Reset.

Ads and Kids: Loopholes in Very Large Online Platforms' Ad Managers

I

Summary

Summary

Reset examined whether Very Large Online Platforms (VLOPs) are collecting extensive personal data from users under 18 year-olds, and the extent to which this data is being used to deliver online advertising.

The audit of three ad managers—Google (which manages advertising on Youtube), TikTok, and Meta (which manages advertising on Facebook and Instagram)—focuses on two aspects: 1) from the advertisers' perspective, what are the ad networks and ad APIs of VLOPs and do they allow the possibilities of targeting minors, and 2) from the users' point of view, what kinds of age propagation take place between a third-party application and the ad network of the platforms, and how is consent gathered or inferred from the underaged users?

The research found several loopholes to circumvent bans of targeting minors:

1. Underaged targeting by age parameter selections is not completely removed from some platforms' ad managers, such as TikTok's ad manager Pangle.

2. Implicit targeting based on groups (e.g. "parent", "not a parent") or by association with interests (e.g. people who searched for "Paw Patrol" on Google) can take place through identity solution providers or through interest-based targeting on Google Ad Campaign Manager, Pangle, and Meta Ads Manager.

3. Custom target groups through the upload of data containing user profiles (e.g., MAIDs or Mobile Ad IDs, emails, phone numbers, or IP addresses) can facilitate targeting via data collected elsewhere about underaged users. Google's own policies, for example, differentiate IP addresses from identifying information. This enables showing ads to minors based on geo-location (e.g., those logged into a classroom Wi-Fi) as contextual targeting instead of personalised targeting.

4. The differentiation between commercial content and advertisement means advertisers can configure their advertising materials into commercial content and circumvent the current regulations restricting underaged user targeting.

5. Logging into apps with underaged social media accounts propagated the age to ad platforms. Platforms do not necessarily block ads if the third-party app developers do not set age restrictions or parameters.

6. Third-party partners using VLOPs' ad software development kits (SDKs) use excessive dark patterns in age verification through self-reporting and consent.

Our findings have regulatory implications, relevant under both the Digital Services Act (DSA) and the General Data Protection Regulation (GDPR), as these loopholes present risks pertaining to the collection and the use of personal data of underage users in advertising practices. To close these loopholes, regulators may consider the following course of action:

- Ban the use of inferred or proxy data for targeting: Prohibit the use of aggregated, location, household, or other proxy data to indirectly target minors with ads.
- Enforce purpose limitation under the GDPR: Behavioral ad targeting should not be considered compatible processing for data originally collected for other purposes like log in or app usage.
- Require ad transparency for minors: VLOPs should be required to provide information on why a minor is seeing a particular ad, similar to Google's "Why this Ad" functionality.
- Mandate privacy reviews of ad systems: Require VLOPs to assess data flows from apps/websites to ad systems when accessed by minors. Address flows not compliant with GDPR or DSA.
- Mandate VLOPs to exercise due diligence in selecting and monitoring third-party partners and establishing guidelines of transparent consent processes with these partners.

We plan to conduct further research into investigating particular ads that underaged sock puppet accounts are exposed to on various VLOPs through other experimental and technical methods, such as unearthing undocumented APIs.

Table of contents

II

Introduction

Introduction

The Digital Service Act (DSA) aims to offer children and young people under 18 years old additional protections in the digital sphere.

- Recital 71 states that 'the protection of minors is an important policy objective of the Union', and describes platforms as accessible to minors when:
  - Its terms and conditions permit minors to use the service
  - Its service is directed at or predominantly used by minors, or
  - Where the provider is otherwise aware that some of the recipients of its service are minors, for example because it already processes personal data of the recipients of its service revealing their age for other purposes.

- Recital 84 explains that in assessing systemic risk—which includes risks to minors—"providers of very large online platforms and of very large online search engines should focus on the systems or other elements that may contribute to the risks, including all the algorithmic systems that may be relevant, in particular their recommender systems and advertising systems, paying attention to the related data collection and use practices."

- In addition, Article 34 places additional requirements on VLOPs and very large online search engines to assess the risks their services pose to children's rights. Specifically, Article 34(1)(d) DSA requires VLOPs to undertake risk assessments, including "any actual or foreseeable negative effects in relation to [...] minors." Article 34(2)(b) DSA explicitly states that algorithmic recommender systems, content moderation systems, enforcement of terms and conditions, and advertising systems be considered.

This report explores VLOPs' compliance with the requirements outlined in these recitals and articles around advertising systems.

This report is part of a series where we test various platform systems and processes for compliance with the DSA, including:

- Content moderation systems
- Algorithmic recommender systems
- Understandability of the platform for younger users
- Safety-by-design settings
- Ad manager systems

