that is provided under the CDR.
44. Due to the time-sensitive nature of location data, it likely will be necessary to address the timeliness of the data transfers requested by consumers in the ACCC's consumer data rules. Those rules should operate to prevent a situation where location data transferred by Google (or any other data holder) to an accredited entity was delayed in a manner that gave a competitive advantage to Google due to its control over and proximity to the valuable data stream.
45. A Data Standards Body assists the Data Standards Chair in making data standards for the CDR. The data standards prescribe the format and process by which CDR data is to be shared with consumers and accredited data recipients within the CDR system and therefore is able to be designed to ensure that security and privacy are protected.
46. Clearly, these requirements will significantly enhance the privacy protections for Australians, as compared to the current situation. At the current time:
 - (a) Location data may be transferred by any person that collects it, provided that where the person collecting the location data is bound by the Privacy Act, its privacy policy permits this. There is no requirement that the transfer occurs in a particular way and therefore no requirement that the protections the Data Standards Body and Chair would require for the transfer of CDR data are applied.
 - (b) There is currently no requirement under Australian law that any third party recipient has any accreditation of any sort.
 - (c) A consumer has no say in how a third party recipient may deal with the data, provided that (if the recipient is in fact subject to the Privacy Act) such use complies with that third party's privacy policy, over which the Australian consumer has no control.

Summary of benefits

47. From the perspective of a consumer, applying the CDR to location data has the beneficial outcomes set out below, which are able to be achieved within a framework that will enhance consumer privacy protections:
 - (a) Providing for the CDR to apply to location data will improve transparency and limit the information asymmetry between OS providers, digital platforms (and other relevant service providers) and consumers, as these providers will be required to disclose to consumers exactly the location data that is collected, to allow each consumer to make a decision as to whether she requires that location data to be transferred to the consumer herself or to other parties. Consumers will in this way also know who receives their highly sensitive location data.

- (b) Giving consumers the right to require their location data to be shared under the CDR will go some way towards addressing the power imbalance between digital platforms (and other relevant service providers), particularly dominant service providers such as Google, and consumers. As we have suggested in this submission, to properly address this issue regulatory change should be implemented to allow consumers to elect for location data to be *transferred*, rather than shared. That is, a consumer should be able to require that a data holder does not retain the location data that is transferred to a third party (or to the consumer herself). Only in that way would a consumer truly be in control of her location data.
- (c) This will also enable the question of the value of location data to be determined. Google and other digital service providers argue that the services they provide in exchange for location data (and the collection of many other types of digital personal information) they collect from consumers is fair consideration for that data. It is simply impossible to determine whether or not that is true because there is no competitively efficient market for any form of digital personal information that Google and other service providers collect, given the information asymmetries and imbalance in bargaining power discussed above. If consumers had the right to provide their location data to third parties, then a competitively efficient market would come into existence and consumers would be able to better assess the value of that information and fairly harvest the value of that information.

Additional competition, including innovation, benefits of applying the CDR to location data

- 48. Applying the CDR to location data will improve efficiency in relevant markets and foster both competition and innovation. This inevitably will assist consumers and the economy as a whole.
- 49. The market for the “sale” of the location data of Australian consumers is not efficient for the reasons outlined earlier in this submission. As consumers do not receive clear information on when their location data is collected or who is collecting or receiving it, do not have visibility on how that location data is used (including by third parties to whom the location data may be transferred after it is initially collected), have little choice as to whether to agree to provide their information if they wish to use a particular digital service and, in reality, cannot require any person that collects that location data to provide it to the consumer¹⁵, then that market is not efficient. Making this market more transparent and increasing the bargaining power of consumers, by providing a greater degree of control to consumers over who may receive their location data, and requiring third parties to compete for the right to receive it, will improve efficiency.
- 50. Applying the CDR to location data will also assist in facilitating the conditions for competition, and therefore have an efficiency dividend, in the adtech services sector. As mentioned previously, the location data that is collected from consumers is important in the delivery of adtech services. At the current time, neither Google, nor other digital service providers, voluntarily transfers any of this information and consumers cannot require them to do this.
- 51. In its Final Report from the Digital Platforms Inquiry the ACCC made the important point that data portability may have the effect of helping rival firms to Google in the adtech market overcome the competitive disadvantage that they have because of Google’s overwhelming

¹⁵ As explained in Oracle’s submissions to the Digital Platforms Inquiry (including its submission to the Preliminary Report, see here: <https://www.accc.gov.au/system/files/Oracle%20Corporation%20%28March%202019%29.PDF>) Google provides access to *some* location and other data that Google collects from consumers but not *all* of that data.

volume of consumer data.¹⁶ This is likely to make the adtech services market more competitive and more efficient, as prices should be reduced for adtech services that rely on location data. Alternative adtech services providers may also be able to provide greater value to publishers, including traditional media companies, which will of course provide benefits to those publishers. Those benefits will have the potential to assist in reversing, at least to some extent, the under-provision of news and journalism that has been highlighted in the Final Report, which will have broader societal benefits.

52. Adtech services providers, and others, are likely to also be able to use valuable location data for the development of innovative products and services for Australians. Of course, it is impossible to specify what all of those innovations may be in this submission. One example of where there would be benefit from increased access (strictly in accordance with the regime provided for in Part IVD of the CCA) is likely to be in the area of AI. AI relies on the provision of high quality data, such as would potentially be available if the CDR was applied to location data.
53. The other innovative uses of location data (and other digital personal information, if ultimately the CDR was to be applied to such other data) will only become apparent when this data is actually available – but, again, there is significant potential for this to be the catalyst for innovation and therefore economic growth. In the current COVID-19 pandemic for example, there would be clear benefit if consumers actually already had the right to direct real-time streams and require the transfer of, at least, their historical location data. If this could be required, the Government’s job of infection tracking would be made considerably easier.
54. Arguments may be raised that applying the CDR to location data may chill competition, as competitors in the adtech services market and other digital markets will cease to provide competitive products that would allow them to directly collect location data from consumers as they will instead rely on the potential to obtain this information under the CDR. However, such an argument should not be accepted. Demand for location data is high because it is so valuable in the adtech services market (and in future may have a value in other markets too). Google’s ability to collect location data arises from its dominance in certain markets, including the market for licensable OS on mobile devices, where it has ownership of Android OS, and in consumer facing markets, such as Google Maps. In the short to medium term it cannot be expected that other service providers would be able to compete to provide alternative services in each of these areas where Google is dominant – for example, to develop an alternative licensable mobile operating system that was widely adopted would take a significant amount of both time and capital. However, given the value of location data, there is no doubt that there are many companies that would actively compete, via the provision of innovative products and services, for consumers to agree to provide that information to them.
55. Although applying the CDR to location data will be a very important step in promoting competition in the Australian economy, this will not be a complete answer to the competition problems that currently exist in the Australian adtech services market and, indeed, exist globally in that market. Oracle’s submission to the ACCC’s Adtech Inquiry addresses the broader regulatory action that the ACCC should take – that action should be taken in addition to applying the CDR to location data and potentially other types of digital personal information in future.

¹⁶ Final Report, see page 115.

Necessary regulatory change

56. To maximise the effectiveness of the implementation of the CDR to location data (and potentially other types of digital personal information in future) it is necessary to make a number of regulatory changes, which are outlined in this section of Oracle's submission.

Changes to Part IVD of the Competition and Consumer Act

Transfer, not sharing, of location data

57. Consumers should have the right to require Google and other digital service providers that are subject to the CDR to transfer the location data of the relevant consumer, rather than simply share that data. This is, in a practical sense, a specific application of the recommendation made by the ACCC in the Final Report from the Digital Platforms Inquiry that individuals have the right to require erasure of the personal information held about them. That is, an individual would be provided with the option to require the original data holder to erase information that is either transferred directly to the individual or transferred to a third party under CDR.
58. The ACCC recommended a right of erasure on the basis that it would provide consumers greater control over their personal information and that it would be likely to help mitigate the bargaining imbalance between consumers and digital platforms.¹⁷
59. Although the Government, in its response to the Digital Platforms Inquiry, stated that the right to erasure would be considered as part of the proposed longer term reform of the Privacy Act, the Government qualified this on the basis that consideration would need to be given to potential freedom of speech concerns, challenges to law enforcement and national security investigations where personal information was erased before an investigation was completed and the practical difficulties that could arise from imposing this obligation.
60. None of the reservations that the Government expressed in relation to a broad right of erasure would apply in relation to the specific application of the right of erasure in this case, given that location data is not of a type of information that would raise freedom of speech concerns, the data would not be deleted entirely (as the transferee would still have it) and there would be unlikely to be difficulties in imposing a deletion requirement on the transferred information, which would need to be specifically identified to be transferred and therefore could easily be erased.

Geographical limitations

61. Geographical limitations are imposed on information that may be designated under section 56AC(2) of the CCA. In so far as is relevant here, information will only be included in a designated class if it:
- (a) has at any time been generated or collected wholly or partly in Australia (or the external Territories) and relates to one or more Australian persons (other than the persons who so generated or collected it); or
 - (b) has only ever been generated and collected outside Australia and the external Territories and has been so generated or collected by or on behalf of one or more Australian persons *and* either relates to one or more Australian persons (other than the persons who so generated or collected it) or relates to goods or services supplied, or offered for supply, to one or more Australian persons.
 - (c) "Australian person" is defined in section 56AO(5) of the CCA to include a body corporate established under an Australian law, an Australian citizen or permanent

¹⁷ See page 471 of the Final Report.

resident, or a person who is ordinarily resident within Australia (or an external Territory) or a Government entity.

62. The application of these geographical limitations would appear to mean that location data collected from the devices of Australian persons outside Australia (and the external Territories) by a person who is not an Australian person would not be designated information.
63. This type of geographical limitation makes little sense in relation to location data. In fact it would be likely to make it more difficult, rather than less, for those entities falling within the data holder category to determine what data would need to be transferred if this geographical limitation was retained as, where the data holder is not an Australian person, it would need to distinguish between data collected from an Australian person when that person was in Australia and data collected when that person was not in Australia, which is a distinction such entities would generally be unlikely to make. Therefore, for the purposes of the application of the CDR to location data, the only requirement should be that the information is collected *from* an Australian person. Of course, in any event, if the CDR regime was also adopted in other jurisdictions, at least in its application to location data, then the question of geographical restriction would be less relevant.

Changes to the Privacy Act

“Personal information” under the Privacy Act

64. Recommendation 16(a) in the ACCC’s Final Report was that the definition of “personal information” in the Privacy Act should be clarified to ensure that it captures technical data such as IP addresses, device identifiers, location data and other online identifiers that may be used to identify an individual. In the Government’s response it was stated that consultation would occur on that proposal, provided that any amendments made do not impose an unreasonable regulatory burden on industry.
65. Oracle’s view is that such data, including in particular location data, where it is able to be directly associated with an identified individual or an individual who is reasonably identifiable, will already fall within the definition of personal information. Nonetheless, if CDR is applied in the manner that we have outlined in this submission, it would be important to expressly include all location data as personal information under the Privacy Act to ensure that the Privacy Act, like the CDR legislation, recognises that location data should receive the highest levels of protection under Australian law.

Rights to object to collection and disclosure of personal information

66. Recommendation 16(c) in the ACCC’s Final Report was that the Privacy Act should be amended to strengthen consent requirements and pro-consumer defaults, including to require that consent to personal information collection is “freely given”, that is, that the provision of services or goods must not be conditional on consent being provided to the collection and processing of personal information that is not necessary for the provision of those services/goods. As in the case of recommendation 16(a), the Government response was that it supports this recommendation in principle. The Government qualified this by stating that this would be in the context of ensuring that the requirements did not impose a significant regulatory burden and did not add to individuals suffering from “consent fatigue”.
67. An examination of this recommendation is particularly important in the context of the application of the CDR to location data. Location data, and other types of personal information is collected by digital services providers for two reasons. The first is for the purpose of using that information to provide a particular digital service that has been directly requested by the relevant consumer. The second is to use that data for other reasons related to the business of the digital service provider, particularly the delivery of targeted advertising.

68. To ensure that the CDR, when applied to location data, provides the intended benefits to individuals (and without limiting the rights of individuals to require that data is transferred rather than shared, as outlined previously), individuals should have the right to:
- (a) restrict the purpose for which location data is used to the purpose of providing the relevant service; and
 - (b) object to location data being collected and then used or transferred to third parties for purposes other than providing the relevant service.
69. Tied to the above, an individual should have a legally enforceable right to be able to continue to use the relevant digital service in the event that she does not agree that location data could be used other than for the purpose of provision of that service. If this, more limited, alternative to recommendation 16(c) was adopted, this would address the concerns that were identified in the ACCC's Final Report whilst at the same time ensuring that an unreasonable regulatory burden is not imposed economy wide and limiting the likelihood of "consent fatigue". This requirement should be supported by a digital platform specific code, as discussed immediately below.

Privacy code for digital platforms

70. The ACCC recommended that an enforceable code of practice be developed specifically for digital platforms (Recommendation 18). Although other types of digital service providers collect location data and other types of personal information, digital platforms, particularly Google, collect more of this information from consumers than anyone else. Therefore it is appropriate that such a code applies only to digital platforms. A code would be important in the context of the application of the CDR to location data, particularly in relation to consent requirements and opt-out controls. The Government's response to this recommendation was to agree that legislation to provide for such a code would be introduced in 2020.
71. The code should be required to address the following:
- (a) The consent requirements of the code should reinforce that consumers must opt-in for any data collection and use, including location data collection and use, that is for a purpose other than the purpose of supplying the relevant consumer-facing services (with such services to exclude targeted advertising). The code should also state that digital platforms may not refuse to provide services where this opt-in consent is not provided.
 - (b) Reinforcing subparagraph (a) above, as recommended by the ACCC, the code should require that digital platforms give consumers the ability to select global opt-outs or opt-ins, such as with regard to the sharing of personal information, including location data, with third parties for targeted advertising. Again, the code should make clear that digital platforms may not refuse to provide services where this opt-in consent is not provided.

Potential for international coordination

72. Although the application of the CDR in the manner that we have suggested in this submission will have significant benefits for Australians, and the Australian economy, there are also benefits in working with other jurisdictions to ensure that a consistent approach is adopted.
73. The UK's Competition & Markets Authority (**CMA**) in late 2019 released its Interim Report from its Online Platforms and Digital Advertising Market Study. Appendix L of that Interim Report considered two different proposals for improving personal data mobility, the first of which would be similar to the application of CDR to digital personal information, at least where such information is collected by digital platforms, in the manner outlined in this

submission. The view of the CMA was that adopting one or both of the proposals could help better protect privacy whilst increasing competition and ensuring that consumers are able to benefit to a greater extent from the value of their data. We agree this is achievable, but recommend that the UK approach more closely align with that of the CDR approach outlined in this submission.

74. There would be benefits in engagement with the CMA to enable both The Treasury and the CMA to consider whether it would be possible to develop a consistent regime. Ultimately, the adoption of a consistent regime across multiple jurisdictions will assist in reducing the costs of the digital service providers that are subject to the CDR. However that consultation should not delay the adoption of these important reforms in Australia.

Thank you very much for considering this submission. Oracle would be very pleased to discuss any aspects of the submission with The Treasury if requested.

Oracle Corporation

10 June 2020

Attachment B: Oracle presentation Adtech Essentials Digital Demand and Supply



ADTECH ESSENTIALS

Digital Demand and Supply



AdTech created a media wholesale market





• Agenda •

- Professional media buying
- What's at stake when buyers use adtech
- Very brief Buying Platforms 101
- How adtech enables advertisers to accomplish their goals
 1. Target
 2. Bid
 3. Measure
 4. Attribute
 5. Interoperate



PROFESSIONAL MEDIA BUYING



Illustrative example: digital advertising for Axe Body Spray

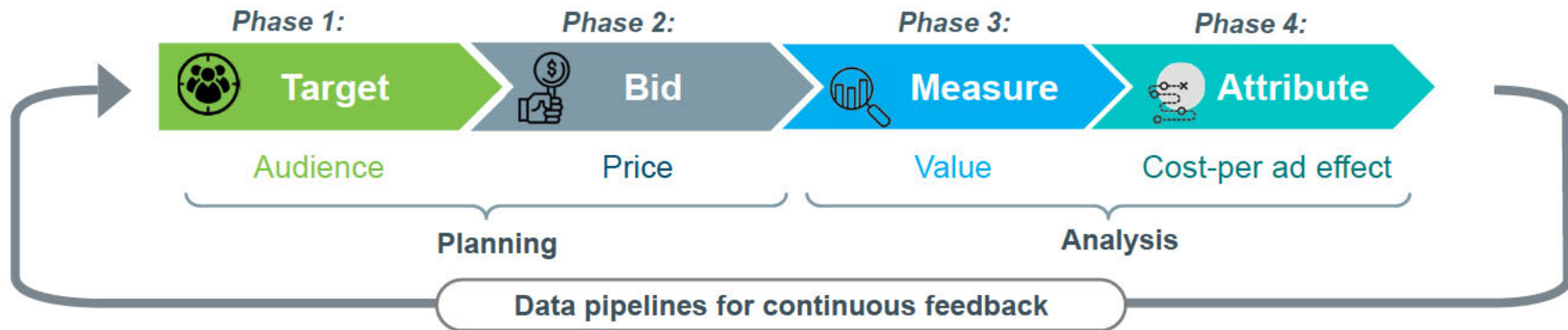


The funnel implies inefficiency that needn't exist in digital

	<u>Example Event</u>	<u>User Yield Count</u>
AWARENESS	User saw an Axe body spray video ad on CBS	100,000
INTEREST	User saw and clicked on an Axe ad on ESPN.com	50,000
CONSIDERATION	User researched Axe and compared to other brands	30,000
INTENT	User visited the Axe website	20,000
TRIAL	User redeemed an Axe coupon for a free sample	5,000
PURCHASE	User purchased an Axe product	500

- By **tracking return on investment (ROI)** and **making data-driven decisions about every transaction**, digital marketers can persuade and grow without wasting money
- Investors demand reports on cost to acquire vs. lifetime value

Efficient digital advertising requires a continuous feedback loop



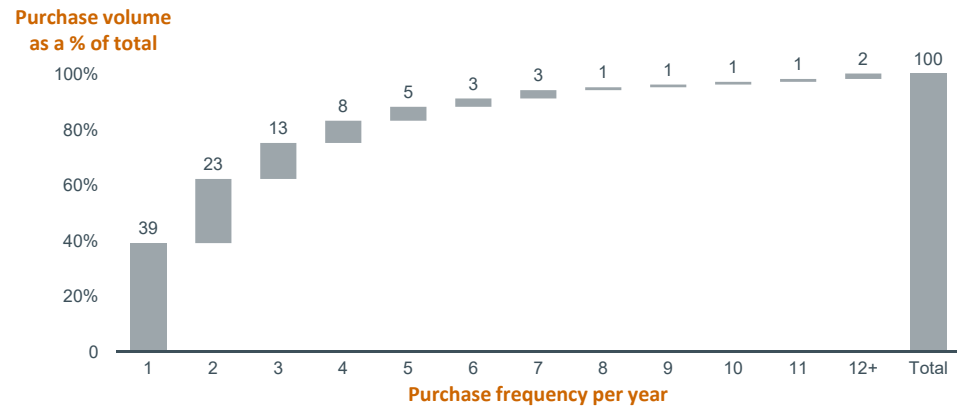
- Imagine buying a used car using tools that calculate total cost of ownership. The friction of needing a mechanic would be relieved
- Adtech provides similar value for advertisers, automatically at scale
- Efficient ad buy decisions require that this feedback loop apply consistently to all ad transactions
- Advertisers are more likely to make inefficient decisions if information is unavailable at any phase



WHAT'S AT STAKE WHEN BUYERS USE ADTECH

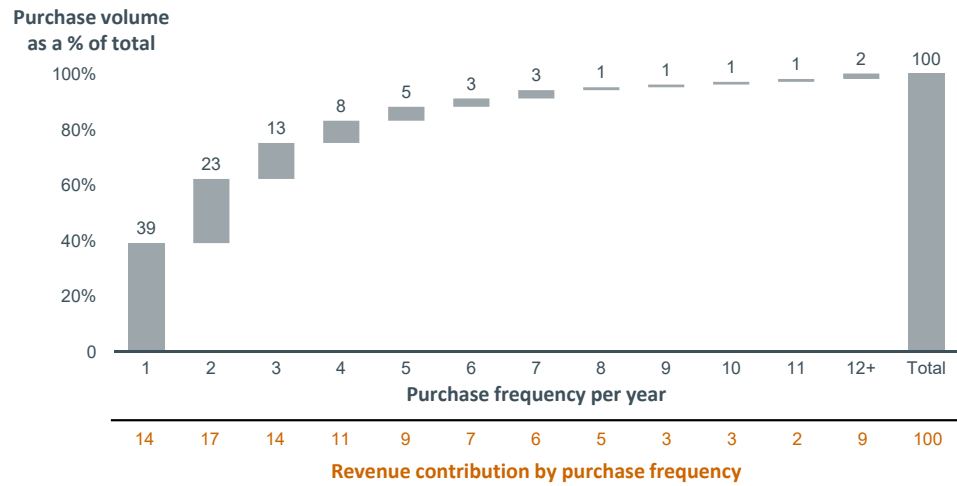


Always consider competing data options



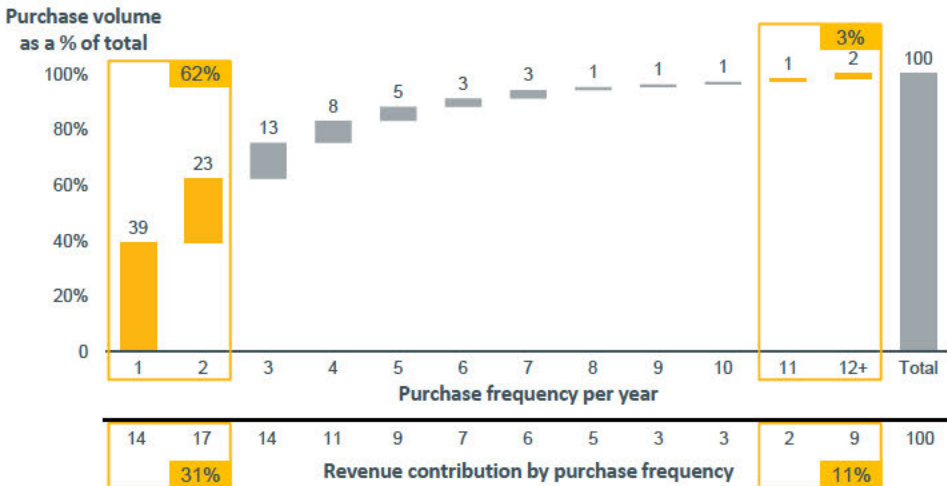
Example: Who should we target?