III

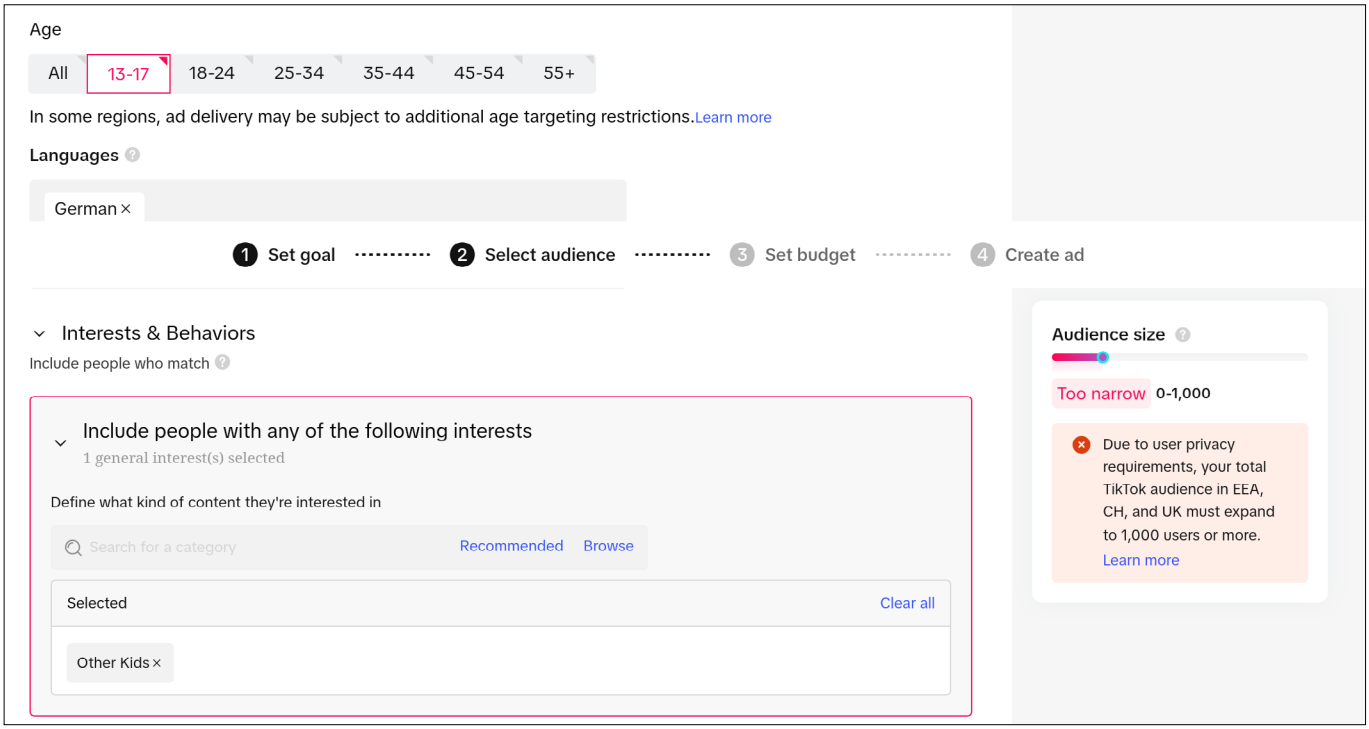
Loophole 1: Existing Age Parameters in VLOP Ad Managers

Loophole 1: Existing Age Parameters in VLOP Ad Managers

Explicit underaged targeting by selecting age categories 13–17 is not possible on Meta Ads Manager and Google Ad Campaign Manager. However, TikTok ad and data collection options present risks.

TikTok Ads

ads.tiktok.com is the platform for the ad buy side of TikTok. Brands, Shops and other buyers can configure their ads and choose a target group. Targeting minors is not completely removed from the dashboard, even if both the age group and the „Games/Kids/Other Kids" group are shown empty (i.e. it is not possible to target either of these groups). The option 13-17 on the dashboard is present for several EU countries as well as for the UK.[1] This means age-related data are still being collected from EU countries for 13- to 17-year-old users. However, the ad delivery may be interfered with based on different regions' targeting restrictions.



1 The list contained: Austria, Belgium, Czech Republic, Denmark, Egypt, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Kuwait, Morocco, Netherlands, Norway, Poland, Portugal, Qatar, Romania, Saudi Arabia, South Africa, South Korea, Spain, Sweden, Switzerland, Turkey, Ukraine, United Arab Emirates, United Kingdom.

Pangle

Pangle is the sell-side SDK from TikTok which enables other app developers to earn money by offering ad space. Pangle states it can deliver ads to users under 12 years old if the content is suitable on its global facing knowledge center. This does not necessarily mean Pangle allows running ads to under 13-year-olds or minors between 13 and 17 years old within the EU. Further testing using Pangle advertising accounts or using underaged sock puppet TikTok accounts will be needed.

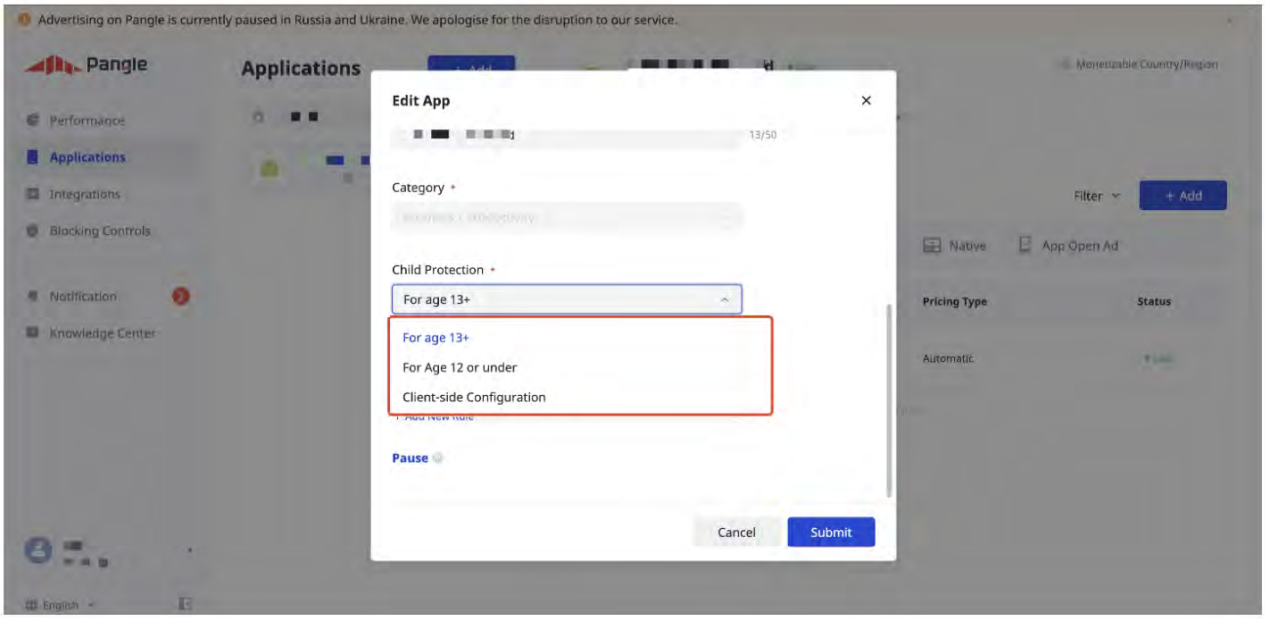
- "For Ages 13 and Above":

With this setting, any requests may be exposed to ads that are intended for users aged 13 and above, and the developer will takes full responsibility for any exposure of immature users to ad content that is rated for ages 13+.

- "For Ages 12 and Under":

The platform will only deliver ads that are intended to be viewable by children.

(Please note that your eCPM will therefore be affected.)



Weak or no enforcement of age and data protection checks

Pangle offers several parameters that can be set to prevent ads form being delivered to kids or without consent. When the Pangle SDK is initialised, the parameters "child", "GDPR" and "CCPA" can be set. Here is a table showing the meaning of the parameters, obtained from the handbook and the class com.bytedance.sdk.openadsdk.api.init.PAGConfig:

Official SDK Name	JSON variable	"0" means	"1" means
PAGChildDirectedType	coppa	adult	child
PAGGDPRConsentType	gdpr	User doesn't grant consent	User has granted the consent
PAGDoNotSellType	ccpa	"sale" of personal information is permitted	user has opted out of "sale" of personal information

In the source code (e.g., com.bytedance.sdk.openadsdk.api.PAGConstant), in default they are set to "-1" so advertisers need to manually indicate the parameter for each variable. If coppa is set to "1", an error will appear and no ads will be shown to indicate Pangle does not facilitate ads targeting children.

However, Pangle allows advertisers to not set these parameters of age protection or consent status. For example, **these parameters are not enforced while the region of the user is set to be in Amsterdam (likely by timezone)**. They are also not enforced **when the GDPR switch is still not set** (i.e., it stays "-1"). When the parameters do not clearly indicate child protection or consent status, the configurations are nevertheless accepted by Pangle and ads are visible in the app. App makers can thus maximise revenue by not setting the parameters and still run child-related ads without barriers from Bytedance.

Age verification in child-related apps containing Pangle SDK

To prove the low enforcement of age verification in apps containing Pangle SDK from TikTok, a randomly chosen list of 20 apps with the SDK using the Exodus Privacy database was audited. These apps are largely such that can be deemed to be of interest to minors, such as gaming apps.

Number	App handle	Age verification?
01	com.h8games.handicraft	Asking if age is over 16
02	com.kwalee.objecthide	No
03	com.BeautifullyMadeGames.ThePresident	No
04	jp.nanameue.yay	Yes (delivering ads anyway, but didn't check if this is related to Pangle)
05	com.happykamp.aquariumland	Asking if age is over 16
06	com.lyrebirdstudio.cartoon.face	No
07	com.oneway.Deathcoming	No
08	com.game.JewelsStar	No
09	com.playcus.findthedifferences2	No
10	com.playspare.shapeshifting	No
11	com.bestringtonesapps.oldphoneringtones	No
12	com.xplay.pop_antistress_simulator	No
13	com.superclay.freecashknight	No
14	com.wordgame.puzzle.block.crush.de	No
15	com.StaffanEkvall.CarpetBombing2	No
16	com.starwavenet.memestar.gp	No
17	com.vector.game.puzzle.numberlink	No
18	net.wellyglobal.led.flashlight.torchlight.colorlight.pro	No
19	com.ezt.monster.playground	No
20	com.funcell.perfectlie	Asking if age is over 16 (using several dark patterns)

This audit underlines that ad SDKs in general, and Pangle in particular, do not force the app creators to implement or use age checks of any kind.

Usage time and used apps data collection

In addition, out of all the data harvested from underaged users, consent may not be explicitly obtained for certain metrics that are then usable as an API parameter on Pangle. For example, Pangle is collecting the usage time of apps through TikTok. This data feed may be then used to create the interest targeting that is available via the TikTok ad-selling platform (ads.tiktok.com) (see Appendix I: TikTok Collection of Duration of Use).