Always consider competing data options



Example: Who should we target?

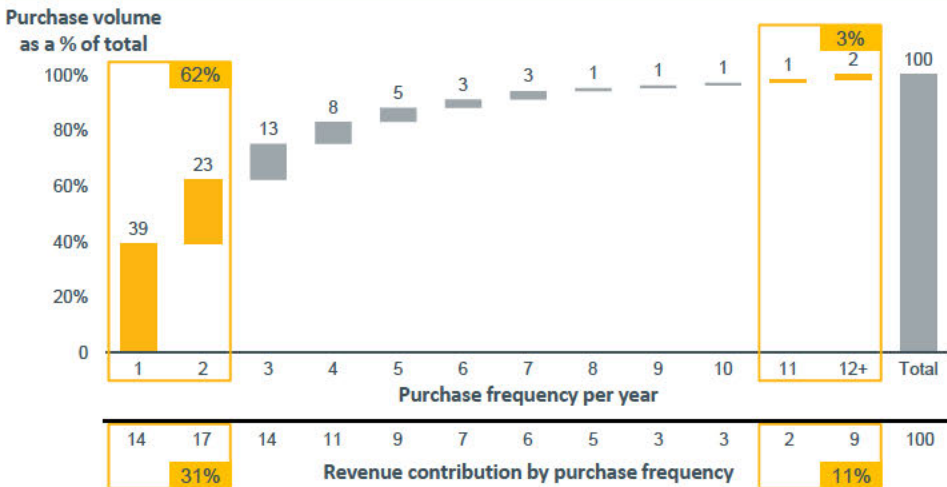
Always consider competing data options



Example: Who should we target?

- Among the Axe customer base:
 - 3% of the customer base buys 11+ times a year. They contribute 11% of the total revenue.
 - 62% of the customer base buys only 1-2 times a year, and they contribute ~1/3 of the total revenue

Always consider competing data options



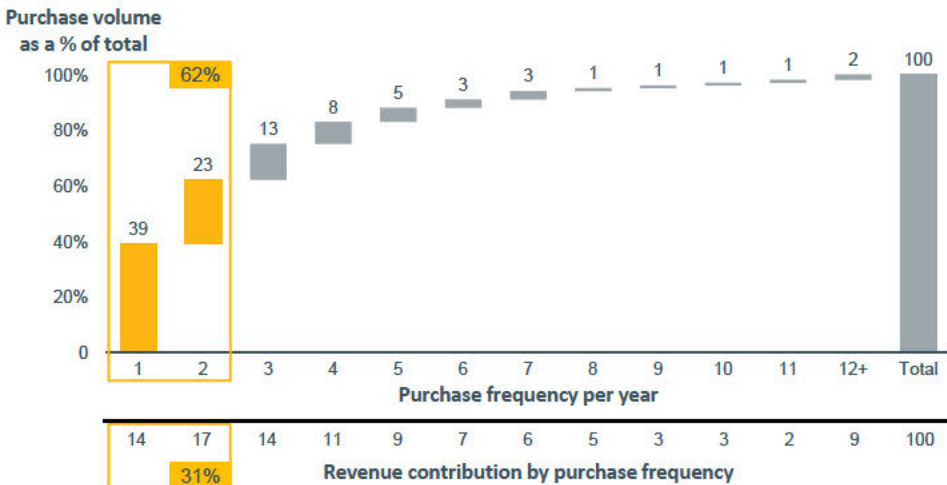
Infrequent but critical customers.
Axe has very little data on this customer group

Loyal customers. Axe has a lot of 1st party customer data

Example: Who should we target?

- Among the Axe customer base:
 - 3% of the customer base buys 11+ times a year. They contribute 11% of the total revenue.
 - 62% of the customer base buys only 1-2 times a year, and they contribute ~1/3 of the total revenue
- A typically tough targeting decision is whether to send ads to the people you've been able to collect data on (the small, loyal audience to the right of the chart) or to purchase data to target people who've purchased your product infrequently or never

Always consider competing data options

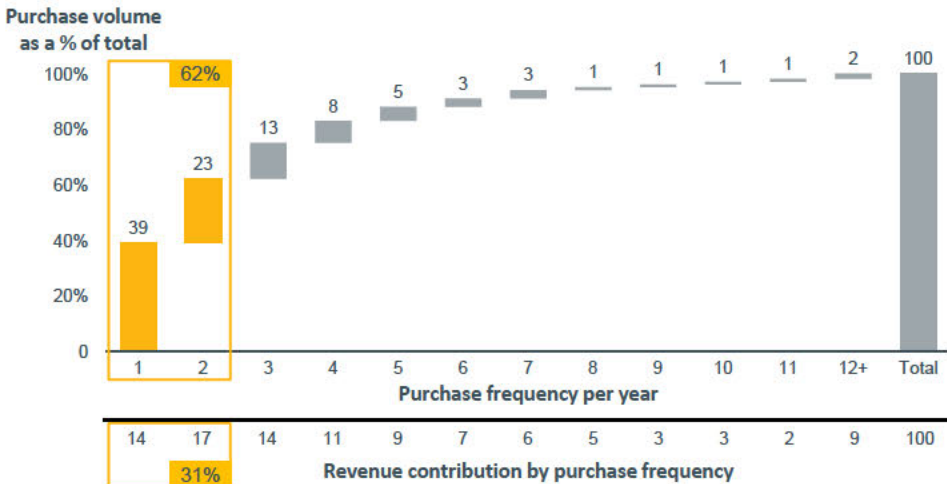


Infrequent but critical customers.
Axe has very little data on this customer group

Example: Who should we target?

- Among the Axe customer base:
 - 3% of the customer base buys 11+ times a year. They contribute 11% of the total revenue.
 - 62% of the customer base buys only 1-2 times a year, and they contribute ~1/3 of the total revenue
- A typically tough targeting decision is whether to send ads to the people you've been able to collect data on (the small, loyal audience to the right of the chart) or to purchase data to target people who've purchased your product infrequently or never
- It's impossible to know in advance if buying data will be justified by the "lift" the data drives. **That's one reason why feedback is so important**

Always consider competing data options



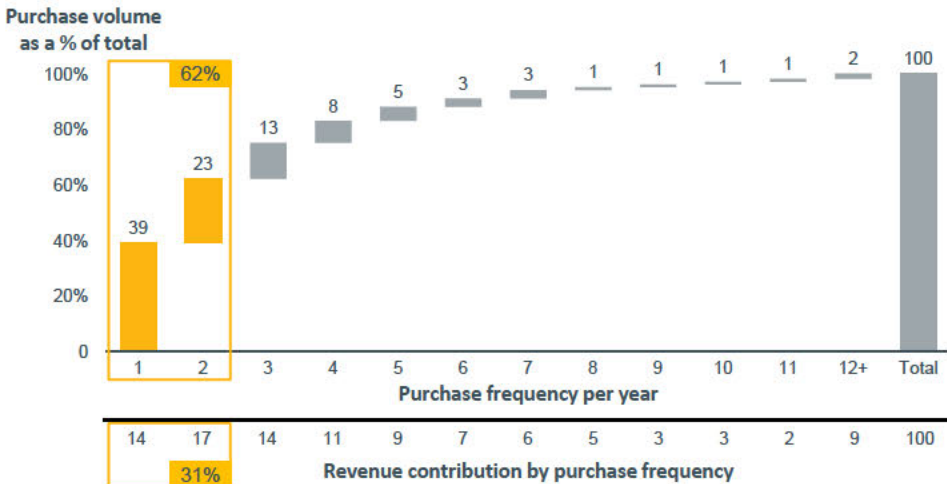
Infrequent but critical customers.
Axe has very little data on this customer group

Tactic	Conversion Rate Lift
No data	0
Neustar audience	75%
BlueKai audience	75%
Acxiom audience	150%

Example: Who should we target?

- Among the Axe customer base:
 - 3% of the customer base buys 11+ times a year. They contribute 11% of the total revenue.
 - 62% of the customer base buys only 1-2 times a year, and they contribute ~1/3 of the total revenue
- A typically tough targeting decision is whether to send ads to the people you've been able to collect data on (the small, loyal audience to the right of the chart) or to purchase data to target people who've purchased your product infrequently or never
- It's impossible to know in advance if buying data will be justified by the "lift" the data drives. **That's one reason why feedback is so important**

Always consider competing data options



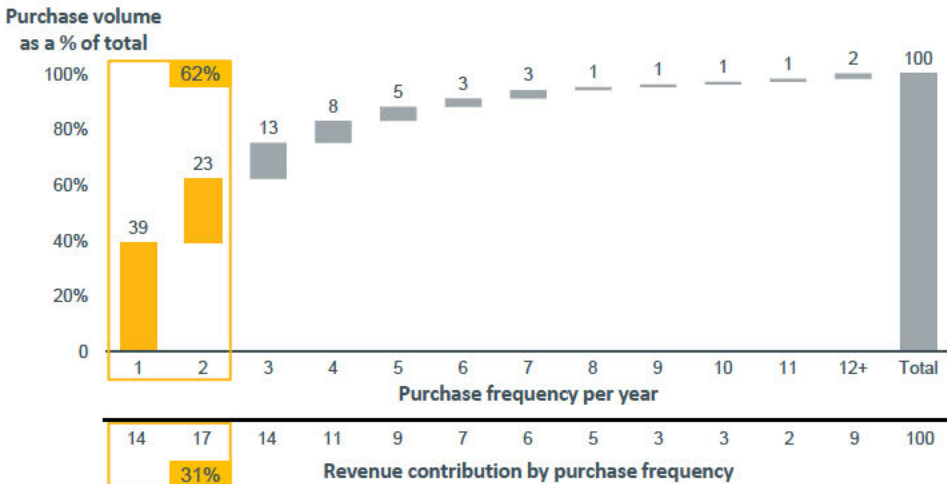
Infrequent but critical customers.
Axe has very little data on this customer group

Tactic	Conversion		Data Cost	Total Cost
	Rate Lift	Media Cost		
No data	0	\$4.00	\$0.00	\$4.00
Neustar audience	75%	\$4.00	\$1.25	\$5.25
BlueKai audience	75%	\$4.00	10%	\$4.40
Acxiom audience	150%	\$4.00	\$2.00	\$6.00

Example: Who should we target?

- Among the Axe customer base:
 - 3% of the customer base buys 11+ times a year. They contribute 11% of the total revenue.
 - 62% of the customer base buys only 1-2 times a year, and they contribute ~1/3 of the total revenue
- A typically tough targeting decision is whether to send ads to the people you've been able to collect data on (the small, loyal audience to the right of the chart) or to purchase data to target people who've purchased your product infrequently or never
- It's impossible to know in advance if buying data will be justified by the "lift" the data drives. **That's one reason why feedback is so important**

Always consider competing data options



Infrequent but critical customers.
Axe has very little data on this customer group

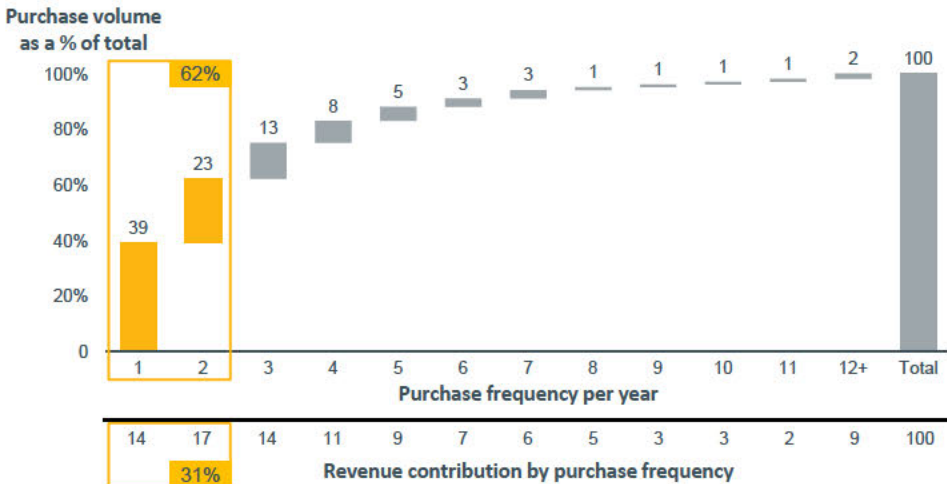
Example: Who should we target?

- Among the Axe customer base:
 - 3% of the customer base buys 11+ times a year. They contribute 11% of the total revenue.
 - 62% of the customer base buys only 1-2 times a year, and they contribute ~1/3 of the total revenue
- A typically tough targeting decision is whether to send ads to the people you've been able to collect data on (the small, loyal audience to the right of the chart) or to purchase data to target people who've purchased your product infrequently or never
- It's impossible to know in advance if buying data will be justified by the "lift" the data drives. **That's one reason why feedback is so important**

Tactic	Conversion		Data Cost	Total Cost	Lifetime Value
	Rate	Lift			
No data	0		\$0.00	\$4.00	\$15.00
Neustar audience	75%		\$1.25	\$5.25	\$15.00
BlueKai audience	75%		10%	\$4.40	\$17.00
Acxiom audience	150%		\$2.00	\$6.00	\$13.00

Sources: 1. "How Brands Grow" by Byron Sharp. 2. Advertiser data.

Always consider competing data options



Infrequent but critical customers.
Axe has very little data on this customer group

Example: Who should we target?

- Among the Axe customer base:
 - 3% of the customer base buys 11+ times a year. They contribute 11% of the total revenue.
 - 62% of the customer base buys only 1-2 times a year, and they contribute ~1/3 of the total revenue
- A typically tough targeting decision is whether to send ads to the people you've been able to collect data on (the small, loyal audience to the right of the chart) or to purchase data to target people who've purchased your product infrequently or never
- It's impossible to know in advance if buying data will be justified by the "lift" the data drives. That's one reason why feedback is so important
- Data costs vary. Data cost can only be justified by efficiency gains

Tactic	Conversion Rate Lift	Media Cost	Data Cost	Total Cost	Lifetime Value	Return per dollar invested
No data	0	\$4.00	\$0.00	\$4.00	\$15.00	\$1.50
Neustar audience	75%	\$4.00	\$1.25	\$5.25	\$15.00	\$1.05
BlueKai audience	75%	\$4.00	10%	\$4.40	\$17.00	\$2.16
Acxiom audience	150%	\$4.00	\$2.00	\$6.00	\$13.00	\$0.87

Sources: 1. "How Brands Grow" by Byron Sharp. 2. Advertiser data.

The price you bid is never the actual cost

Publisher Site Categories	On-Target Rate	Media Price
A	60%	\$8.00

The price you bid is never the actual cost

Publisher Site Categories	On-Target Rate	Media Price
A	60%	\$8.00

On-target cost = $\$8 \div 60\% = \13.33

Young men on NCAA site

- For example, Axe is targeting 18-25 years old men online
- One option is placing ads on Site A (e.g., NCAA.com), where 60% of the visitors are 18-25 years old men (i.e. a 60% on-target rate)

The price you bid is never the actual cost

Publisher Site		Media Price						
Categories	On-Target Rate	\$2.00	\$3.00	\$4.00	\$5.00	\$6.00	\$7.00	\$8.00
A	60%							
B	50%							
C	40%							
D	30%							
E	20%							

The price you bid is never the actual cost

Publisher Site Categories	On-Target Rate	Media Price						
		\$2.00	\$3.00	\$4.00	\$5.00	\$6.00	\$7.00	\$8.00
A	60%							\$13.33
B	50%					\$12.00	\$14.00	\$16.00
C	40%			\$10.00	\$12.50	\$15.00	\$17.50	\$20.00
D	30%	\$6.67	\$10.00	\$13.33	\$16.67	\$20.00	\$23.33	\$26.67
E	20%	\$10.00	\$15.00	\$20.00	\$25.00	\$30.00	\$35.00	\$40.00

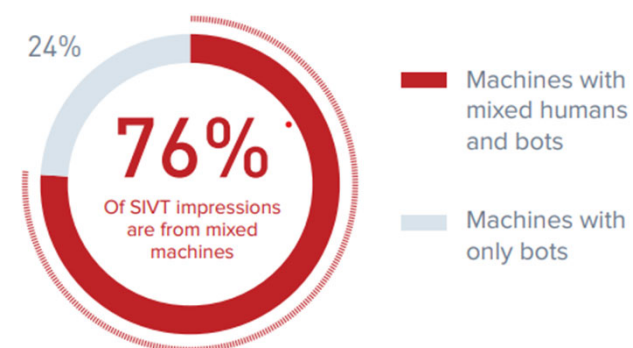
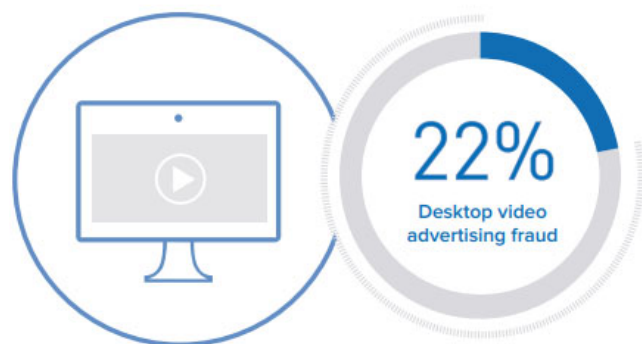
The price you bid is never the actual cost

Publisher Site Categories	On-Target Rate	Media Price							
		\$2.00	\$3.00	\$4.00	\$5.00	\$6.00	\$7.00	\$8.00	
A	60%							\$13.33	Young men on NCAA site
B	50%					\$12.00	\$14.00	\$16.00	
C	40%			\$10.00	\$12.50	\$15.00	\$17.50	\$20.00	
D	30%	\$6.67	\$10.00	\$13.33	\$16.67	\$20.00	\$23.33	\$26.67	
E	20%	\$10.00	\$15.00	\$20.00	\$25.00	\$30.00	\$35.00	\$40.00	

Young men on online poker site

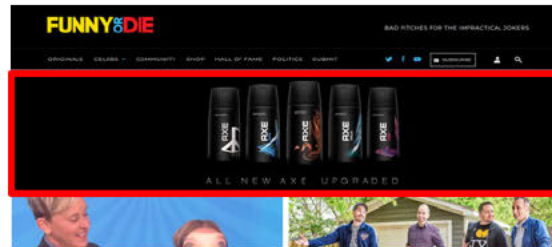
- When at least two factors vary significantly – in this example, price and on-target rate – the worst adjusted cost can be an order of magnitude higher than the best
- In this example, the best on-target cost is \$6.67 CPM (Site D, 30% on-target rate, \$2.00 media price). Bidding \$8 to achieve a 60% on-target rate may seem to make sense without feedback, but in fact doubles the on-target cost
- Advertisers lose billions of dollars when data on what advertisers value isn't available where and when advertisers bid

Ad Fraud is a threat that requires vigilance



- Demand for digital video exceeds supply, creating an opportunity for fraudsters to exploit the marketplace
- Ad fraud costs advertisers in the US ~\$9B annually and growing
- SIVT stands for “Sophisticated Invalid Traffic.” It’s usually caused by malware on a human-operated device. Video might run behind the browser or in a player too small to see.

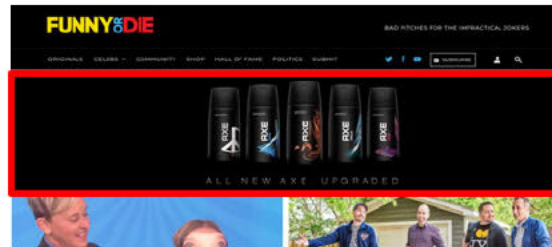
Fraud example: Effective cost of a homepage banner ad



Homepage banner campaign

Cost	\$100
# of impressions	10,000
CPM	\$10

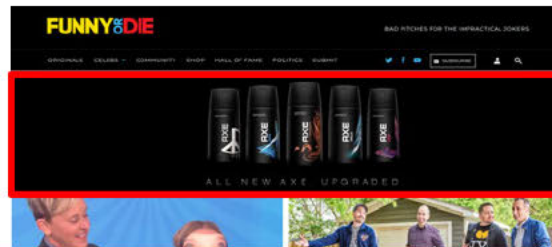
Fraud example: Effective cost of a homepage banner ad



Homepage banner campaign

Cost	\$100
# of impressions	10,000
CPM	\$10
Viewable rate	60%
# of viewable impressions	6,000

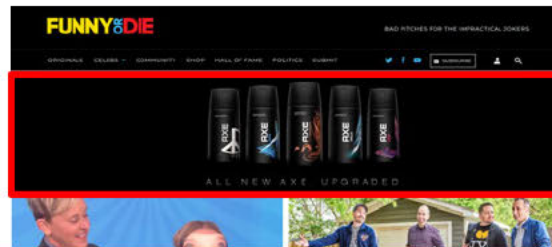
Fraud example: Effective cost of a homepage banner ad



Homepage banner campaign

Cost	\$100
# of impressions	10,000
CPM	\$10
Viewable rate	60%
# of viewable impressions	6,000
Non-fraud rate	70%
# of viewable, non-fraud impressions	4,200

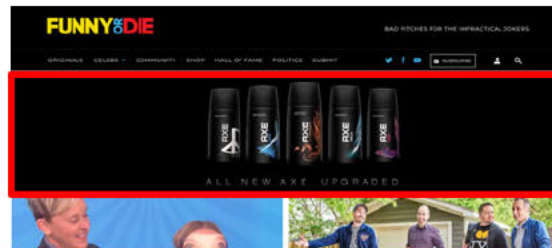
Fraud example: Effective cost of a homepage banner ad



Homepage banner campaign

Cost	\$100
# of impressions	10,000
CPM	\$10
Viewable rate	60%
# of viewable impressions	6,000
Non-fraud rate	70%
# of viewable, non-fraud impressions	4,200
Brand-safe environment rate	80%
# of verified (viewable, non-fraud, brand-safe) impressions	3,360

Fraud example: Effective cost of a homepage banner ad

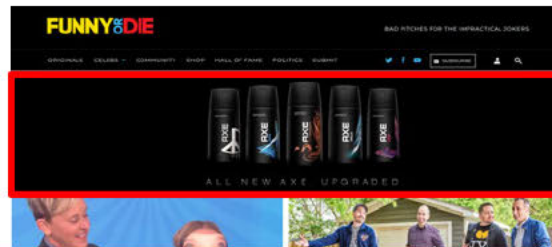


Homepage banner campaign

Cost	\$100
# of impressions	10,000
CPM	\$10
Viewable rate	60%
# of viewable impressions	6,000
Non-fraud rate	70%
# of viewable, non-fraud impressions	4,200
Brand-safe environment rate	80%
# of verified (viewable, non-fraud, brand-safe) impressions	3,360

Measured by 3rd party vendors

Fraud example: Effective cost of a homepage banner ad

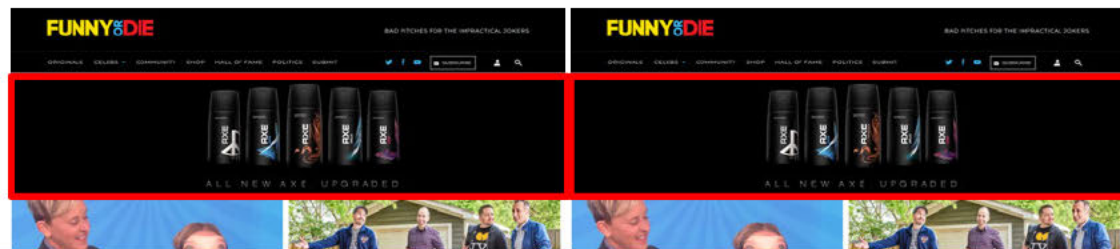


Homepage banner campaign

Cost	\$100
# of impressions	10,000
CPM	\$10
Viewable rate	60%
# of viewable impressions	6,000
Non-fraud rate	70%
# of viewable, non-fraud impressions	4,200
Brand-safe environment rate	80%
# of verified (viewable, non-fraud, brand-safe) impressions	3,360
Quality-adjusted CPM (qCPM) (cost per thousand verified impressions)	\$30 ($\$100 / 3360$) x 1000

Measured by 3rd party vendors

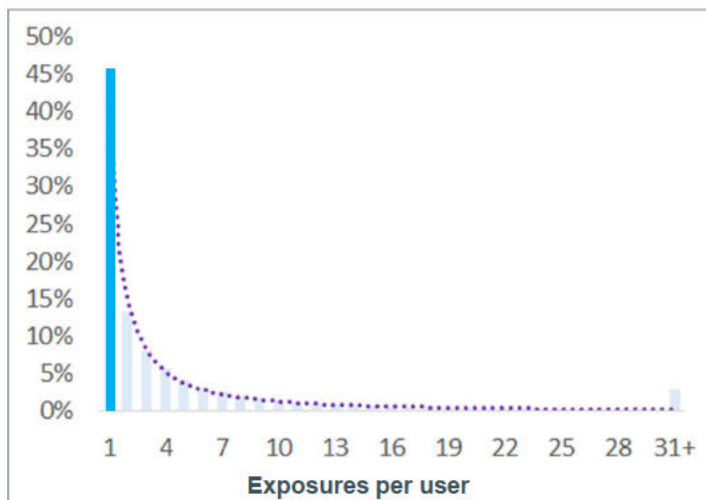
Fraud example: Effective cost of a homepage banner ad



	Homepage banner campaign	Same campaign, fraud problem detected
Cost	\$100	\$100
# of IMPRESSIONS	10,000	10,000
CPM	\$10	\$10
Viewable rate	60%	60%
# of viewable impressions	6,000	6,000
Non-fraud rate	70%	10%
# of viewable, non-fraud impressions	4,200	600
Brand-safe environment rate	80%	80%
# of verified (viewable, non-fraud, brand-safe) impressions	3,360	480
Quality-adjusted CPM (qCPM) (cost per thousand verified impressions)	\$30 $(\$100 / 3360) \times 1000$	\$210 $(\$100 / 480) \times 1000$

Question the method for assigning sales credit to ads

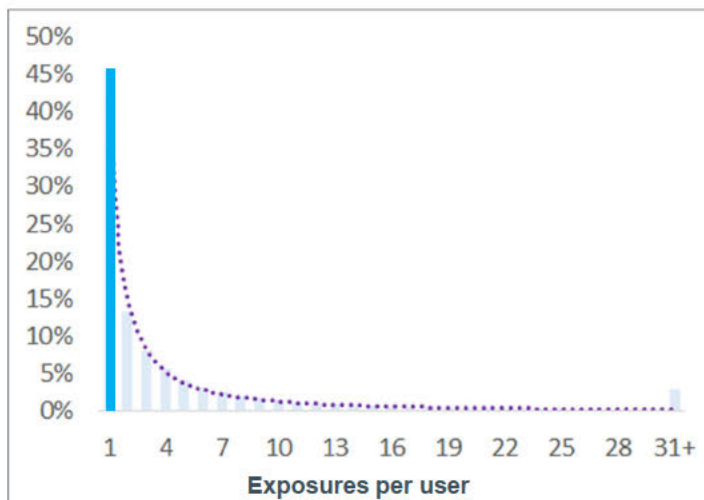
Ad frequency distribution



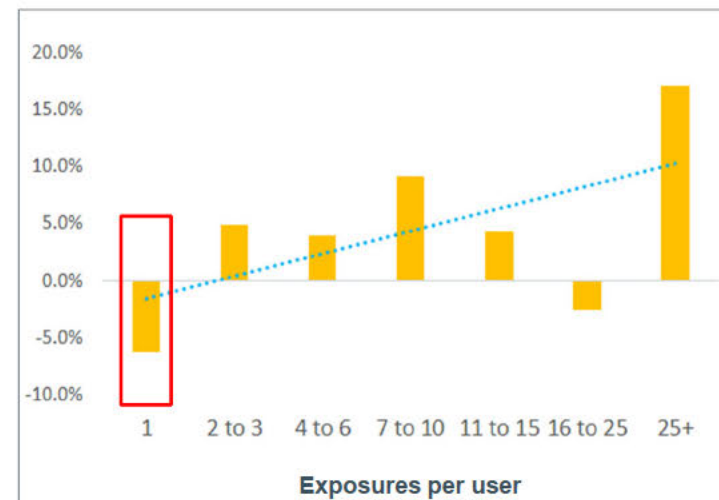
- Axe body spray is a well-known consumer brand that expects sales even without ad campaigns
- Axe ran display advertising using Google for 12 months. Google reported very high return on ad investment
- Deeper analysis revealed that 45% of Axe's audience reached online saw only one ad
- Axe wondered if they'd been gamed by Google

Question the method for assigning sales credit to ads

Ad frequency distribution



Conversion lift % over control



- Axe body spray is a well-known consumer brand that expects sales even without ad campaigns
- Axe ran display advertising using Google for 12 months. Google reported very high return on ad investment
- Deeper analysis revealed that 45% of Axe's audience reached online saw only one ad
- Axe wondered if they'd been gamed by Google

- Suspicious, Axe conducted a controlled experiment. It proved a single ad exposure does not affect conversion at all
- Half of Axe's reach was ineffective
- If anyone but Google controlled attribution, the appearance of extreme efficiency in single-exposure display (and search) would trigger alerts



VERY BRIEF BUYING PLATFORMS 101



Advertiser ad servers first brought spend and return for all ad transactions together (1995)



- Advertiser ad servers were developed in response to advertisers' demand for seamless auditing and measurement of campaigns
- The Advertiser Ad Server was advertisers' first virtual monitor in the marketplace, observing and sending details on transactions advertisers agreed to, but could not personally witness. Inside the advertiser ad server console, advertisers track planned spend and observed returns together
- Leveraging advertiser ad servers, advertisers improved direct deals with publishers. A direct deal guarantees advertisers pre-determined ad placement (i.e. all banners on Yahoo Finance Jan 1-31) at a pre-determined price (e.g., \$15 per thousand impressions)
- Feedback from ad servers quantified the effectiveness of every placement (ad slot) in a package. To optimize deals, advertisers bargained to cut the worst placements and increase presence on the best. In early days, publishers couldn't see the data driving these decisions

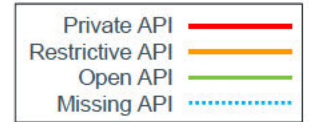
Auctions using the OpenRTB standard eliminated the friction of manual renegotiations (2010)



- Advertisers demanded dynamic pricing to leverage their analytics and improve ROI quickly across many sites at once
- The tech marketplace needed to also satisfy publisher demand for maximum competition among advertiser, and data on what each advertiser was willing to pay
- The solution was OpenRTB (open real time bidding): by standardizing display auctions (bid request-and-response protocol), it leveled advertisers' access to supply and publishers' access to demand
- Advertisers and publishers agreed to transact at the impression level. All auction participants see the closing cost

Note: Though the vision of OpenRTB was to eventually encompass the entire ad marketplace, direct deals persist today

The messaging system of OpenRTB is a set of APIs



ADVERTISER WEBSITE

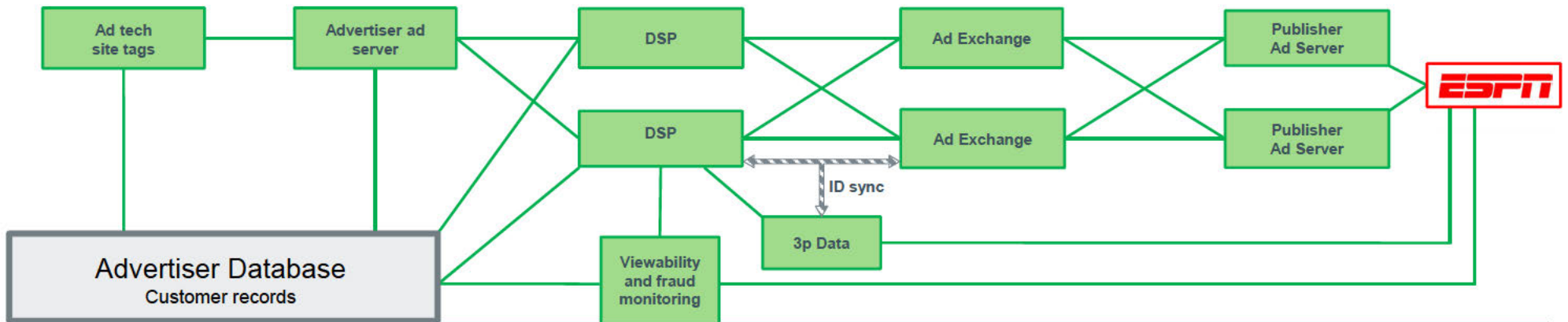
CONVERSION TRACKING

BIDDING

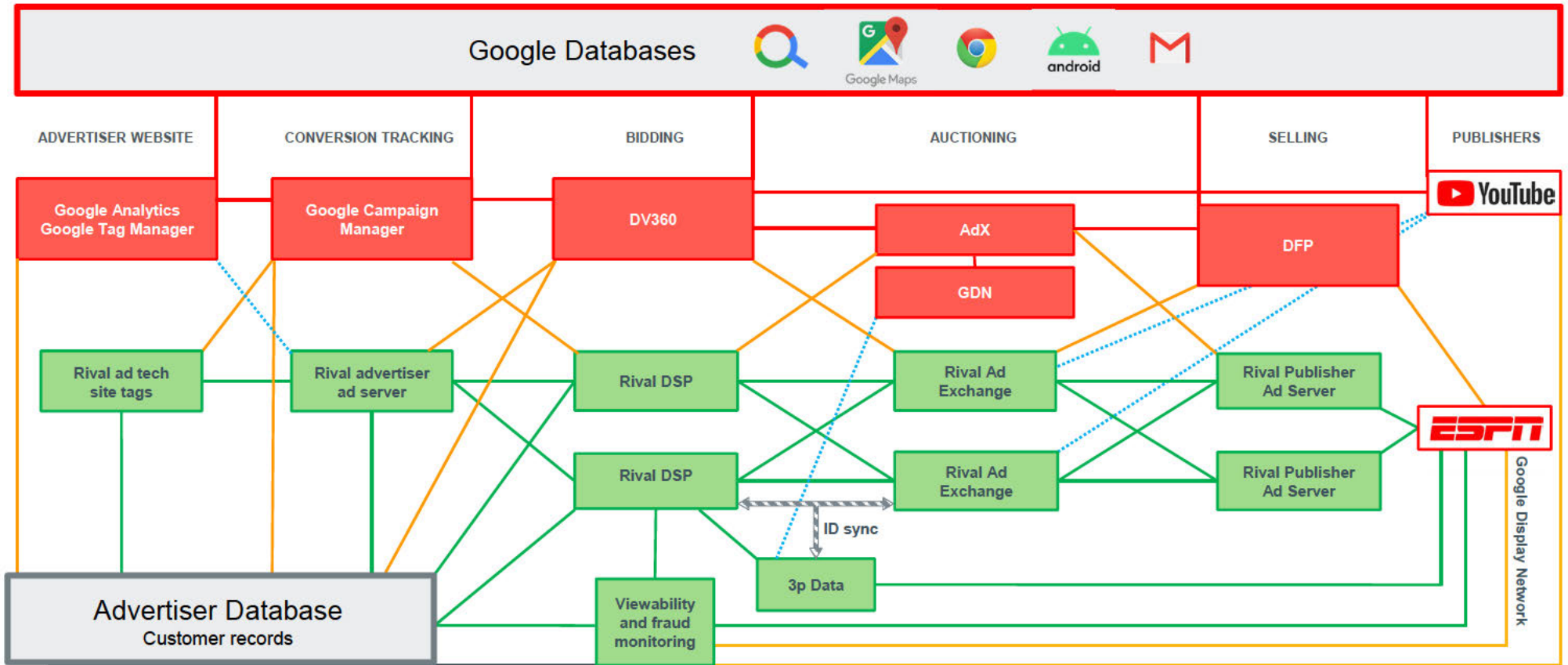
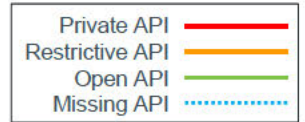
AUCTIONING

SELLING

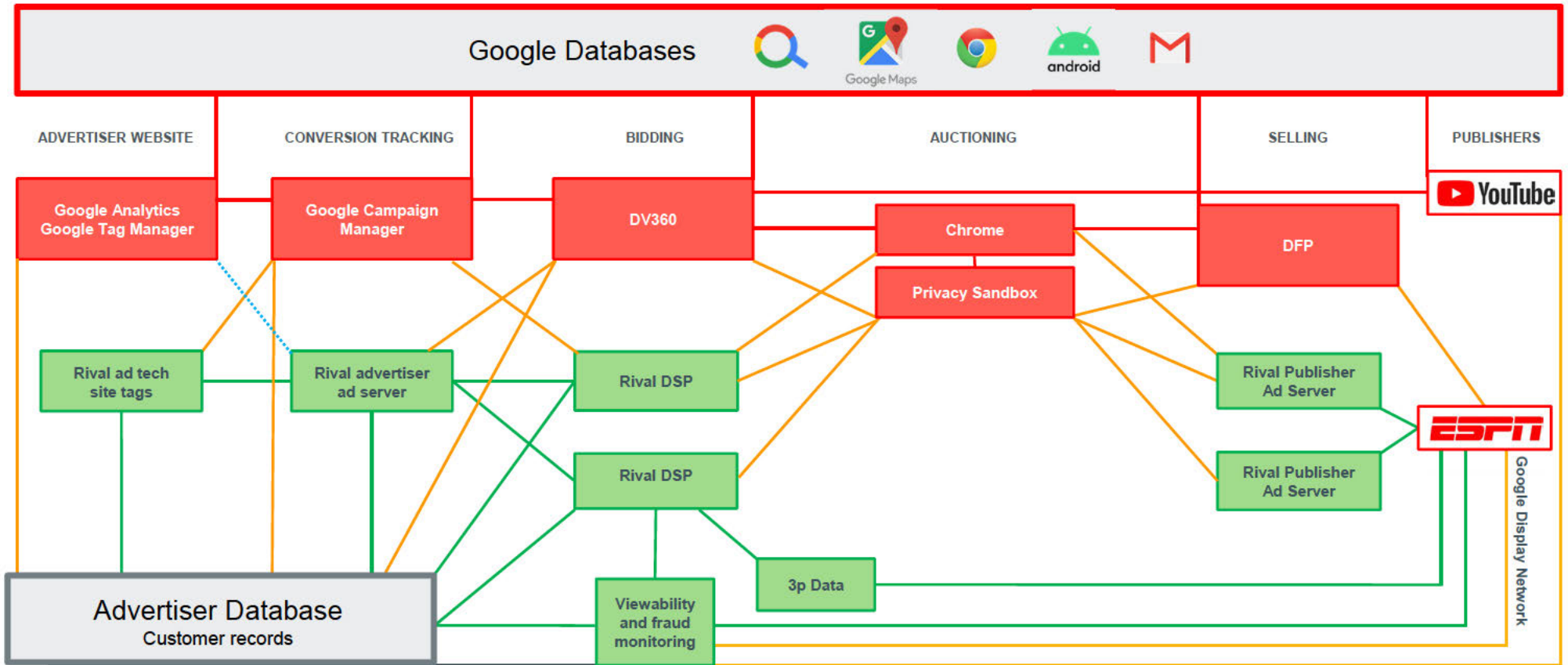
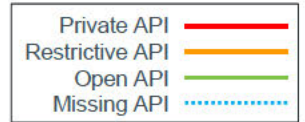
PUBLISHERS



Google took steps to replace open APIs with private APIs, sometimes closing off access completely