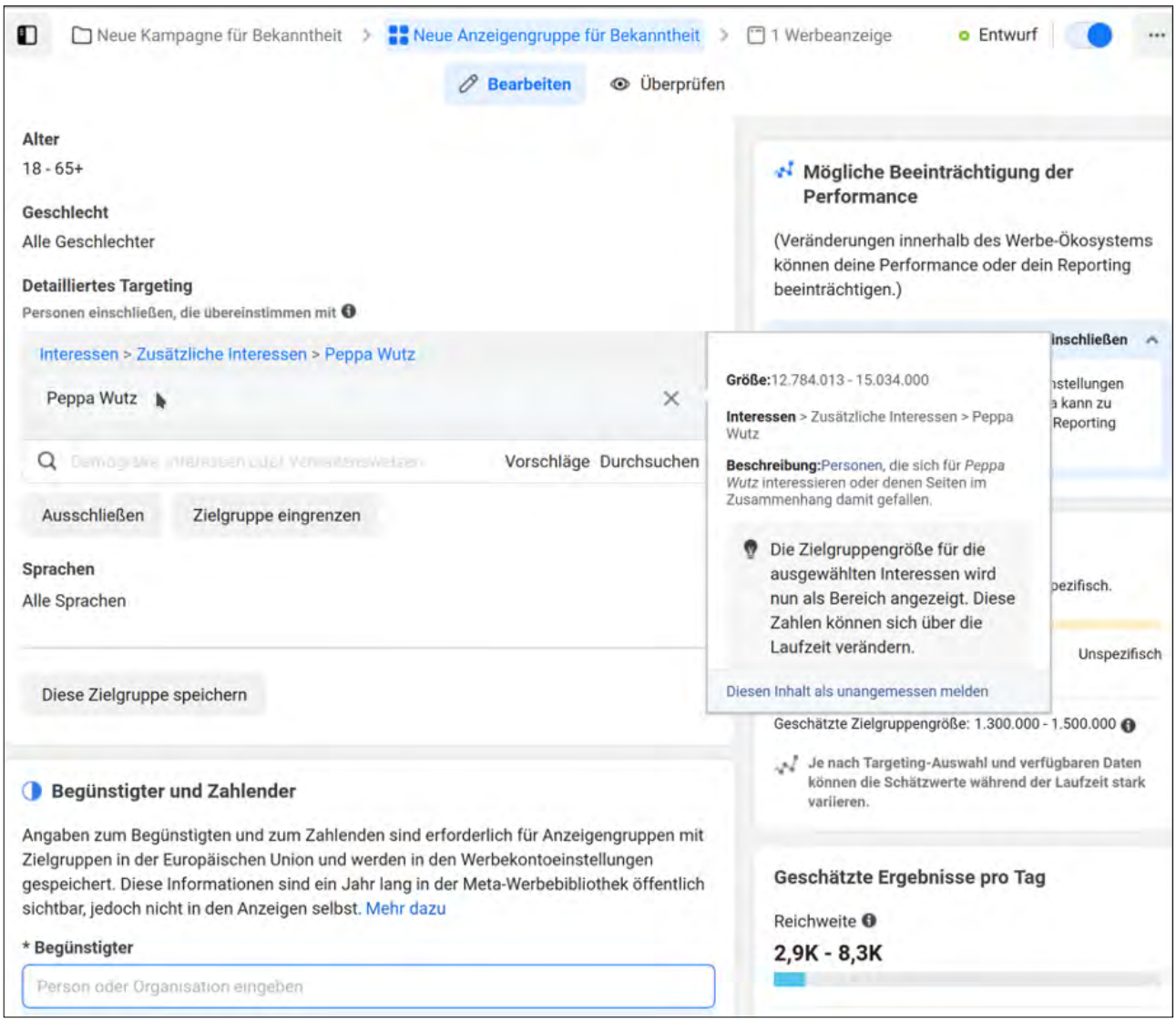
IV

Loophole 2: Implicit Targeting Based on Groups and Associations

Loophole 2: Implicit Targeting Based on Groups and Associations

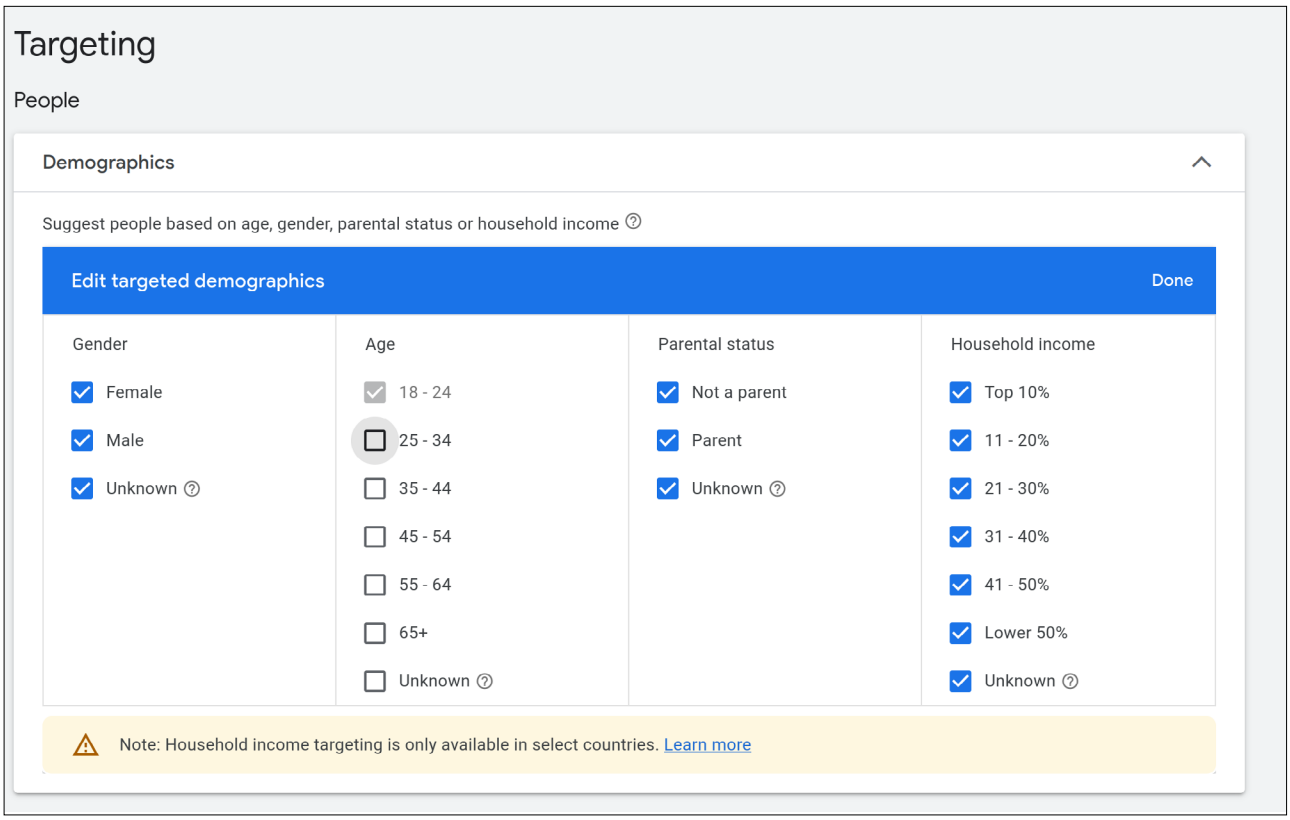
Some common forms of targeted advertising are based on device IDs or website cookies, or based on IP addresses in households. Even if the IP of a household changes, some identity solutions partners such as Lotame can update the login data and make it available to advertisers choosing to use VLOP ad SDKs. Because devices in households can be used by more than one person, some identity solution companies have technologies in place to differentiate single users within one household or even device, e.g. by recording usage patterns. This is also why the above-mentioned collection of app usage duration and patterns can be used to differentiate between users on one device.