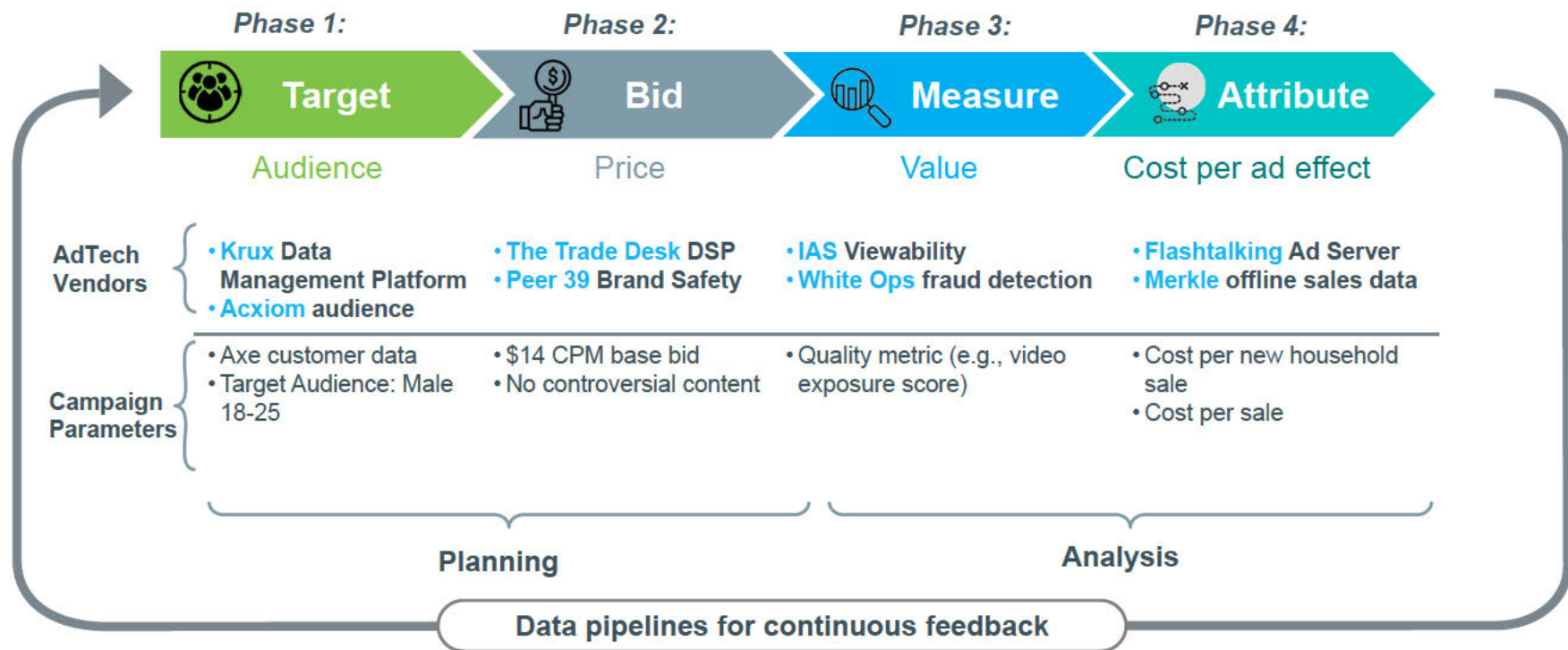


2022 forecast, based on Chrome announcements



A continuous feedback requires extensive data “plumbing”

Example: An Axe body spray digital ad campaign

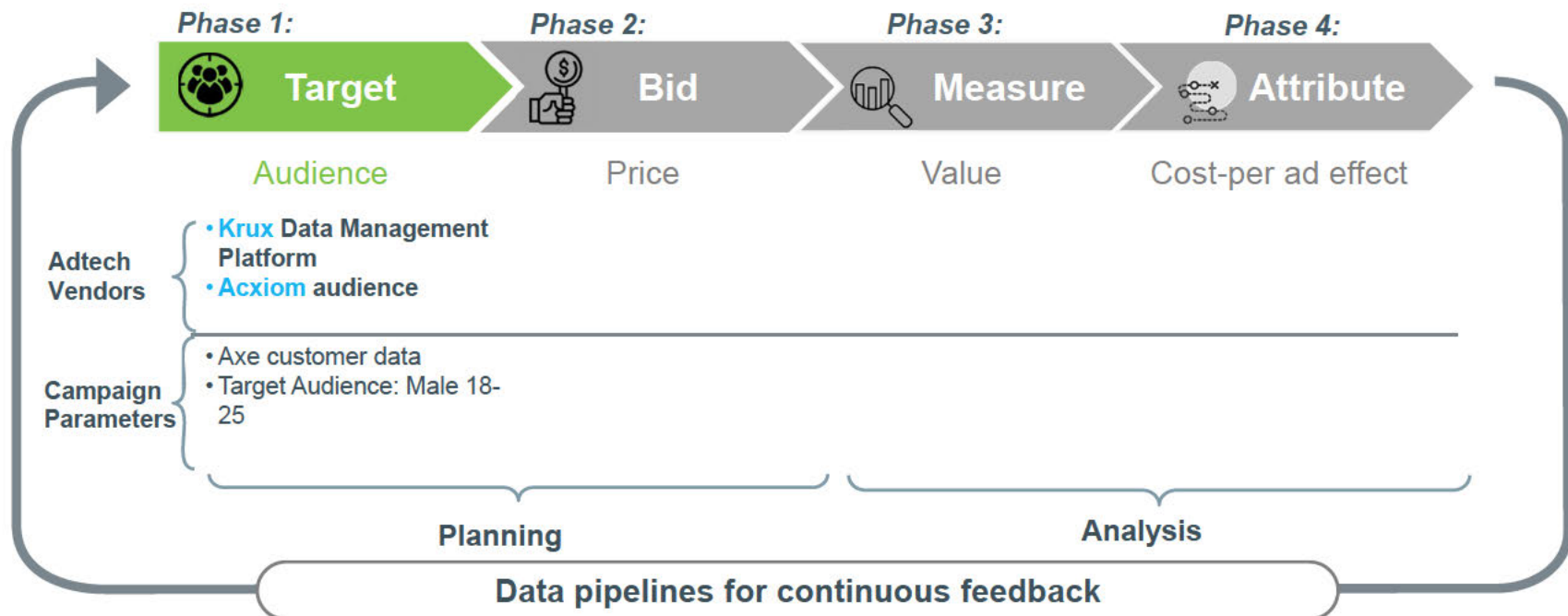




HOW ADTECH ENABLES
ADVERTISERS TO ACCOMPLISH
THEIR GOALS

Phase 1: Target Audiences

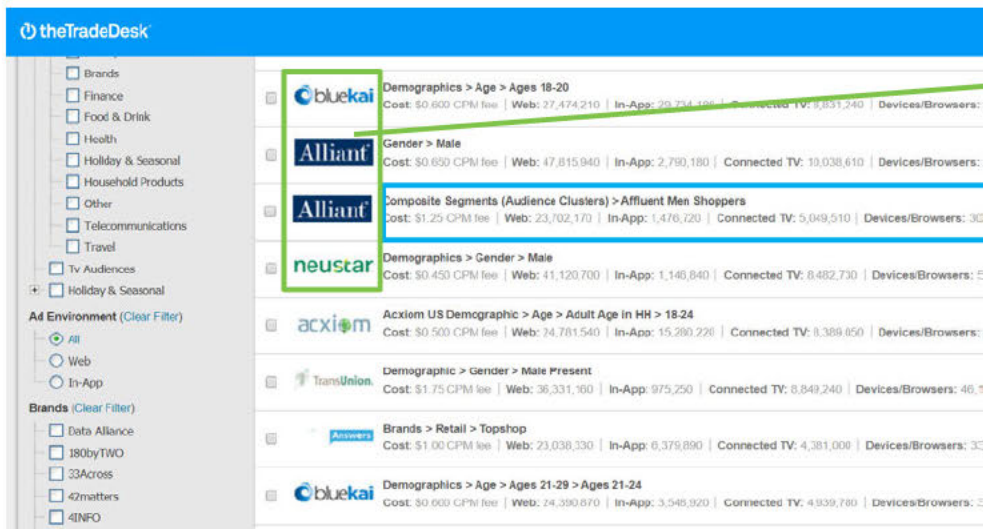
Example: An Axe body spray digital ad campaign



Advertisers want a wide selection of audience segment providers in a competitive marketplace, and data from a variety of sources to enhance owned data

Advertisers select target audiences from an open marketplace of competing providers

Example:  theTradeDesk® (DSP)



theTradeDesk









- Brands
- Finance
- Food & Drink
- Health
- Holiday & Seasonal
- Household Products
- Other
- Telecommunications
- Travel
- Tv Audiences
- Holiday & Seasonal

Ad Environment (Clear Filter)

- All
- Web
- In-App

Brands (Clear Filter)

- Data Alliance
- 180byTWO
- 33Across
- 42matters
- 4INFO

	Demographics > Age > Ages 18-20 Cost: \$0.600 CPM fee Web: 27,474,210 In-App: 20,754,166 Connected TV: 9,831,240 Devices/Browsers: 33
	Gender > Male Cost: \$0.650 CPM fee Web: 47,815,940 In-App: 2,790,180 Connected TV: 13,038,610 Devices/Browsers: 33
	Composite Segments (Audience Clusters) > Affluent Men Shoppers Cost: \$1.25 CPM fee Web: 23,702,170 In-App: 1,476,720 Connected TV: 5,049,510 Devices/Browsers: 33
	Demographics > Gender > Male Cost: \$0.450 CPM fee Web: 41,120,700 In-App: 1,146,840 Connected TV: 8,482,730 Devices/Browsers: 33
	Acxiom US Demographic > Age > Adult Age in HH > 18-24 Cost: \$0.500 CPM fee Web: 24,781,540 In-App: 15,280,226 Connected TV: 8,389,650 Devices/Browsers: 33
	Demographic > Gender > Male Present Cost: \$1.75 CPM fee Web: 36,331,160 In-App: 975,250 Connected TV: 8,849,240 Devices/Browsers: 46,1
	Brands > Retail > Topshop Cost: \$1.00 CPM fee Web: 23,038,330 In-App: 6,379,890 Connected TV: 4,381,000 Devices/Browsers: 33
	Demographics > Age > Ages 21-29 > Ages 21-24 Cost: \$0.600 CPM fee Web: 24,390,670 In-App: 3,546,920 Connected TV: 4,939,780 Devices/Browsers: 33

 bluekai

 Alliant®

 neustar.

- Audience segment: Affluent Men Shoppers
- Cost: \$1.25 CPM fee
- Size (Web): 23,702,170
- Size (In-App): 1,476,720
- Size (Connected TV): 5,049,510

- Advertisers want to target consumers who are most likely to generate a return – the best performing audience
- Advertisers want to choose their desired audience segment from a variety of providers
- Independent data providers compete with each other on price – audience fees are transparent and easy to compare

Advertisers enhance their own data with an array of additional data sources

Example:  theTradeDesk® (DSP)

Core Audience
How do you want to power your plan? Koa™ will analyze the actions of users in your audience elements to inform Planner's recommendations.

First-Party Insights

First Party Insights Type
Imported 1st Party Data ✕ ▾

Audience Elements

1P | Modeled Segment | hairstyle tips sign-ups

1P | Modeled Segment | newsletter sign-ups

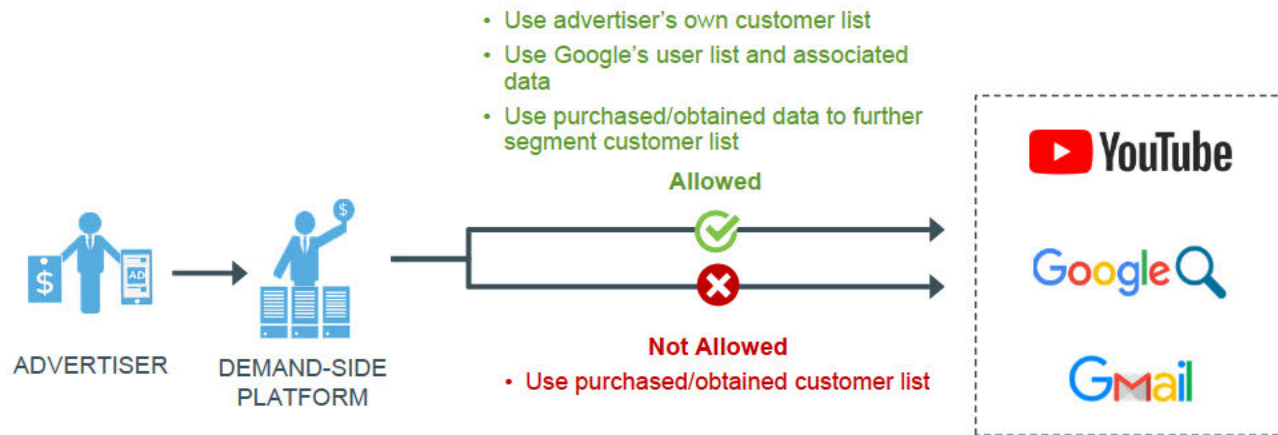
look ✕ ▾

1,143,000 Aggregate Unique Users

Data Sources:



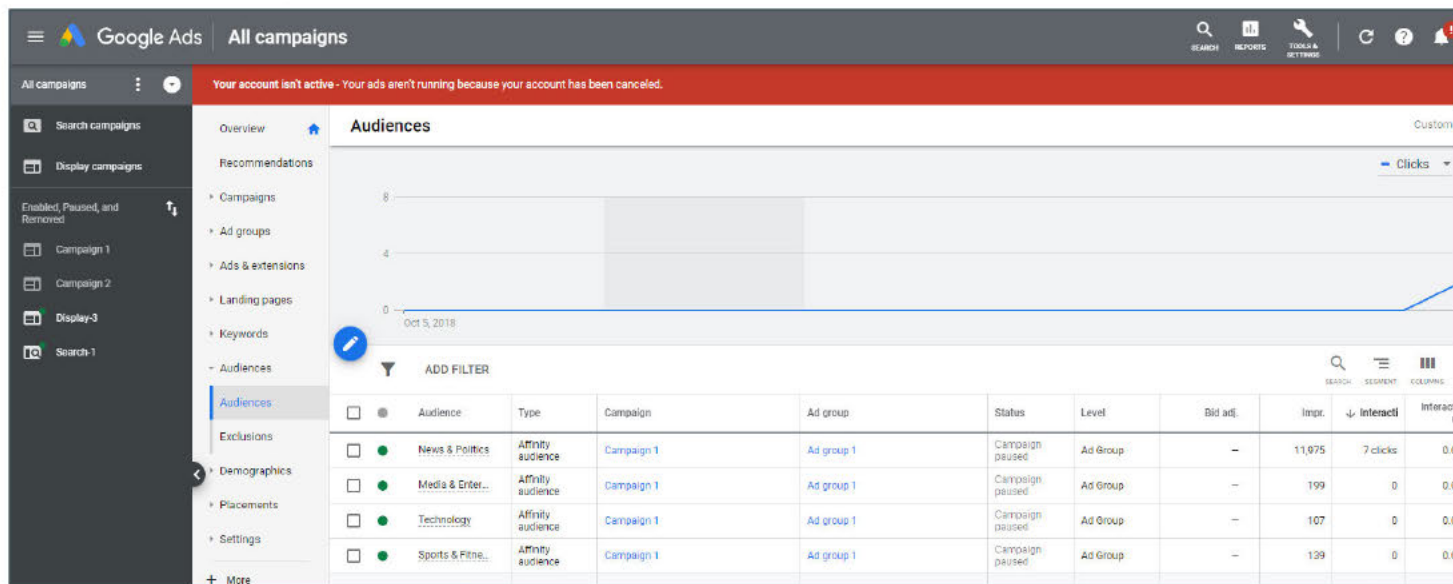
Google restricts advertisers' use of their preferred data partner for new customer prospecting on YouTube, Search, and Gmail



- Advertisers need to select the consumers to whom they wish to show ads (create a target audience)
- **Industry standard:** Advertisers are able to create a target audience using advertisers' existing customer database or website visitor history, and/or data providers (e.g., independent DMPs, data brokers, Google)
- **On YouTube, Google Search, and Gmail:** Google disallows advertisers from using their own chosen partner to categorize and target prospects; this forces advertisers to use Google data to create prospect target audiences

Google's buying tools are vehicles for Google's "zero-cost" proprietary audience data, which skews buying toward Google sell-side properties

Example:  Google Ads or  Display & Video 360



- Google Ads neither allows nor provides audience segments from outside data providers, restricting advertiser choice and competition. Google DV360 provides data from outside providers but doesn't negotiate best-available rates.
- Neither Google Ads nor DV360 put a price on Google data or allow it to be used in competing platforms

Like their competition, Google shares user tracking data from an array of sources to enhance advertisers' owned data — only with no transparency

Example:  Display & Video 360

Create a Lookalike Audience

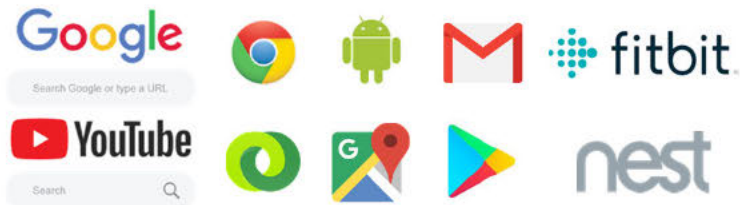
When expanding your audiences, prioritize:

Off  More reach

Exclude first-party lists 

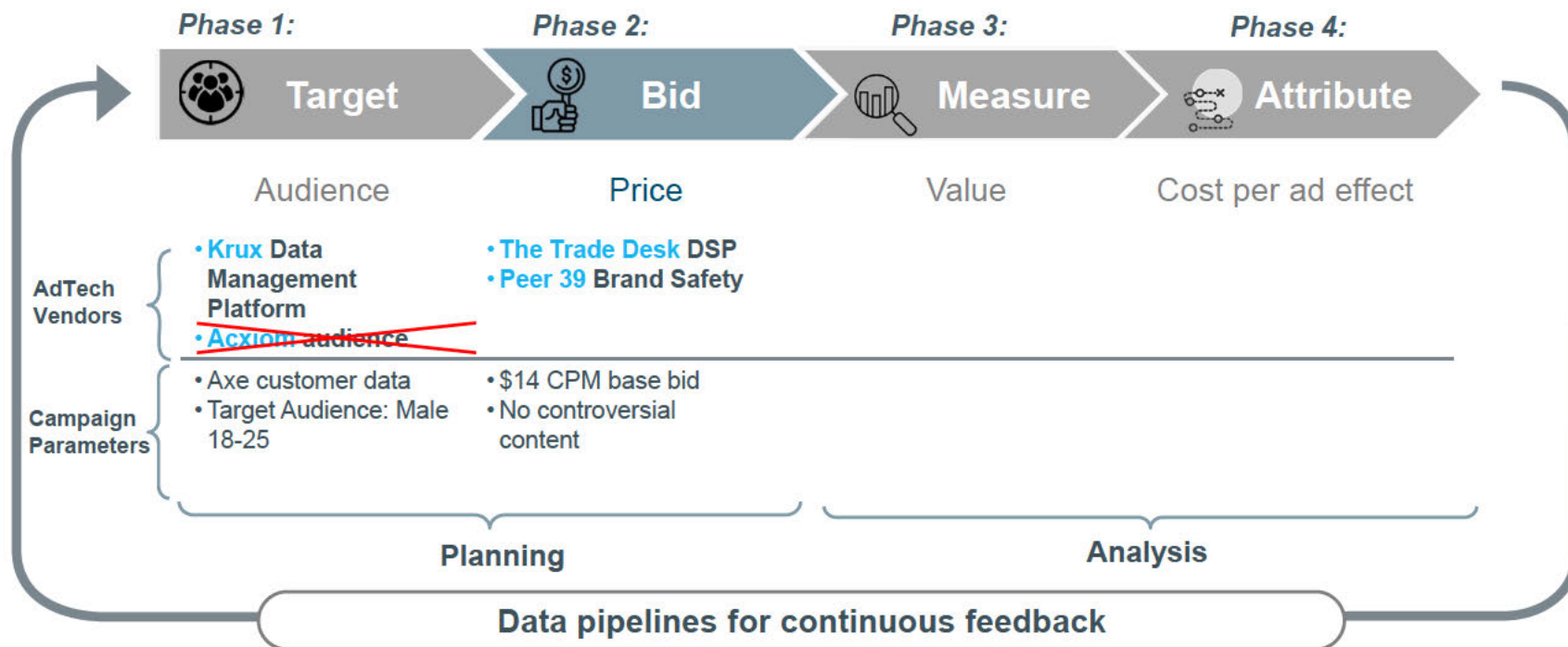
When first-party lists are included, make sure your line item is using a fixed bid.

Data Sources:



Phase 2: Bid

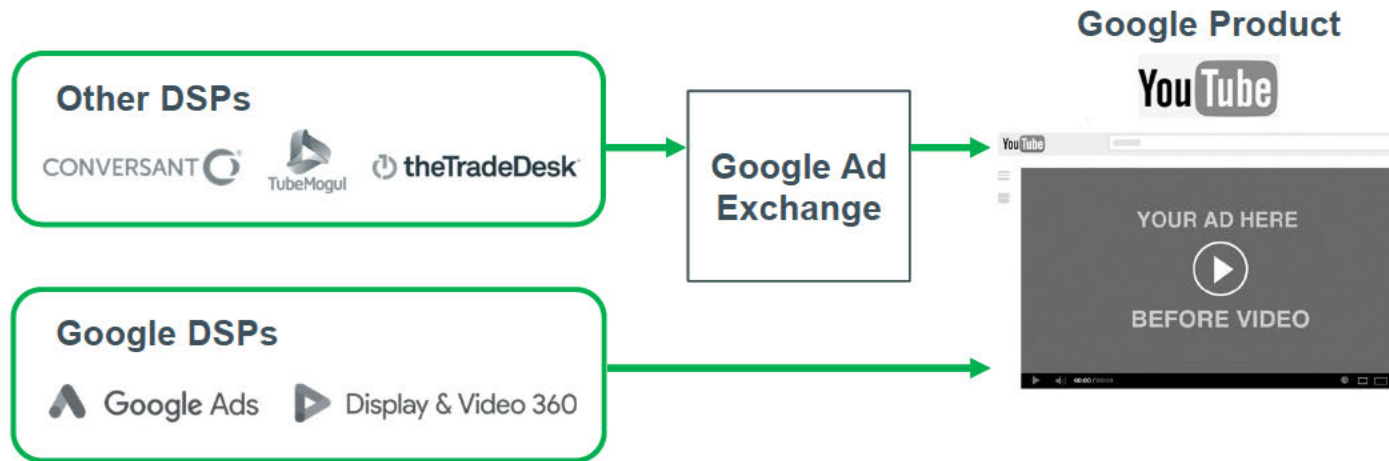
Example: An Axe body spray digital ad campaign



Advertisers want to use their chosen DSPs to bid on all available ad placements

Google completely excludes all competing DSPs from accessing YouTube

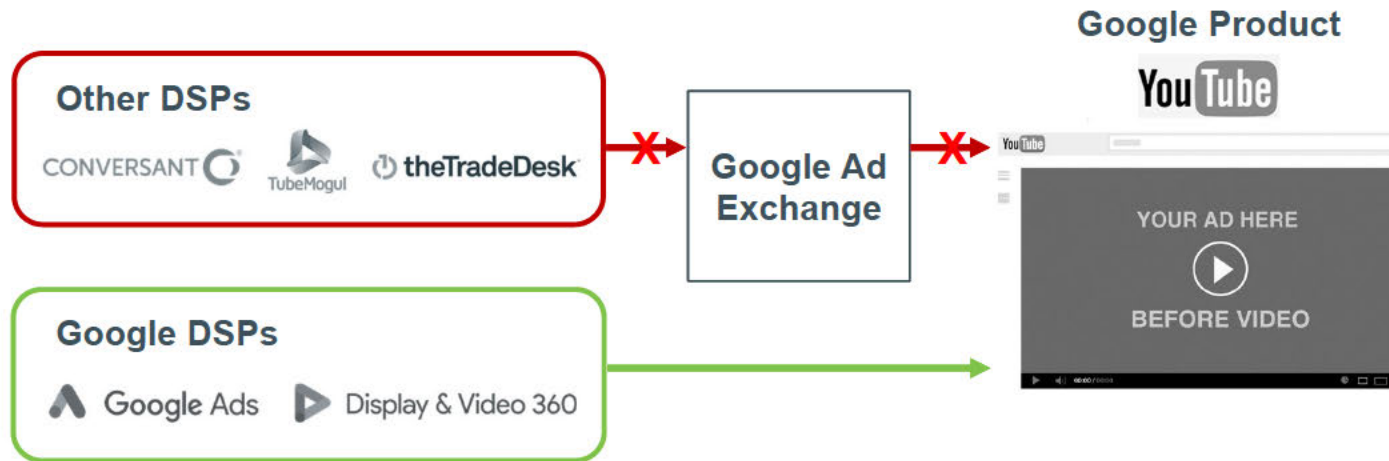
PRE-2015



- YouTube is a must-buy for advertisers and dominates the sale of online video ad placements
- Prior to 2015, non-Google DSPs could bid on YouTube, with advertisers' choice of guardrails

Google completely excludes all competing DSPs from accessing YouTube

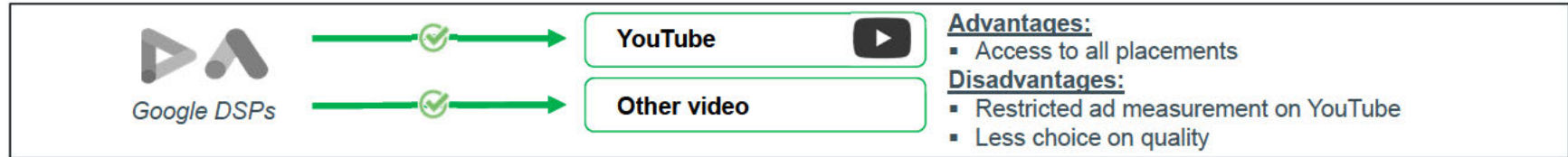
POST-2015



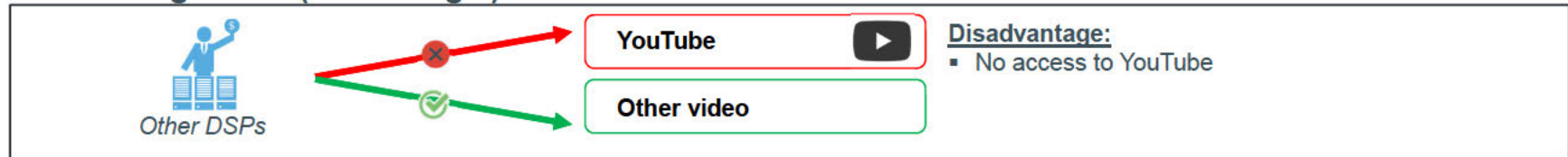
- YouTube is a must-buy for advertisers and dominates the sale of online video ad placements
- Prior to 2015, non-Google DSPs could bid on YouTube, with advertisers' choice of guardrails
- In 2015, Google withdrew YouTube from the Google Ad Exchange, excluding competing DSPs

Because of the YouTube restriction, advertisers are incentivized to use only the Google DSPs

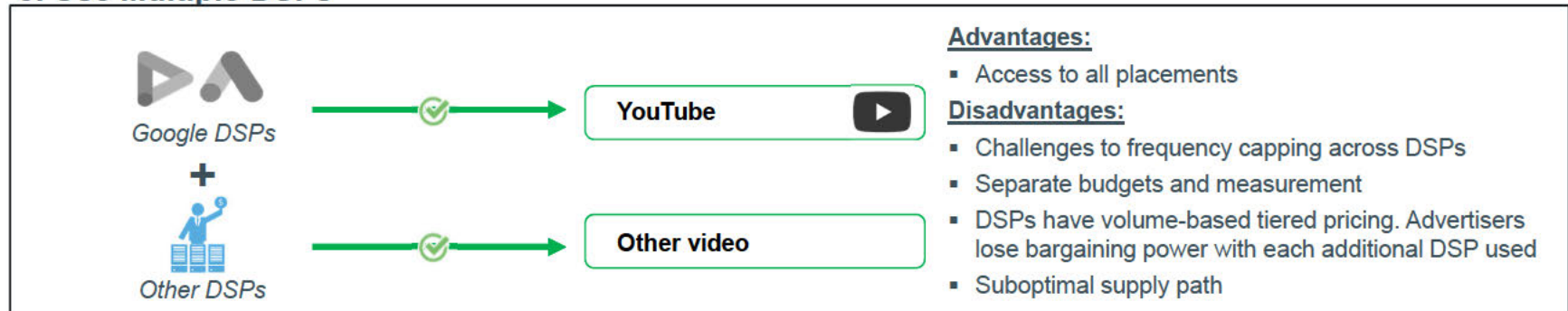
1. Use Single DSP (Google)



2. Use Single DSP (Non-Google)

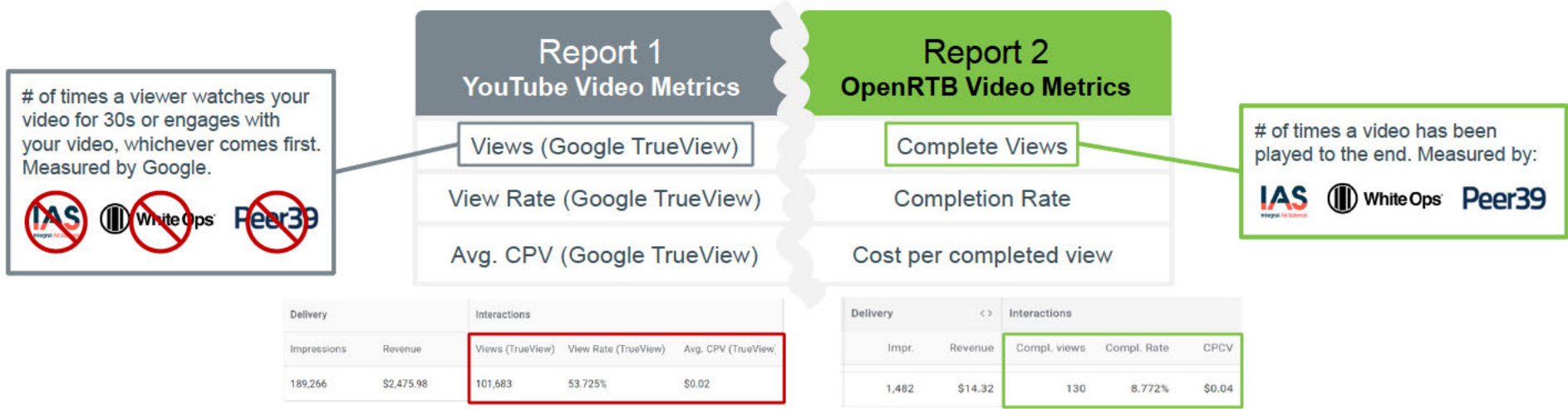


3. Use Multiple DSPs



In Google's DV360, YouTube and non-YouTube video ad performance appear on separate reports and are measured on different metrics

Example:  Display & Video 360 (Google DSP)



- In DV360, YouTube ad performance and non-YouTube ad performance must be evaluated on separate screens. Hence, their respective budgets have to be assigned separately
- Advertisers using DV360 are unable to make apples-to-apples comparisons between YouTube ad performance and non-YouTube ad performance

Google's rationale for YouTube DSP restriction: Development efforts


Focusing investments to improve buying on YouTube

Posted: Thursday, August 6, 2015 [Tweet](#) [Share](#)

At YouTube, over the past few years we've heard from clients that they want to access our marquee formats, such as TrueView, through programmatic channels. We've been investing to make that happen and recently made TrueView ads, which represent 85% of YouTube in-stream ads, available programmatically in DoubleClick Bid Manager (DBM). Clients have been pleased with the performance: those buying TrueView this way are already seeing higher engagement and view-through rates than with other video ad formats.

To continue improving the YouTube advertising experience for as many of our clients as possible, we'll be focusing our future development efforts on the formats and channels used by most of our partners. To enable that, as of the end of the year, we'll no longer support the small amount of YouTube buying happening on the DoubleClick Ad Exchange.

With this change, we'll be able to invest even more in creating the best and most effective YouTube advertising and buying experiences possible, continuing our efforts in TrueView and offerings like Google Preferred. Video advertising and programmatic buying are growing rapidly and being focused in our investments will help us drive them forward at an even faster rate.

 Posted by Neal Mohan
VP, Display & Video Advertising, Google



Translation: We're prioritizing direct deals and upfront deals over programmatic selling in our development efforts for YouTube advertising

Question

Since programmatic selling remained available in Google's DV360, just how much engineering effort is required to maintain programmatic selling on YouTube?

Google's rationale for YouTube DSP restriction: Advertisers' "demands"

Focusing investments to improve buying on YouTube

Posted: Thursday, August 6, 2015

[Tweet](#)

[Share](#)

At YouTube, over the past few years we've heard from clients that they want to access our marquee formats, such as TrueView, through programmatic channels. We've been investing to make that happen and recently made TrueView ads, which represent 85% of YouTube in-stream ads, available programmatically in DoubleClick Bid Manager (DBM). Clients have been pleased with the performance: those buying TrueView this way are already seeing higher engagement and view-through rates than with other video ad formats.

To continue improving the YouTube advertising experience for as many of our clients as possible, we'll be focusing our future development efforts on the formats and channels used by most of our partners. To enable that, as of the end of the year, we'll no longer support the small amount of YouTube buying happening on the DoubleClick Ad Exchange.

With this change, we'll be able to invest even more in creating the best and most effective YouTube advertising and buying experiences possible, continuing our efforts in TrueView and offerings like Google Preferred. Video advertising and programmatic buying are growing rapidly and being focused in our investments will help us drive them forward at an even faster rate.



Posted by Neal Mohan

VP, Display & Video Advertising, Google

One possible explanation is Google's Display and Video Incentive Program* (DVIP)

Under DVIP, big advertising agencies committed to large ad spend on YouTube in exchange for discounted YouTube rates. Discounted YouTube rates are important for agencies to win clients, because prospective clients want agencies to prove they have clout with powerful publishers like Google. DVIP deals also counted ad spend through DV360 (Google's DSP) toward agency commitments

After several years of ~50% annual growth in DVIP commitments, during which agencies grew at a much slower rate, it became impossible to buy enough YouTube as promised. With Google threatening to claw back discounts retroactively, agency leaders had no choice but to meet DVIP commitments by reallocating spend from rival DSPs to DV360

Though agency subject-matter experts pushed back, claiming that Google's DSP was inferior or otherwise unsuitable, the YouTube exclusion made that position untenable



Google's action appears consistent with the strategy of excluding competing intermediaries and increasing overall spend on Google

From: Neal Mohan [REDACTED] on behalf of Neal Mohan
Sent: Tuesday, February 09, 2010 12:28 AM
To: Henrique DE Castro
Cc: [REDACTED]
Subject: Re: Fwd: Pw: 2/1 - AdX Follow-up

+Scott since he understands this issue the best and is leading our agency demand-side platform (aka bidder) strategy...

Thanks for raising this issue, Henrique. I am glad that we are following up on the various action items that came out of our strategy deep dive with Vivaki back in December. Around this specific issue...

1) Fundamentally, we should have agency-level attribution through to AdX. Right now of course this happens at the aggregate level as you describe based on what bidders like Invite are contractually obliged to tell us. I will discuss how we will address this in the future further down in the note.

2) A couple things to note that I want to make sure we are all on the same page on however:

a) This is NOT the top priority from an AdX (or Google agency spend) standpoint. There are several other issues on sales and product that are actual gating factors to spend on AdX right now that we must address urgently and that the teams are working very hard on. This is not a gating factor to spend on AdX for Vivaki (or any of the other agencies for that matter right now).

As discussed today, we can go over the top 5-10 gating factor type issues in next week's GFM. There are several on the product, services and sales sides that are bigger than this one right now.

b) This is NOT the top priority from a Vivaki standpoint either. As we covered in the sessions with them back in December, there are several other product (and inventory) enhancements they would like to see on AdX that will actually increase spend. This is not one that will grow their spend. Curt Hecht reiterated all these points with me again last week when I saw him at an industry event. We are working on those other roadmap items to continue to increase their spend over time (which is already ahead of what they had committed to in our deal).

3) Yes, we should build a bidder and this has been part of our strategy for 2010. But this reporting issue is not the primary benefit of owning our own bidder of course but will be a nice side effect. The primary benefits on having a bidder are eliminating the disintermediation risk and substantially increasing display spend with Google from agencies (through the combined use of DFA - bidder - AdX). However we are in the early days here as you note - the teams are just getting staffed up. We are looking at options to accelerate this (potentially through M&A for example).

4) Until we have our own bidder, there are ways we will address this issue but each option has some strategic implications for us. We can ask Invite to append it to every response on the real-time bidder (however we are still dependent on them reporting on this accurately just like we are today and therefore may be the WRONG

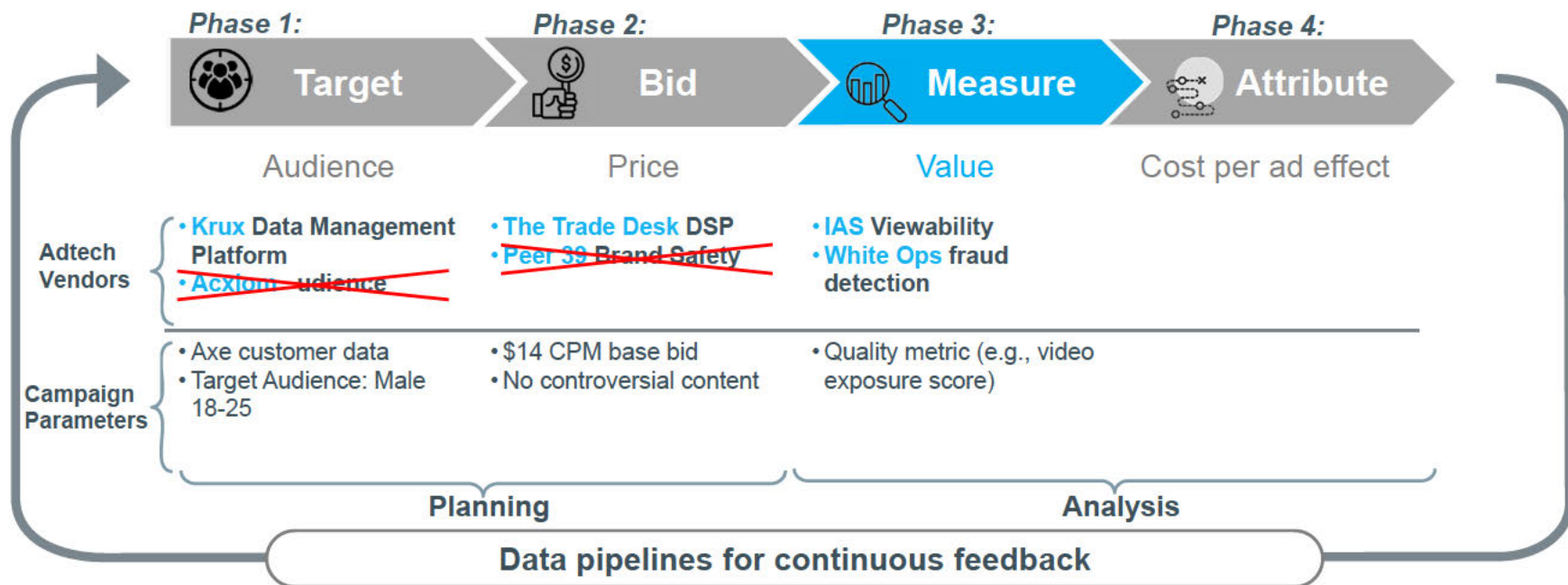


"The primary benefits on having a bidder are eliminating the disintermediation risk and substantially increasing display spend with Google from agencies (through the combined use of DFA – bidder – AdX)."

– Neal Mohan, Google SVP Display and Video Ads commenting on risks posed by 3rd party DSPs like Invite Media. Four months later, Google acquired Invite Media

Phase 3: Measure value

Example: An Axe body spray digital ad campaign



Advertisers use analytics tools to independently “grade” ad campaigns, just as rating agencies grade public companies. This enables advertisers to compare ad quality across publishers on the same metrics and adjust their buys accordingly

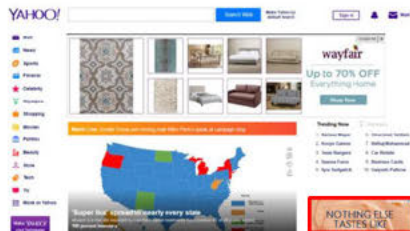
Digital advertising promises granular, real-time tracking, but in reality these promises are often compromised



VIEWABILITY

Did the ad have the opportunity to be seen?

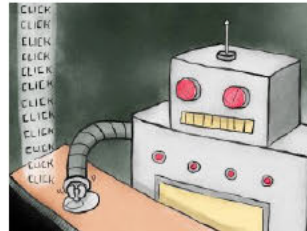
Ad buy is compromised when the ad is blocked or partially displayed



AD FRAUD

Was the ad seen by a human?

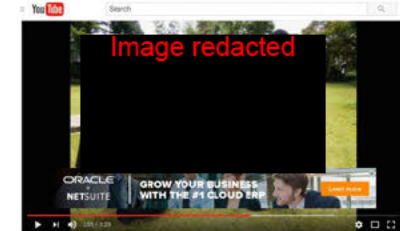
Ad buy is compromised when the ad view or click is generated by Invalid Traffic (IVT) such as a bot



BRAND SAFETY

Was the ad served in a brand-safe environment?