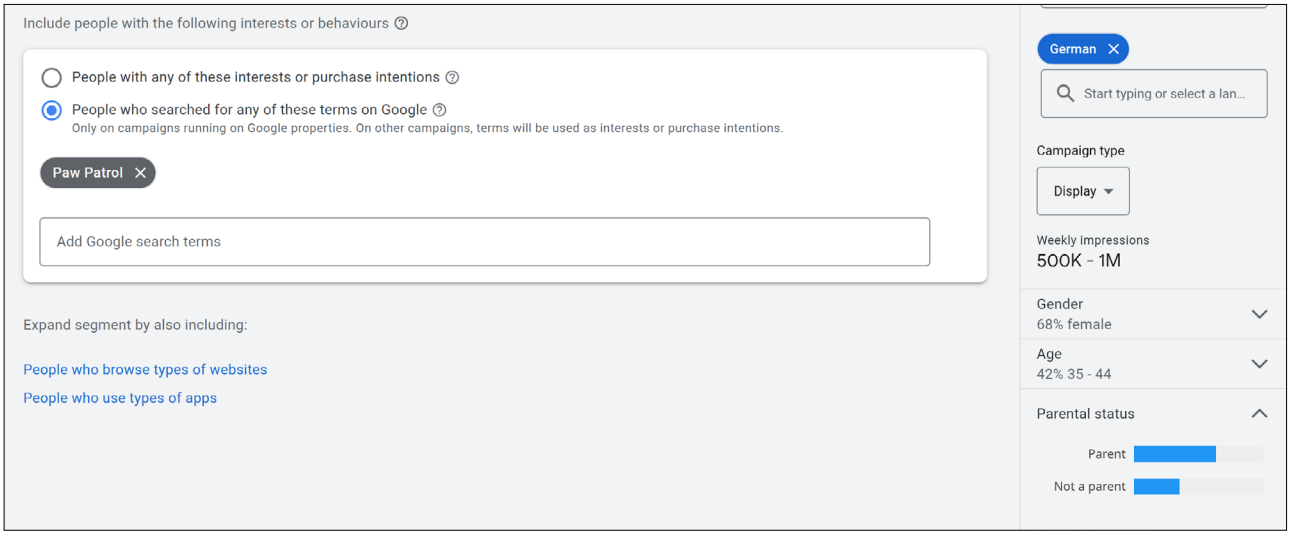
The "parent", "child" or "not a parent" grouping is available in many VLOPs' ad managers or SDKs as targeting segments. The grouping can also be combined with other interests. Such an option is available on Meta ads manager (see below a screenshot of German Facebook accounts with an interest in "Peppa Pig"), TikTok's ad buy manager (ads.tiktok.com), and on Google Ads. On TikTok, for example, a good chance for having kids in the target group would be to select "Watched Videos/Entertainment/Anime" and "Comic Interest" and to combine this with interests like "Games/Dress up" and "Lifestyle."