Ad buy is compromised when the ad appears next to unsafe content

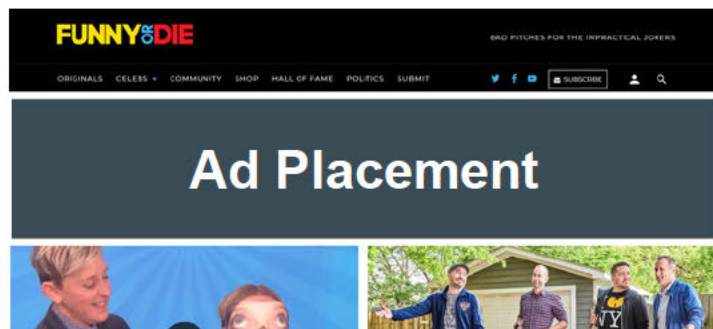


	Viewability (DoubleVerify)		Display Invalid Traffic (Moat)		Brand Safety (DoubleVerify)
	Viewability (IAS)		Display Suspicious Activity Protection (IAS)		Brand Safety (Grapeshot)
	Viewability (Moat)		Fraud & Invalid Traffic Avoidance (DoubleVerify)		Brand Safety (Peer 39)
					Brand Safety (IAS)

Example tools that monitor exposures

How ad serving works

A. The user's browser requests the page from the publisher's ad server



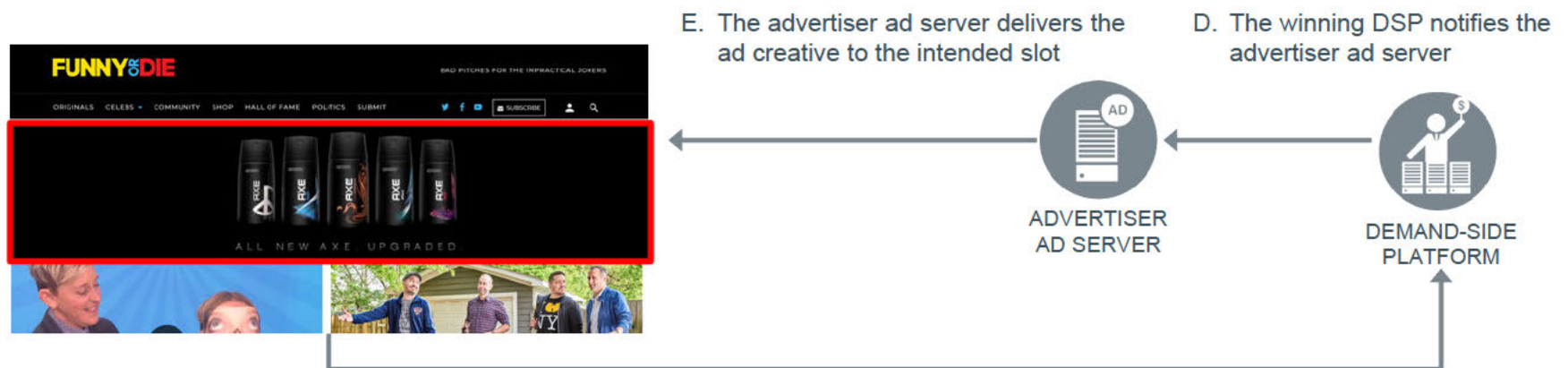
B. An ad tag (pieces of code) associated with the ad slot is called

```
<script language="javascript" type="text/javascript">
new function() {
this.rand = Math.floor(Math.random() * 1000000000000);
this.dvparams = 'ctw=2602318&mp=18647412&plc=15024192&sf=1702187';
this.dvregion = '0';
this.tagsrc = '';
this.altsrc = '<script src="https://secure.adnxs.com/pa?format=js&size=728x90" data-cm="1" src="">';
};
```

C. Publisher requests bids for the ad slot

```
{
  "id": "1234534625254",
  "at": 2,
  "tmax": 120,
  "imp": {
    {
      "id": "1",
      "banner": {
        "w": 320,
        "h": 50,
        "pos": 1,
        "battr": [
          13
        ]
      }
    }
  ],
  "badv": [
    "company1.com",
    "company2.com"
  ],
  "app": {
    "id": "234563",
    "bundle": "com.rovio.angrybirds",
    "cat": [
      "IAB2-1",
      "IAB2-2"
    ]
  },
  "publisher": {
    "id": "pub12345"
  }
}
```

How ad serving works



F. Once the ad is served, analytics vendors' JavaScript codes are triggered and call the DSP to provide monitoring information about the impression: e.g., how many seconds did the ad show on the browser

It is the industry standard to use independent analytics vendors to tag ads and provide consistent, unbiased metrics via open APIs

Many adtech vendors provide independent ad quality ratings

**Example:
Measuring video
ad quality**

$$\left\{ \frac{\text{Audible Time} + 50\% \text{ On-Screen Time}}{2 (\text{Averaged Ad Length})} \times \log_2 (\text{Screen Real Estate} \times 1) \right\} \times 100$$



AUDIBLE TIME

Audibility is another indicator of audience attention and the quality of that attention



50% ON-SCREEN TIME

50% On-Screen Time quantifies the opportunity for a user to actually see the ad in motion



AVERAGED AD LENGTH

The ad length (in seconds) of the creative, as a weighted average by impression volume. When used with 50% On-Screen Time and Audible Time, this component quantifies the percentage of video seen and heard



SCREEN REAL ESTATE

The more pixels an ad takes up on the screen, the fewer elements it is competing with for a viewer's attention

Advertisers join ad spend data and ad quality data using open APIs to automatically calculate value-adjusted cost

Example:  theTradeDesk[®]



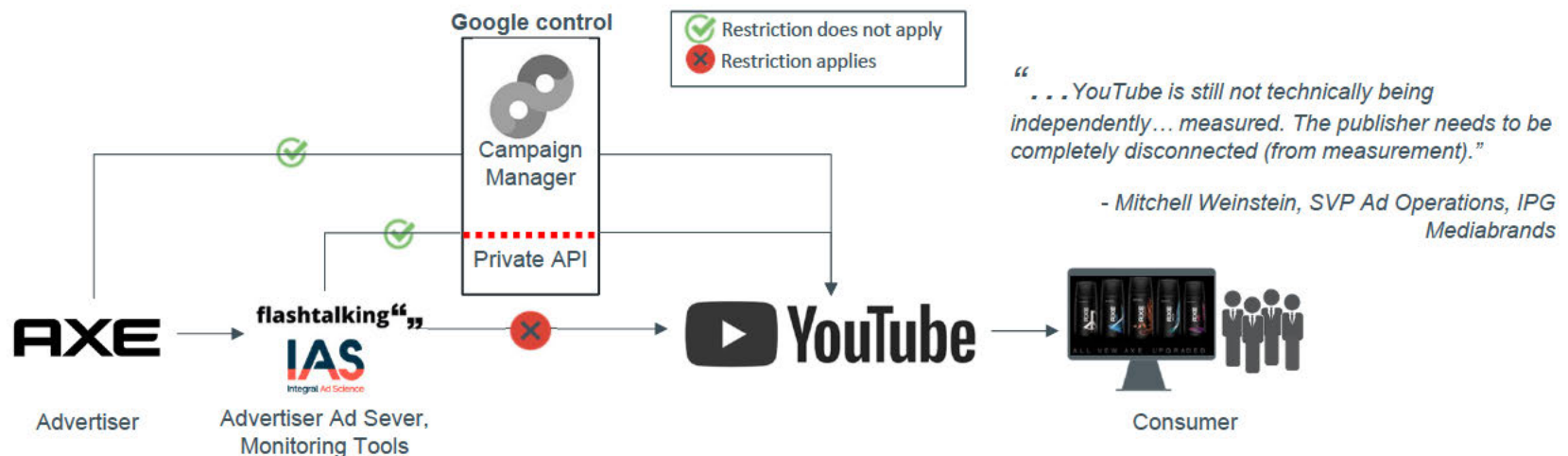
In a non-Google DSP (e.g., The Trade Desk), advertisers choose from many competing vendors (e.g., DoubleVerify, IAS) for independently-measured ad quality data to be utilized in DSP optimization and machine learning

Add Metrics

Which calculated performance metrics should your report include?

Metric
All <input type="text" value="Name Search"/>
Items to add (2)
<input type="checkbox"/> DoubleVerify IAB Video Viewable 3rd Quartile Rate
<input type="checkbox"/> DoubleVerify IAB Video Viewable 4th Quartile
<input type="checkbox"/> DoubleVerify IAB Video Viewable 4th Quartile Rate
<input type="checkbox"/> DoubleVerify IAB Viewable at 10 seconds
<input type="checkbox"/> DoubleVerify IAB Viewable at 10 seconds Rate
<input type="checkbox"/> Total Seconds In View
<input type="checkbox"/> Video In View Event
<input type="checkbox"/> White Ops SiVT Bids Avoided
<input type="checkbox"/> IAS Display Fully In View 1 Second
<input type="checkbox"/> IAS Display Fully In View 1 Second Rate
<input type="checkbox"/> IAS Display Fully In View 15 Seconds
<input type="checkbox"/> IAS Display Fully In View 15 Seconds Rate
<input type="checkbox"/> Advertiser Viewable CPM (vCPM) (Adv Currency)
<input type="checkbox"/> Advertiser Viewable CPM (vCPM) (USD)

YouTube's ad serving restriction forbids advertiser "presence" during ad transactions



- **Before:** advertisers on YouTube could use non-Google advertiser ad servers and monitoring tools to independently verify the data supplied by YouTube
- **After:** In May 2019, Google mandated that all non-Google monitoring tools must use a Google-controlled API to serve ads on YouTube. Fraud and viewability measurement vendors were restricted to a similar private-API process. Google obfuscates the data sent to adtech vendors, who do not have access to raw YouTube ad data
- Google withholds feedback on the specific YouTube video on which each ad appeared – a glaring brand-safety risk
- As advertisers lose independent measurement, publishers are disincentivized to create high quality, premium-priced video placements



YouTube’s ad serving restriction forbids advertiser “presence” during ad transactions: a detailed comparison

Example: Measuring video ad

	Open API method for all video publishers except YouTube	Private API method for YouTube only
Data collection	<ul style="list-style-type: none"> Vendor deploys tags to independently collect raw data 	<ul style="list-style-type: none"> Vendors are prohibited by Google from deploying their standard tag on YouTube ads Google collects the raw data, aggregates measurement data, stores the data in Google’s Ads Data Hub (ADH)
Data Analysis	<ul style="list-style-type: none"> Vendor conducts independent analysis of raw data without interference from outside parties 	<ul style="list-style-type: none"> Vendor retrieves Google’s aggregated measurement data from ADH and calculates quality metrics
Effect	<ul style="list-style-type: none"> Vendor provides truly independent ad measurement service to advertisers 	<ul style="list-style-type: none"> Without access to raw data, vendor is effectively “measuring” data curated by Google Independent measurement is degraded, with vendors’ independence severely compromised by Google

YouTube Spars With Auditor Over Transparency of Advertising Risks

OpenSlate has declined to sign a Google contract it believes bars sharing of information on hate speech, profanity and violence

Google wants to substantially limit the information a key auditor of YouTube can share about the risks of advertising on the video service, according to people familiar with the situation, highlighting tensions between the tech giant and Madison Avenue.

The auditor, New York-based OpenSlate, is refusing to sign a contract that would prevent it from reporting to clients when ads have run in videos with sensitive subject matter, including hate speech, adult content, children’s content, profanity, violence and illegal substances, according to an email the firm sent over the weekend to ad agencies.

Under the terms Google proposed, OpenSlate would need approval from Google to share certain metrics about YouTube’s content, one of the people familiar with the situation said.

OpenSlate works with leading brands and ad agencies, like McDonald’s Corp., MCD 2.04% ▲ Pfizer Inc., PFE 1.95% ▲ Unilever PLC and WPP WPP 4.21% ▲ PLC, providing them with information to confirm that their ads on YouTube are appearing alongside content that marketers deem safe.

In the email to ad agencies, which was reviewed by The Wall Street Journal, OpenSlate said it hasn’t been able to reach an agreement with Google to be included in a new, updated version of YouTube’s ad-measurement program.

Source: *The Wall Street Journal*, April 19, 2020

Sources: <https://www.wsj.com/articles/ad-measurement-feuds-on-facebook-youtube-hinge-on-code-1478689200>; <https://marketingland.com/google-ads-data-hub-beta-216059>; https://www.wsj.com/articles/youtube-spars-with-auditor-over-transparency-of-advertising-risks-11587340250?shareToken=st46c12208670843c9a5035c6b9caf42e7&reflink=share_mobilewebshare

Advertisers using the Google platform cannot integrate metrics from any independent viewability vendors

The screenshot shows the Google Ads interface with the 'Metrics' section expanded. A red box highlights the 'Active View' metrics, which are proprietary to Google. The metrics listed are:

- Booked Viewable Impressions
- Active View: % Measurable Impressions
- Active View: % Viewable Impressions
- Active View: Average Viewable Time (Seconds)
- Active View: Eligible Impressions (checked)
- Active View: Impression Distribution (Not Measurable)
- Active View: Impression Distribution (Not Viewable)
- Active View: Impression Distribution (Viewable)
- Active View: Measurable Impressions (checked)

- Independent ad measurement on the Google Display Network isn't completely blocked. However, Google only provides disjointed reports (Google placements, non-Google placements) that must be manually integrated
- Disjointed reports offer very limited value to advertisers since they can't be used in algorithmic optimization
- Google's "Active View" is a proprietary viewability offering, tied to the Google stack. It can't be an optimization signal in competing platforms

YouTube's lack of transparency and feedback makes it a risky site

- Open standards for ad serving and quality monitoring enable advertisers to scrutinize the commercial web marketplace. Advertisers' scrutiny has a disinfectant effect, like sunlight
- On the open web, advertisers' scrutiny help clean up the marketplace

Google's bad week: YouTube loses millions as advertising row reaches US

Major brands including Verizon and Walmart pulled their ads after they were found to be appearing next to videos promoting extremist views or hate speech

It's been a bad week for Google, with major brands pulling millions of dollars in advertising amid rows over extremist content on [YouTube](#).

In the US, the telecom companies [AT&T](#) and [Verizon](#), as well as the pharmaceutical company GSK, Pepsi, Walmart, Johnson & Johnson and the car rental firm Enterprise, have all pulled advertising from Google's video-sharing platform, a contagion spreading from Europe, where a number of high-profile advertisers pulled out of YouTube following an investigation by [the Times](#).

Major brands' content was found to be appearing next to videos promoting extremist views or hate speech, with a cut of the advertising spend going to the creators.

Verizon's ads were featured alongside videos made by Egyptian cleric Wagdi Ghoneim, who was banned from the US over extremism, and the hate preacher Hanif Qureshi, whose preachings were said to have [inspired the murder](#) of a politician in Pakistan.

YouTube fraudulent "views" for sale



buy youtube views

Buy YouTube Views from \$5 per 1000 views (Instant, Safe ...

<https://buildmyviews.org/buy-youtube-views>

When it comes to promotion of your YouTube channel it's a complete no-brainer to choose BuildMyViews as it's the best way to buy real YouTube views. From here you can buy YouTube views very easily because BuildMyViews is the most efficient and safest way to grow your YouTube channel. So, here, you will get to know all about how to buy YouTube Views easily and grow your channel fast. As you can ...

Buy YouTube Views 100% Active and Real \$1.39 - InstaFollowers

<https://www.instafollowers.co/buy-youtube-views>

Buy YouTube Views. YouTube craze continues. Everyone, from 10-year-olds to 70-year-olds, wants to make money with YouTube. When you explore this in detail, you will find that it is not easy at all. Don't dream of making money by taking only a video. However, you can buy YouTube views for a faster process. This service is legal and does not damage your YouTube account.

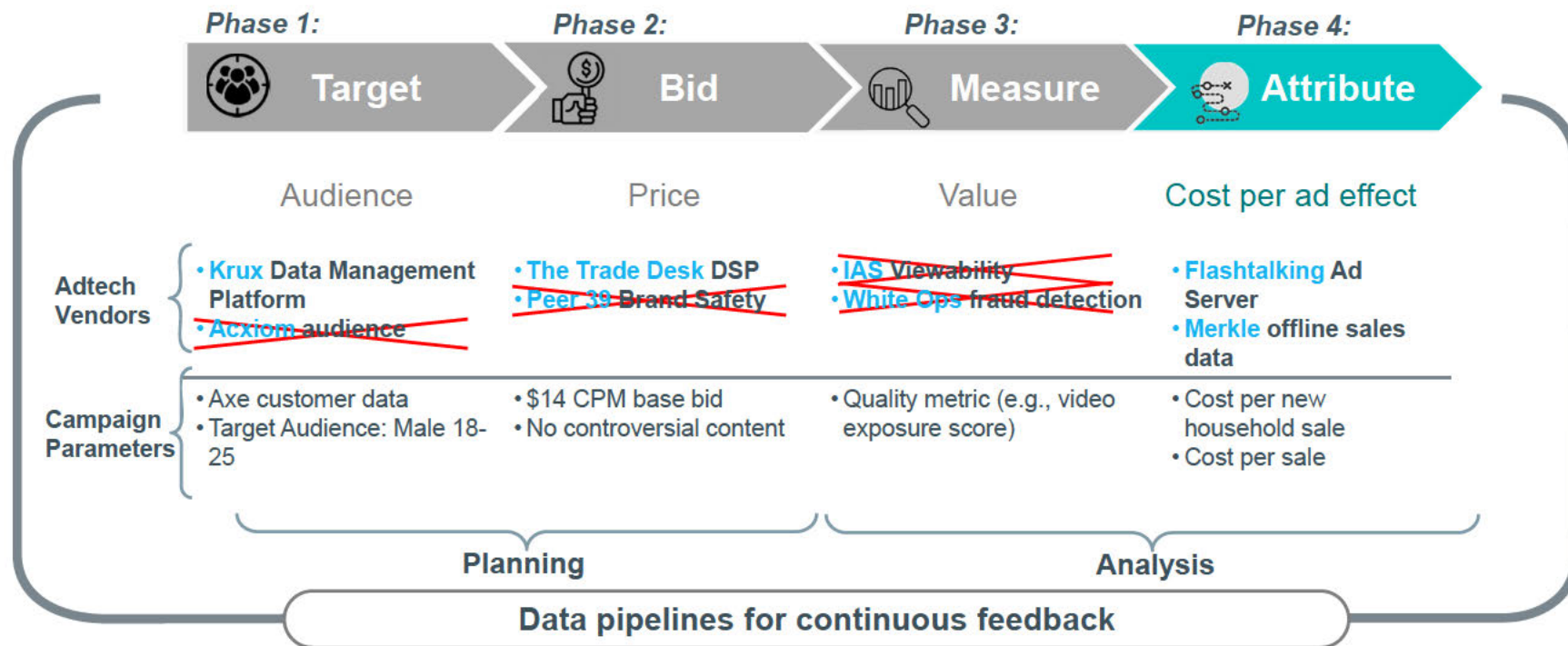
Buy YouTube Views : \$5 for 1000 Views | \$9 for 2000 ...

<https://buildmyviews.org/worldwide-views>

BUY WORLDWIDE YOUTUBE VIEWS. Here at BUILDMYVIEWS having your video seen by a wide range of people can sometimes be a hard job, to be seen you have to have a certain amount of people view your

Phase 4: Attribute credit

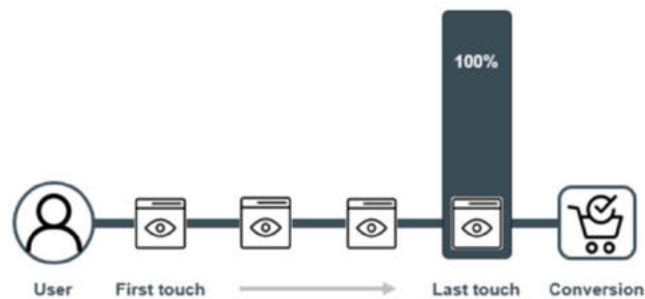
Example: An Axe body spray digital ad campaign



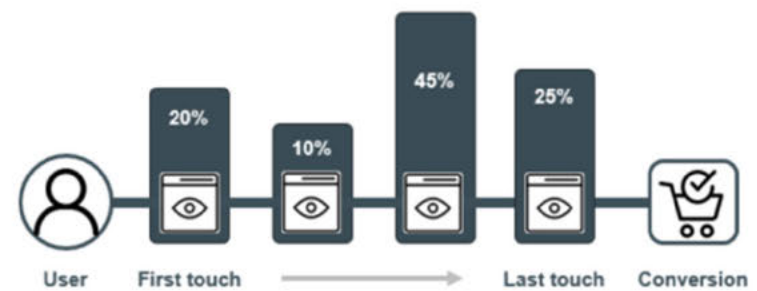
Advertisers want to attribute credit to ad conversions so they can optimize ad budget allocation

It's easy to count total conversions, but difficult to attribute credit

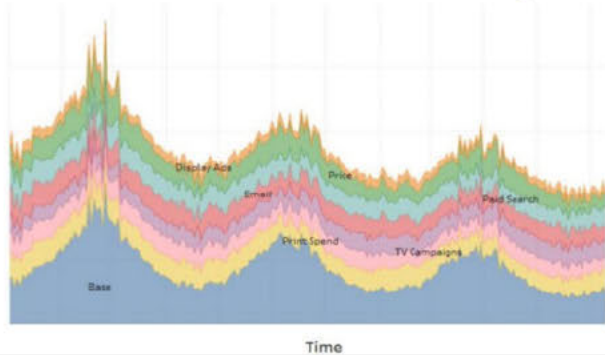
Simple attribution



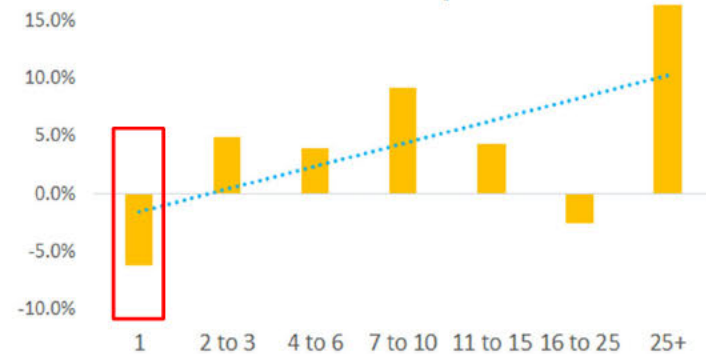
Custom attribution



Econometric mix modeling

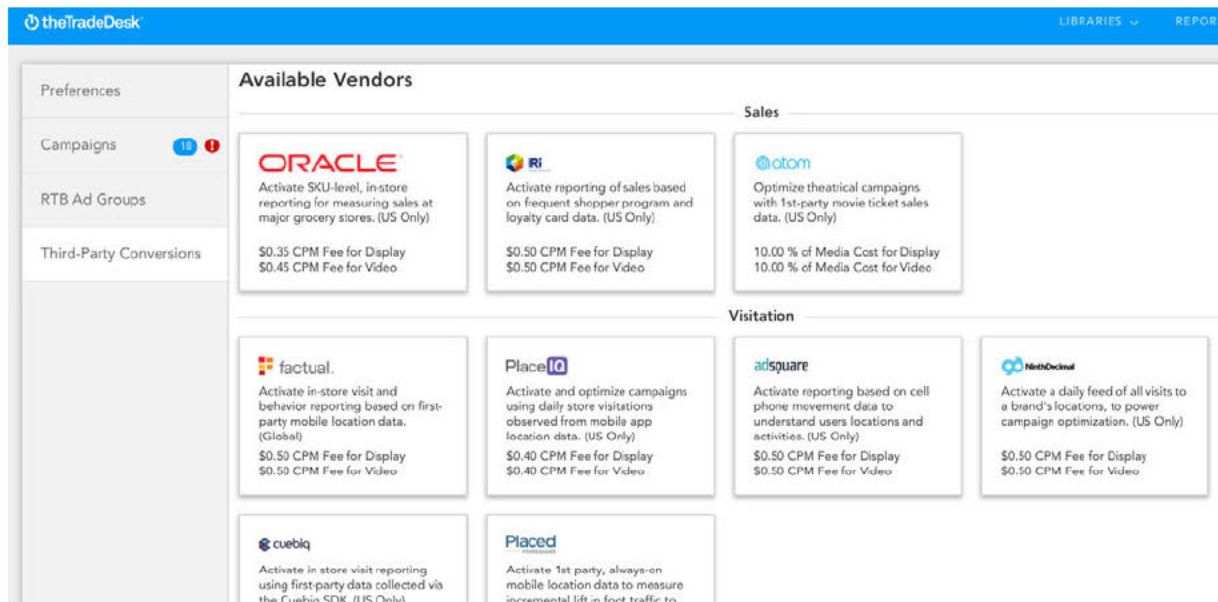


Controlled lift experiments



Some DSPs have options for conversion counting...