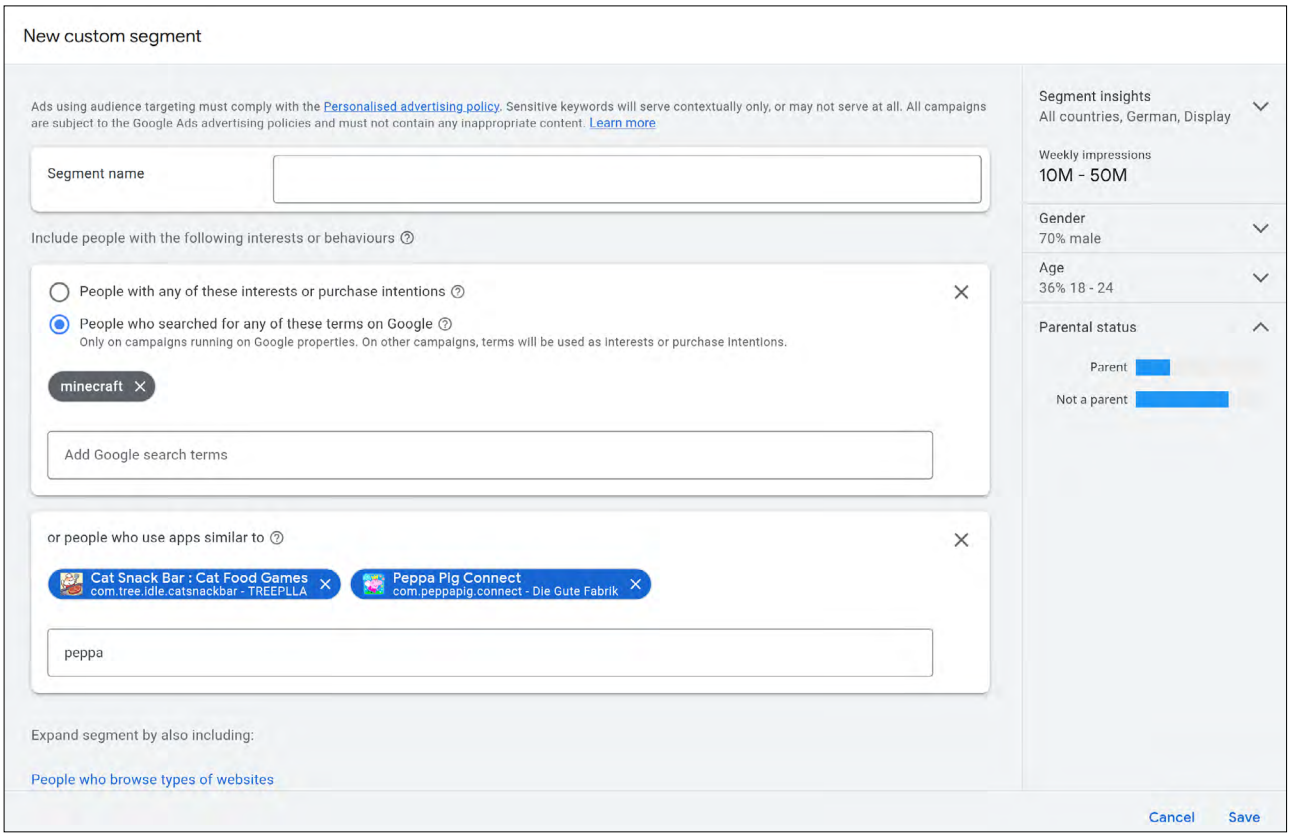
Another illustrative example: The screenshot of Google Ads parameters below indicates a target group of German-speaking data subjects that searched for "Paw Patrol" on Google. The parental status then differentiates between "Parent" and "Not a parent". While "Not a parent" does not necessarily mean the user is underage, the search term likely aligns with the interests of underaged users, and the fact that kids can often consume content using the devices of their parents or grandparents, the advertisers for Paw Patrol merchandise can rely on these grouped targeting segments to:

1. Target parents searching for child-related content, which does not fall under the risk of targeted advertising to children;
2. Target children watching child-related content on parents' devices;
3. Target some children through "Not a parent" status, especially those that falsified their age during the age verification step on platforms in order to access content.

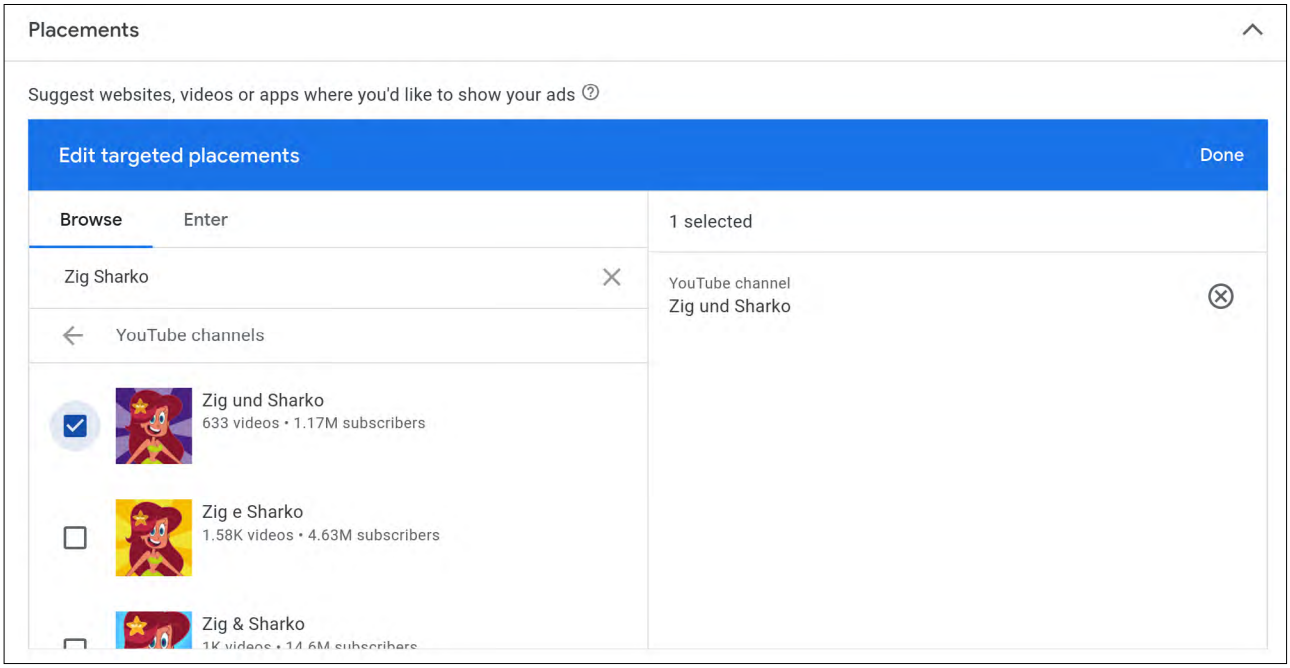




The ad targeting tool from Google Ads not only allows advertisers to select from certain demographics and categories but also allows them to freely search by unlimited keywords or according to app usage. It is therefore easy to target children. For example, we combined users who searched for Minecraft, a popular video game, with users who used a little-known gaming app called Cat Snack Bar and a more popular one called Peppa Pig App. The segment then produced mostly "Not a parent" users.



Additionally, Google allows for targeting based on child-related websites, YouTube channels, and single YouTube videos. It is even possible to target using websites similar to the German children-only TV channel KiKa. KiKa is distributed by a public broadcaster and does not include any ads or tracking embedded from Google. However, targeting based on its website can nevertheless be done by other data collected by Google, such as DNS data from Android devices, search history on one's search engine, or data collected when using the Google Chrome browser.



As long as it is allowed to target based on child-related content, parental status as a grouping, or search histories and other behavioral data collected that can be approximated for age, the age restriction in targeted advertising is not working effectively to protect children.

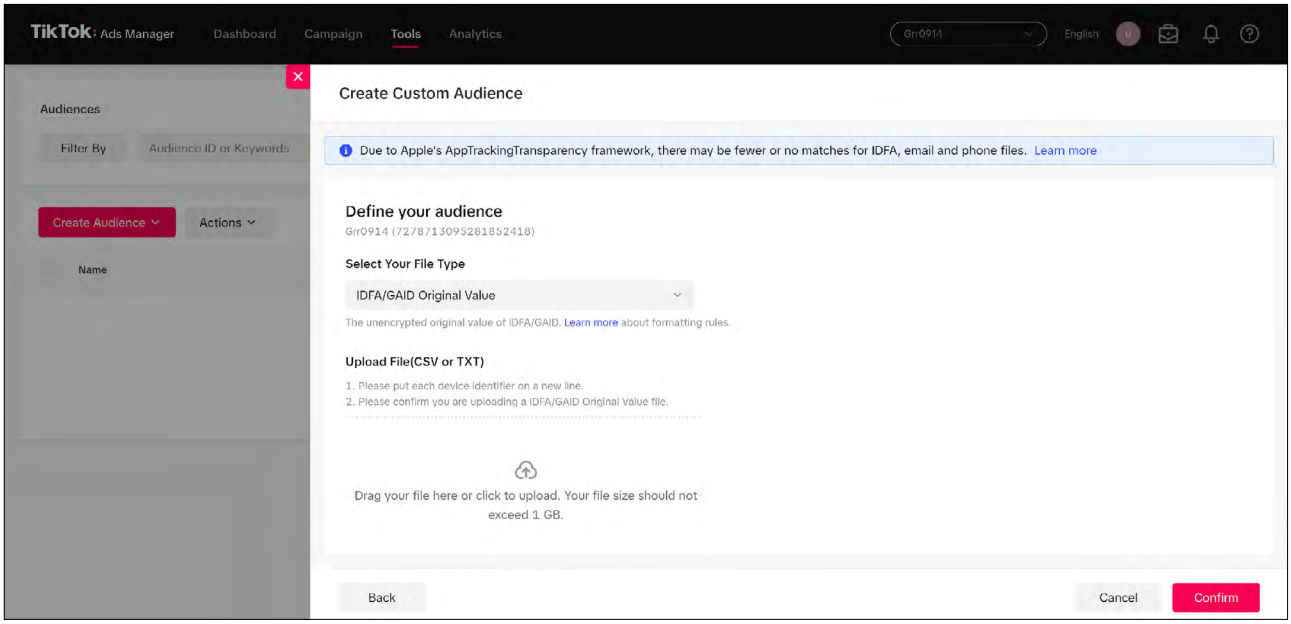
V

Loophole 3: Custom Target Groups Based on Data Collected Elsewhere

Loophole 3: Custom Target Groups Based on Data Collected Elsewhere

VLOPs with an ad network allow for the creation of custom target groups by uploading user data such as MAIDs (Mobile Ad IDs), email addresses, phone numbers, or IP addresses. In this way, target groups can be built not only after direct interactions between an advertiser and a visitor or an app user, but also from hundreds of companies that collected large amounts of targeting data. Most of them are able to filter for age and/or interests, across huge marketplaces. For example, the Polish company OAN specialises in offering gaming-related IDs likely containing many underaged users. Therefore, targeting can be done completely outside of the VLOPs' ad manager targeting options, simply by importing a list of MAIDs into the dashboard.

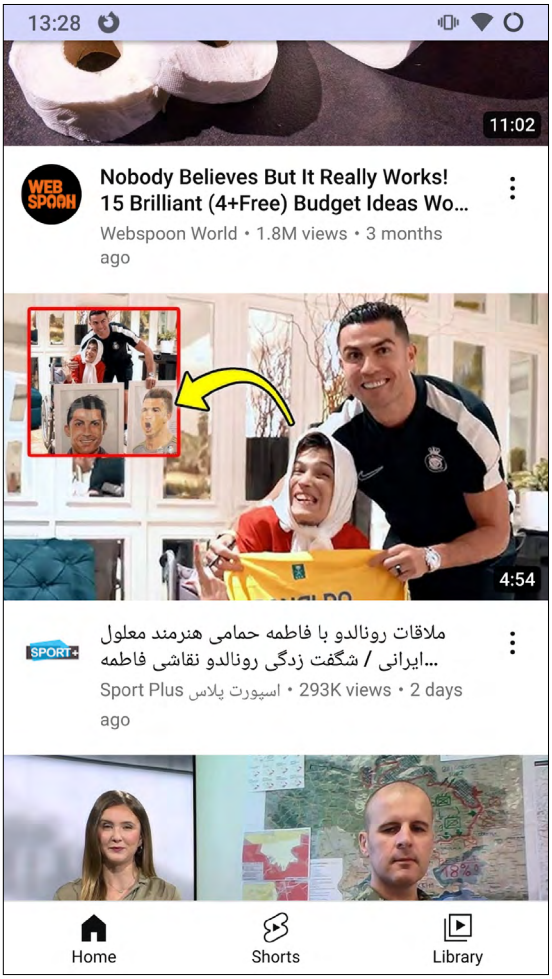
As VLOPs are not serving ads to accounts on their platforms that belong to under-18-year-olds, this loophole affects the group of minors who have indicated a higher age when creating an account with the VLOPs. They can then be targeted externally based on their real age, which has been collected elsewhere, despite their falsified account age registered with the VLOP.