Example: theTradeDesk® (DSP)

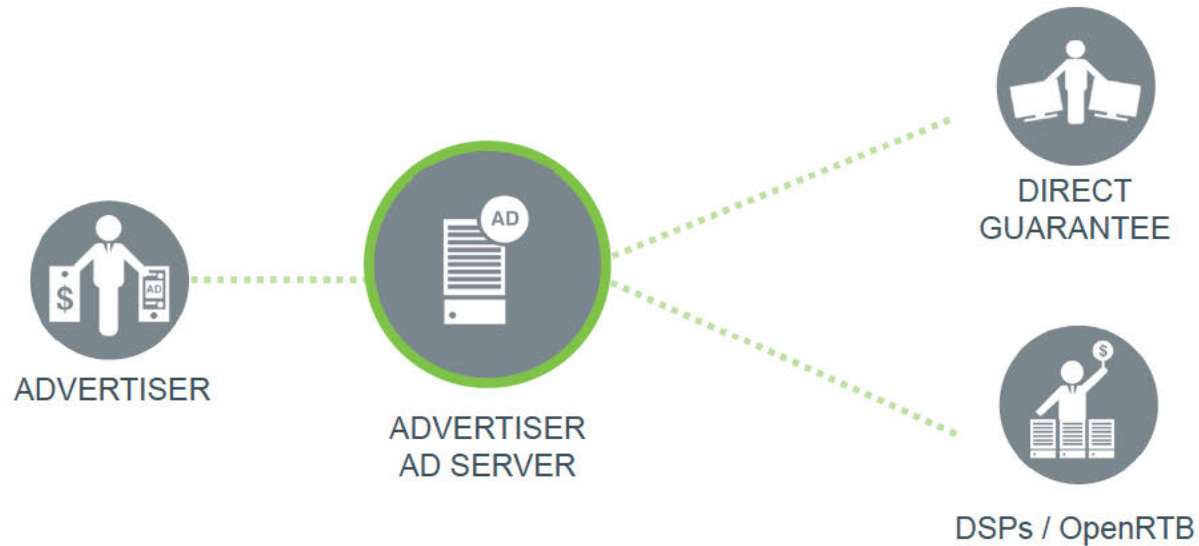


The screenshot shows the 'Available Vendors' section in theTradeDesk. The interface is divided into 'Sales' and 'Visitation' categories. A sidebar on the left contains navigation options: Preferences, Campaigns (with 18 items), RTB Ad Groups, and Third-Party Conversions. The 'Available Vendors' section lists several vendors with their respective features and fees.

Vendor	Description	Display Fee	Video Fee
ORACLE	Activate SKU-level, in-store reporting for measuring sales at major grocery stores. (US Only)	\$0.35 CPM	\$0.45 CPM
Ri	Activate reporting of sales based on frequent shopper program and loyalty card data. (US Only)	\$0.50 CPM	\$0.50 CPM
ctom	Optimize theatrical campaigns with 1st-party movie ticket sales data. (US Only)	10.00 % of Media Cost	10.00 % of Media Cost
factual.	Activate in-store visit and behavior reporting based on first-party mobile location data. (Global)	\$0.50 CPM	\$0.50 CPM
PlaceIQ	Activate and optimize campaigns using daily store visitations observed from mobile app location data. (US Only)	\$0.40 CPM	\$0.40 CPM
adsquare	Activate reporting based on cell phone movement data to understand users locations and activities. (US Only)	\$0.50 CPM	\$0.50 CPM
NorthDecimal	Activate a daily feed of all visits to a brand's locations, to power campaign optimization. (US Only)	\$0.50 CPM	\$0.50 CPM
cuebiq	Activate in-store visit reporting using first-party data collected via the Cuebiq SDK. (US Only)		
Placed	Activate 1st party, always-on mobile location data to measure incremental lift in foot traffic to		

- In a non-Google DSP (e.g., The Trade Desk), advertisers choose from many competing attribution partners to help measure conversions
- Attribution data partners differentiate based on data source and attribution methodology, thus providing advertisers with choice and innovations

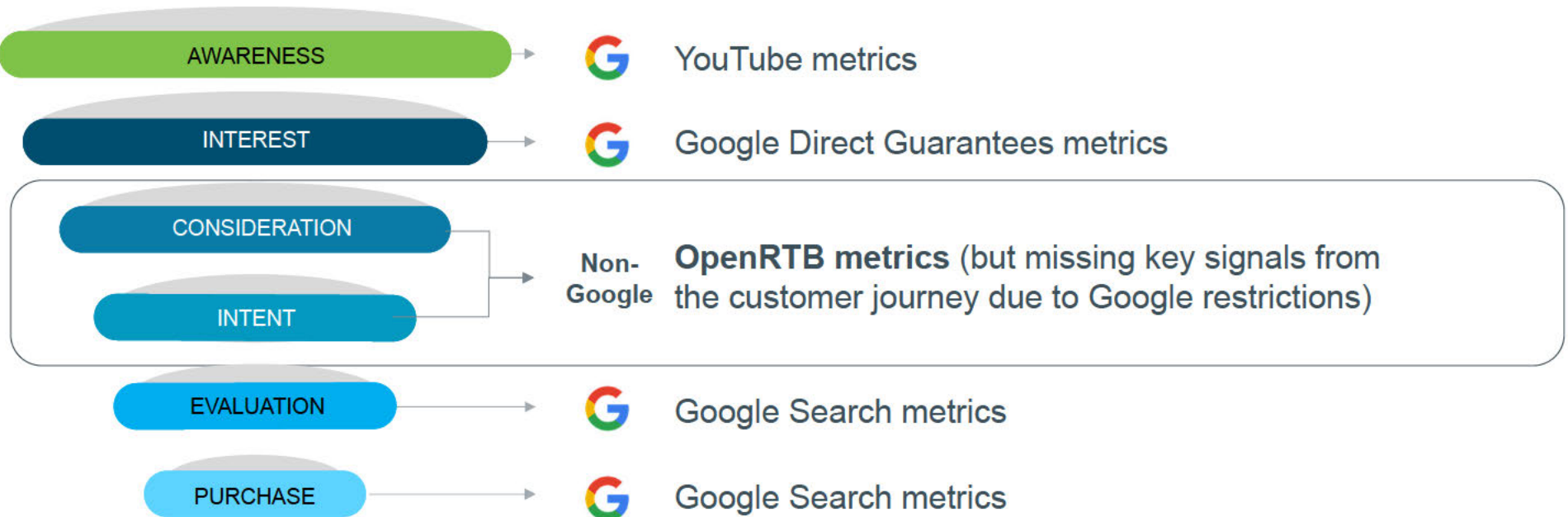
...but the advertiser ad server is the hub, and important to any attribution method



Advertiser ad servers are bookkeepers that provide advertisers with a consolidated view of spend AND returns. They are technological agents of buyer interests, built to be present during every transaction








Google's dominant advertiser ad server gives Google a significant information asymmetry vs advertisers

Example: Attribution metrics available to a typical large advertiser

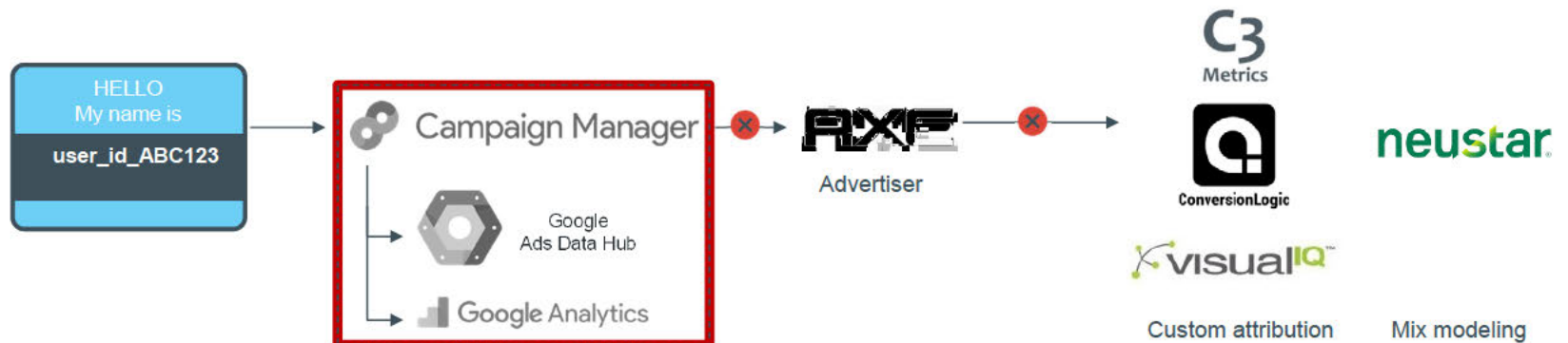


It's in advertisers' interest for all adtech vendors to know what ads each user has seen and where. However, Google's advertiser ad server prohibits ad interaction data from leaving the Google console. There's no API out of Google's advertiser ad server

Google's dominant advertiser ad server gives Google a significant information asymmetry vs advertisers: a detailed comparison

	   Rival advertiser ad servers	 Google Campaign Manager (CM) Google's advertiser ad server
 Ad Serving	<ul style="list-style-type: none"> To serve ads on YouTube, Rival advertiser ad servers have to be certified by Google, and serve ads indirectly via a Google-owned API. Feedback is aggregated 	<ul style="list-style-type: none"> CM is the only advertiser ad server allowed to serve ads unfettered on YouTube CM is the only ad server that can attribute credit across YouTube, search and banner display without complicated integrations or workarounds
 Tracking	<ul style="list-style-type: none"> Rely on publisher partnerships (Transparency and Consent Framework) for consent to track 	<ul style="list-style-type: none"> Google was advantaged by GDPR in a market where Google was already dominant Google obtains consumers' consent to track when they use Google services (e.g., Google Search, Gmail, Chrome, Android, Map, YouTube, Google Home)
 Attribution	<ul style="list-style-type: none"> Designed to accommodate advertisers' needs. Often highly customizable 	<ul style="list-style-type: none"> CM has no API to export ad interaction data Furthermore, the default attribution model in DCM is "last touch." This model prioritizes search clicks and favors Google, since Google search is often the last step before purchase When there is no click preceding a conversion, Google's DSP is advantaged via exclusive access to video and direct impression data in CM

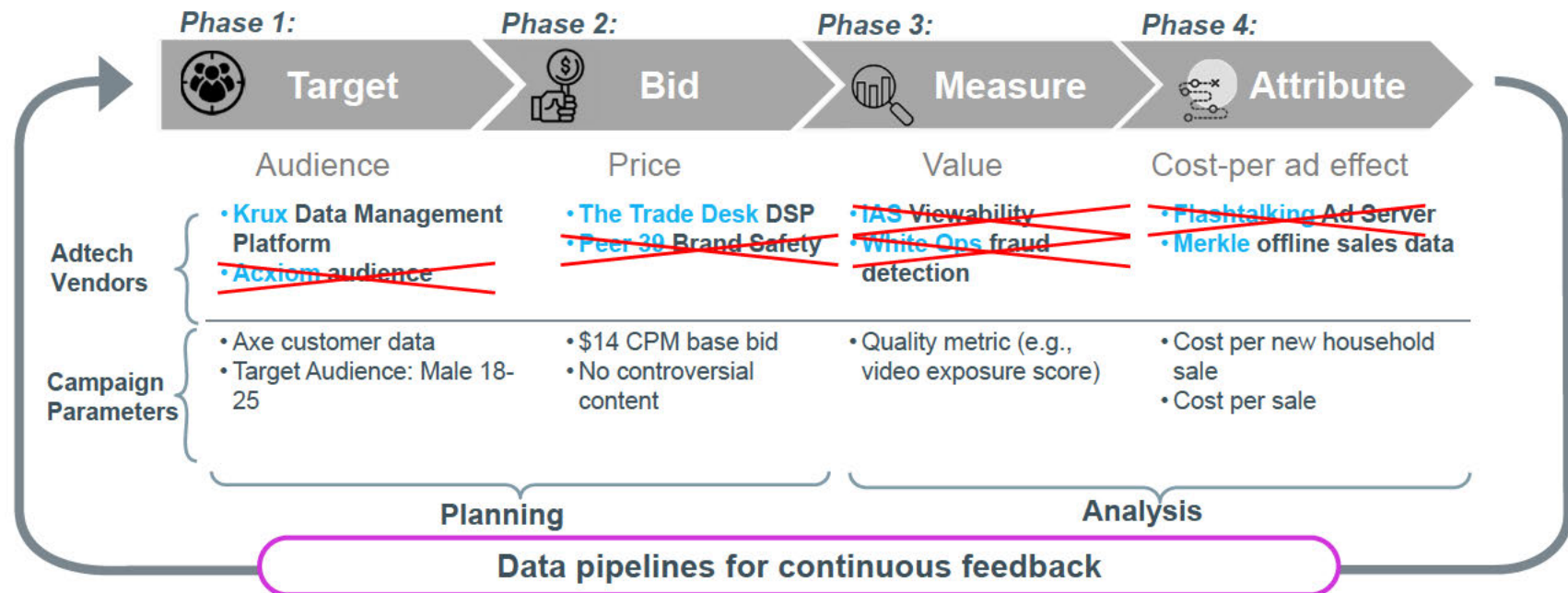
In 2018, Google also blocked manual transfer of raw data for custom attribution



<p>In 2018, Google announced that it would limit access to Google's UserIDs</p> <p>The move forced advertisers to choose between: (a) switching to a non-Google ad server, which is costly and complex; or (b) relying on Google's full set of adtech products - particularly Ads Data Hub and Google Analytics</p> <p>Google's restriction excludes rival DMPs and Analytics tools. It deepens the market opacity by enabling Google alone to "grade its own homework"</p> <p>Competitors (Xandr, The Trade Desk, LiveRamp, and MediaMath) continue to share user IDs today in a GDPR-compliant framework</p>	<p>Post-2018, Advertisers can no longer use Google's ad server with independent:</p> <ul style="list-style-type: none"> ⊘ Segmentation ➔ Target ⊘ Frequency Capping ➔ Bid ⊘ Verification ➔ Measure ⊘ Attribution ➔ Attribute
--	---

Phase 5: Interoperate: cookies and user IDs

Example: An Axe body spray digital ad campaign



Advertisers want the ability to track consumer behavior online for targeting, conversion tracking, and frequency capping. Advertisers and adtech tools rely on cookies to perform these functions

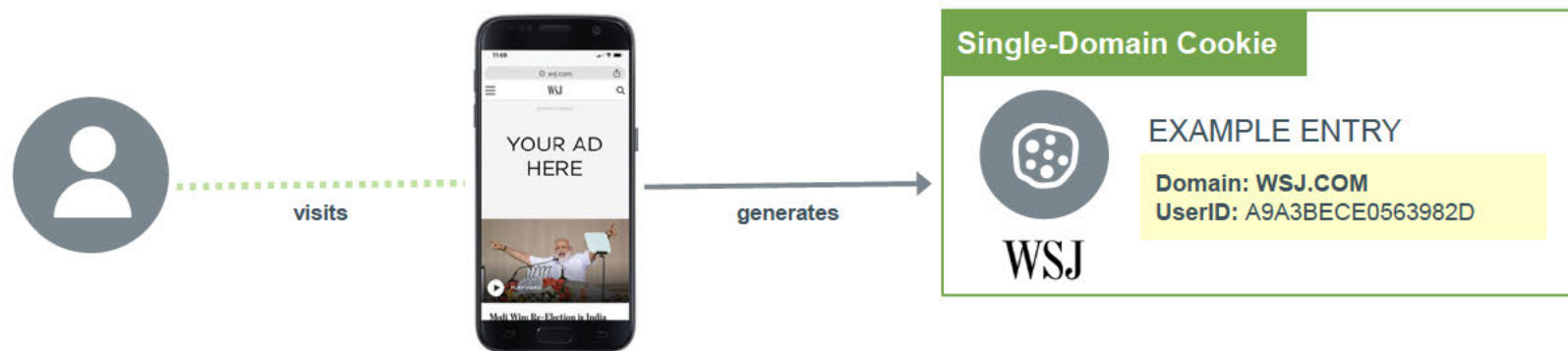
Online Identity

Why isn't web browsing completely private?

- Core functionality like going back a page wouldn't work without recognition
- Enforcement of cyber-criminality would be hindered
- Continuity of experience across devices and programming languages requires disclosure of "user agent" data

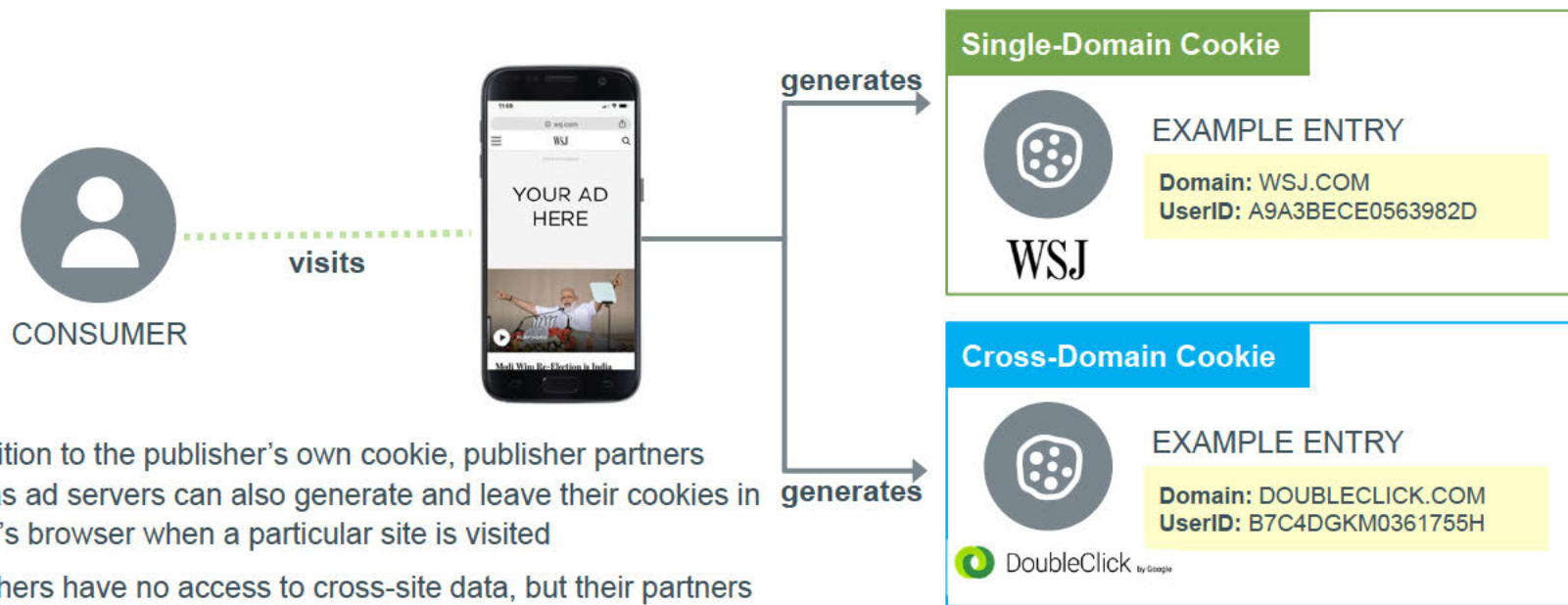


Single-Domain Cookies



- Generated by the publisher's domain when user visits the site
- While such cookies can be used to track user behavior, visibility is limited to only users and activities on the publisher's domain as publisher cannot access cookies from other domains

Cross-Domain Cookies

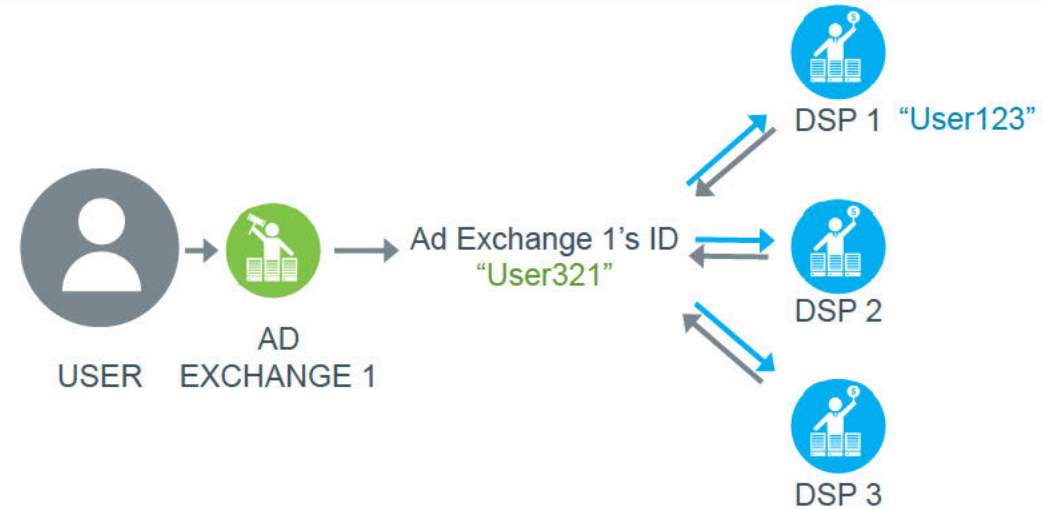


- In addition to the publisher's own cookie, publisher partners such as ad servers can also generate and leave their cookies in a user's browser when a particular site is visited
- Publishers have no access to cross-site data, but their partners have historically been allowed to link data from all cookies placed on all partners' behalf. The standard was to only sell this data as anonymous, aggregated segments

Cookie Syncing Overview

What is Cookie Syncing?

- A process through which companies involved in programmatic transactions build match tables, allowing them to recognize users identified by other firms' IDs
- Different platforms (DSP, Ad Exchange, DMP, etc.) store any information they've collected on a user under their respective IDs
- These companies work together to match IDs and each leverage their own data without sharing more than IDs.



Why is Cookie Syncing Necessary?

- Cookie syncing is necessary because web servers can only request cookies set to their own domain
 - DSPs need a way to identify users in auctions without making an unauthorized request for their own ID
- Cookie syncing enables competition:
 - It creates a level playing field for recognition, not data collection
 - The information acquired by any given party remains with that party

Match table of DSP1:

DSP 1's ID	Exchange 1's ID	Exchange 2's ID
User123	User321	User ABC
User234	?	?

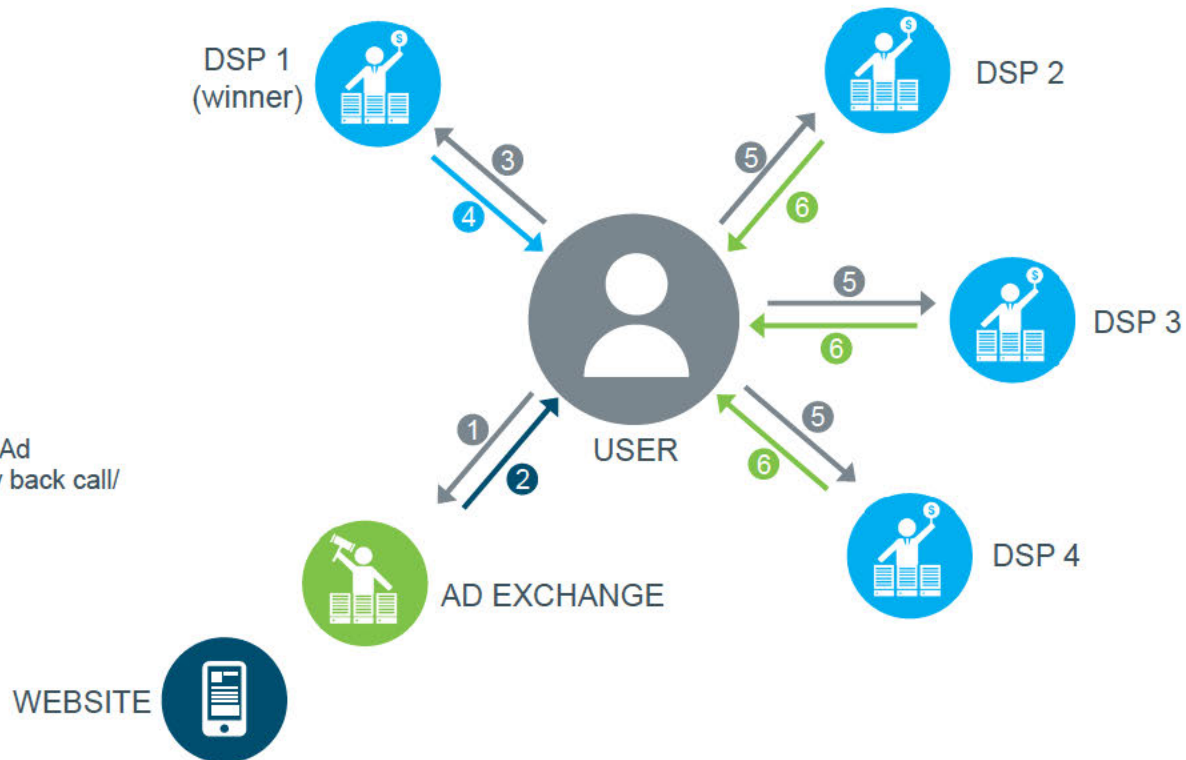
How Cookie Syncing Works

Recognition Process

1. User visits advertiser website
2. Redirected to Marketer's DSP
3. Calls the Marketer's DSP
4. DSP cookie delivered

Matching Process

5. Redirected to various DSPs that Ad Exchange is syncing with ("Piggy back call/ Cookie Sync")
6. Ad Exchange Cookie Delivered



Challenges to Cookie Syncing & Potential Alternatives

Challenges to Cookie Syncing

- Large size of the ad ecosystem makes finding and matching users challenging
- Cookie matching is an imperfect process with only 60% of data being correctly matched
 - Multiple users with the same profile
 - Cases where multiple profiles exist for the same user
- 40% of online users' data is still not being monetized optimally creating a big gap in audience targeting methods
- Targeting based on cookie matching is a real-time task
 - Given number of syncs involved between DSPs, Ad Exchanges and DMPs, ad loading is slow
 - Delay of a few seconds can majorly impact the experience
- Cookies are limited to the only browser-based environment & log-in services like Facebook target their users perfectly in a walled garden
 - Not all walled gardens are willing to share this data
 - Creates a challenge for others to match walled gardens' level of targeting

Potential Alternatives

- Initiatives like advertising ID consortium and Digitrust are designed to offer people-based identifier
 - Leveraging cookie data from every possible source (demand side, supply side, advertisers and publishers)
 - Intent is to create a standard platform for audience targeting
- Implementing advertising ID consortium at scale can solve sync issue by:
 - Standardization cookie ID and device ID
 - Identification of users rather than their devices or browsers
 - Creation of an interconnected channel for adtech to share data while ensuring security of user data
 - Consensus across members of consortium to respect privacy of user data and protect it at all costs

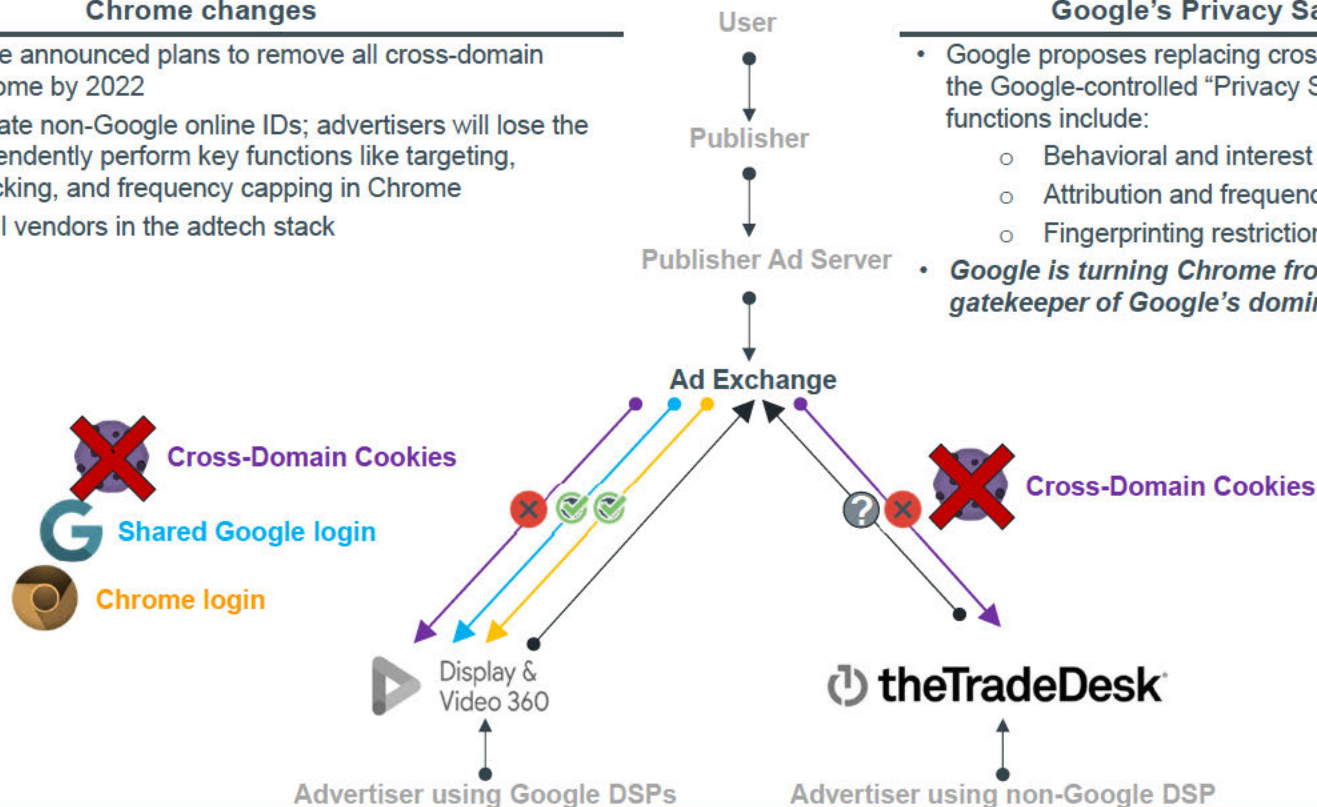
Google's Chrome changes threaten to put Google in charge of all adtech

Chrome changes

- In 2020, Google announced plans to remove all cross-domain cookies in Chrome by 2022
- This will decimate non-Google online IDs; advertisers will lose the ability to independently perform key functions like targeting, conversion tracking, and frequency capping in Chrome
- This impacts all vendors in the adtech stack

Google's Privacy Sandbox "alternative"

- Google proposes replacing cross-domain cookie functionality with the Google-controlled "Privacy Sandbox" private APIs. The functions include:
 - Behavioral and interest tracking
 - Attribution and frequency capping
 - Fingerprinting restrictions
- *Google is turning Chrome from a simple web browser to the gatekeeper of Google's dominant data trove and adtech stack*





CONCLUSION

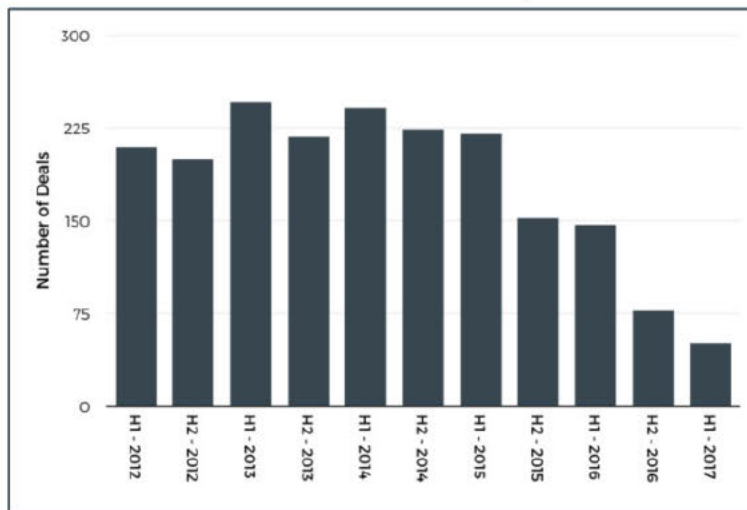


YouTube ads appear cheap if you trust Google. If not: ?

	<i>YouTube ads (measured by Google)</i>	<i>Non-YouTube video ads (measured by independent vendors)</i>
CPM (cost per thousand impressions)	\$10	\$12
# of impressions	20,000	10,000
Total Cost	\$200	\$120
Quality	90% ?	66%
On-target rate	?	90%
Brand-safe rate	?	90%
Non-fraud rate	?	90%
Viewability	?	90%
# of effective reach impressions	18,000 ?	6600
Quality-adjusted CPM (qCPM) (cost per thousand effective reach impressions)	\$11 ?	\$18

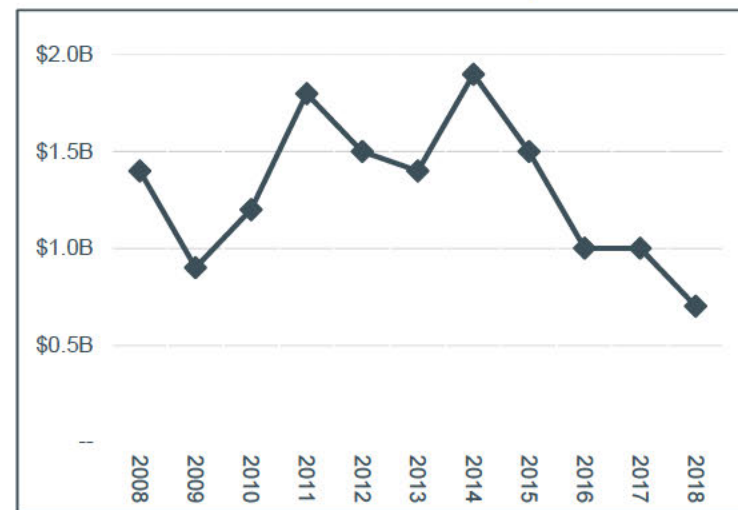
Innovation in adtech slowed as the market consolidated and VC funding dried up

VC deal count in US adtech companies



- Consolidation of adtech companies created a challenging investment environment

VC investment in US adtech companies



- Venture capital investment in adtech has declined even as programmatic spend has increased

Glossary: Key terms

Term	Definition
Ad Exchange	An online marketplace that enables advertisers to bid on placements from publishers in real time
Ad fraud	A type of online fraud where a perpetrator makes an advertiser pay for low quality and fake traffic
Advertiser Ad Server	A technology used by advertisers and media buyers to manage and track ads as they appear on publishers' website/apps
Audience	The (unique) users who visit or use a publisher's property
Attribution	The process of matching a set of user actions across touch points to determine which advertisements prompted the desired actions
Campaign	The advertising period in which an ad delivery strategy is executed
Conversions	An action that's counted when someone interacts with your ad
Cookie	Technology for recognizing a browser and recording behaviors for later re-recognition
CPM (Cost per Thousand Impressions)	The price of 1000 advertisement impressions on one webpage
Data Management Platform (DMP)	Company that provides technology to store and catalog marketer data
Demand Side Platform (DSP)	A company that provides technology for media buyers to purchase ad placements, typically via bids in exchanges' auctions
First Party Data	The information that an entity has collected about its own audience
Impressions	A metric used to measure the display of an advertisement on a web page. One impression refers to each occurrence of a user finding a webpage and loading it
Programmatic Buying	The use of technology to automate and optimize the ad buying process
Publisher Ad Server	A technology that allows publishers to easily store and manage what ads appear on their sites/apps
Real-Time Bidding (RTB)	The buying and selling of online ad impressions through real-time auctions
Third Party Data	Any information collected by an organization that does not have a direct relationship with the users the info is being collected on
Verification	The process of ensuring ads are viewable and seen by a human
Viewability	Measures the likelihood that an advertisement will be viewed and then the actual result of whether or not the advertisement was viewed
Walled Garden	A closed ecosystem where the service provider has total control over all the operations in the ecosystem

Glossary – Full (1/4)

Term	Definition
Ad Exchange	An online marketplace that enables advertisers to bid on placements from publishers in real time
Ad fraud	A type of online fraud where a perpetrator makes an advertiser pay for low quality and fake traffic
Ad Slot	The location on hosting website page where an advertisement loads
Advertiser Ad Server	A technology used by advertisers and media buyers to manage and track ads as they appear on publishers' website/apps
Attribution	The process of matching a set of user actions across touch points to determine which advertisements prompted the desired actions
Audience	The (unique) users who visit or use a publisher's property
Average Cost per Action (CPA)	The total cost of conversions divided by the total number of conversions
Avg CPV	Google's metric for YouTube that measures the average amount paid when a viewer watches 30 seconds of your video or engages with our video, whichever comes first
Awareness	Uppermost stage of the marketing funnel where prospective customers are drawn in via marketing campaigns, research and discovery
Bot	Software that performs automated tasks such web crawling. They can often be used for harmful purposes such as enabling fake ad impressions
Campaign	The advertising period in which an ad delivery strategy is executed
Complete Views	# of times a video has played until the end
Completion rate	The percentage of video impressions that played to completion
Consideration	Stage in the marketing funnel where leads are seen as prospective customers

Glossary – Full (2/4)

Term	Definition
Conversions	An action that's counted when someone interacts with your ad
Cookie	Technology for recognizing a browser and recording behaviors for later re-recognition
Cost Per Completed View (CPCV)	The price an advertiser pays every time a video ad runs through to a completion
CPC (cost per click)	The price paid by an advertiser to a publisher for a single click on the ad that brings the user to the intended destination
CPM (Cost per Thousand Impressions)	The price of 1000 advertisement impressions on one webpage
Creative	Advertisement presented to the targeted user
CTR (Click-through rate)	CTR is the percentage of people who saw an advertiser's ad and clicked on the ad.
CVR (conversion rate)	Number of conversions divided by number of impressions
Data Management Platform (DMP)	Company that provides technology to store and catalog marketer data
Demand Side Platform (DSP)	A company that provides technology for media buyers to purchase ad placements, typically via bids in exchanges' auctions
Evaluation	Stage of the marketing funnel in which buyers make a final decision about whether or not to buy a product or service
First Party Data	The information that an entity has collected about its own audience
Impressions	A metric used to measure the display of an advertisement on a web page. One impression refers to each occurrence of a user finding a webpage and loading it

Glossary – Full (3/4)

Term	Definition
Intent	Prospects have demonstrated that they are interested in buying a product
Interest	Stage after lead generation where prospective customers learn more about the company, products and information and research
Placement	The amount of ad space a publisher has available to sell to an advertiser
Lookalikes	An audience of people who are similar to an advertiser's existing customers
Measurement	The process of collecting and analyzing advertising metrics to determine the impact of a campaign
Media Buying	The process of purchasing ad inventories from publishers' websites/apps
Open Auction	Matches multiple advertisers' targeting with publishers' placement and the highest bidder wins the impressions. Any publisher or advertiser can participate in the auction and placement prices are decided in real time
Placements	The places where advertisements are run
Private Auction	Very similar to an open auction except participation is restricted to selected advertisers
Programmatic Buying	The use of technology to automate and optimize the ad buying process
Programmatic Direct	An ad transaction negotiated directly between a publisher and advertiser through automated buying systems
Publisher Ad Server	A technology that allows publishers to easily store and manage what ads appear on their sites/apps
Purchase	Last stage of marketing funnel where prospective customer decides to buy and becomes a customer

Glossary – Full (4/4)

Term	Definition
Reach	The number of users that are exposed to an advertisement
Real-Time Bidding (RTB)	The buying and selling of online ad impressions through real-time auctions
Retargeting	Using information on who has visited an advertiser's website without purchasing something to show the same visitor ads on different websites
Segments	Selections based on a set of criteria that results in a set of users whom advertisers can target
Third Party Data	Any information collected by an organization that does not have a direct relationship with the users the info is being collected on
Verification	The process of ensuring ads are viewable and seen by a human
View rate	Google's metric for YouTube that is a ratio showing the number of paid views of a video ad to the number of impressions
Viewability	Measures the likelihood that an advertisement will be viewed and then the actual result of whether or not the advertisement was viewed
Viewable Impressions	The number of impressions on the site that were viewable out of all measurable impressions
Views	# of times a viewer watches your video for 30s, or engages with your video, whichever comes first
Walled Garden	A closed ecosystem where the service provider has total control over all the operations in the ecosystem