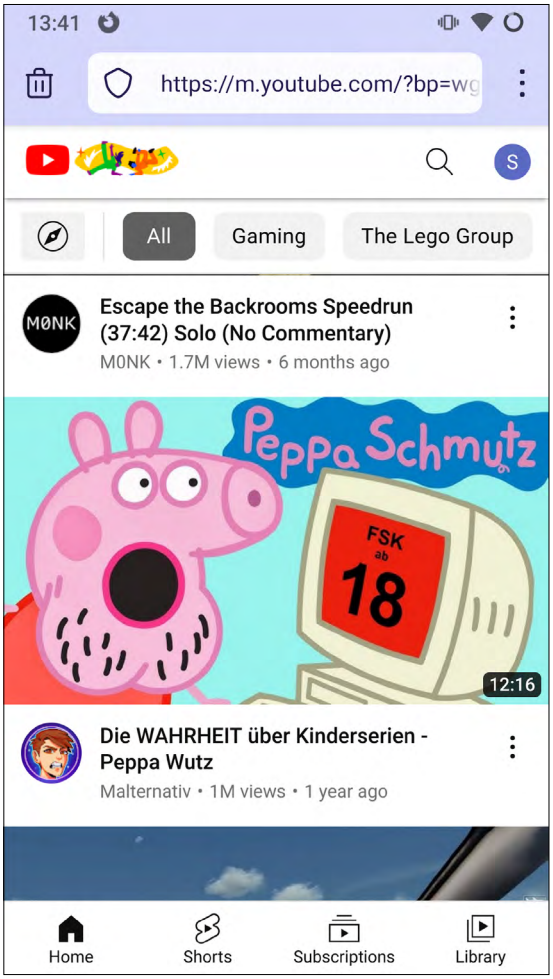


Case study: Google's aggregated data and location targeting

While testing with the Google account of a 16-year-old, we received the statement that Google would not be personalising the ads. While it is true that the ads had no connection to the search history and the activity of the individual, there were a striking amount of ads that were evidently linked to previous household activities. This may indicate that Google is targeting households even if ad personalisation for a particular account—in this test case an underaged sock puppet account—is deactivated. Technically, if the IP address changes, the household can still be connected to past behavioral data if just one household member is using any sort of Google login (e.g., for Android, Chrome, Youtube, or Gmail). Also, the link between login data and IP addresses can be bought from several ID providers like Lotame's Panorama ID.

A member of our research team discovered that despite using YouTube with a test phone and a sock puppet account for the first time, YouTube suggested a Persian-language video. Another device active at the same IP address had a view history of Persian-language videos. This suggestion disappeared after the sock puppet account "watched" several German language videos. At the same time, suggestions of Peppa Wutz (Peppa Pig) videos on the sock puppet account on the test phone can be connected to prior research in this audit that searched for Peppa Pig/Peppa Wutz.





To further test the algorithmic targeting, which allows content-based targeting to carry over to any newly registered accounts at the same IP address, we compared 15 ads shown to the 16-year-old sock puppet account with ads shown while using a proxy IP address without logging into an account.

New underaged YouTube account created at the same IP address

We primed the 16-year-old YouTube sock puppet account that has ad personalisation deactivated to watch mostly teenage influencers and gaming content. The ads shown by YouTube did not reflect these interests but prior interests from the view histories of other accounts with the same IP address.

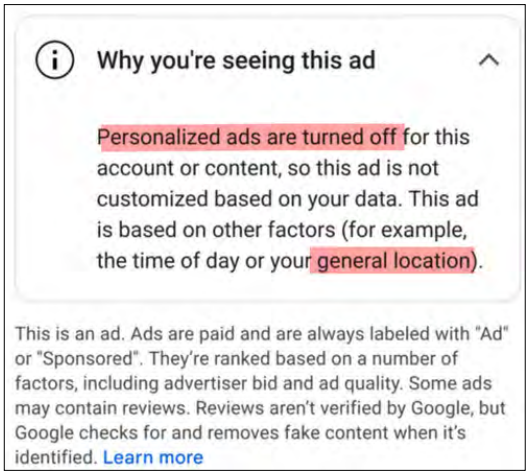
Ad topic	Connection with activities at the same IP adress	Explanation
B2B eco power from Vattenfall	High	One account with the same IP address is interested in building a solar panel, visited Vattenfall website and installed its app.
Energy efficiency	High	One account with the same IP address is working in the energy efficiency sector, sometimes from home.
Solar Panel	High	One account with the same IP address is interested in building a solar panel.
Job offer	Medium	One account with the same IP address is looking for a job, but not in this field.
B2B Power from Vattenfall	High	Second ad, slightly different content, see above.
UTA Business Fuel Card	High	One account with the same IP address was researching EV charging cards and downloading several apps, including competing business carfleets.
ESG for german businesses	High	One account with the same IP address is working in the energy efficiency sector and stated that ESG (Environmental, Social and Governance) is one of the main concepts of the work.
Energy efficiency	High	Second time, see above.
Solar Panel	High	Second time, see above.
European pallet	Low	
European pallet	Low	
Rollei photo backpacks	Low	
Golfing in Northeim	Low	
B2B Power from Vattenfall	High	Third time, see above.
Sas Viya Analytics	High	One account with the same IP address is researching analytics software.

Using Youtube with a proxy IP without an account

Using YouTube with a private SSH proxy, we primed YouTube without creating an account by watching mostly random football videos. The ads shown in this case mostly had no connection with prior activities at the same IP address.

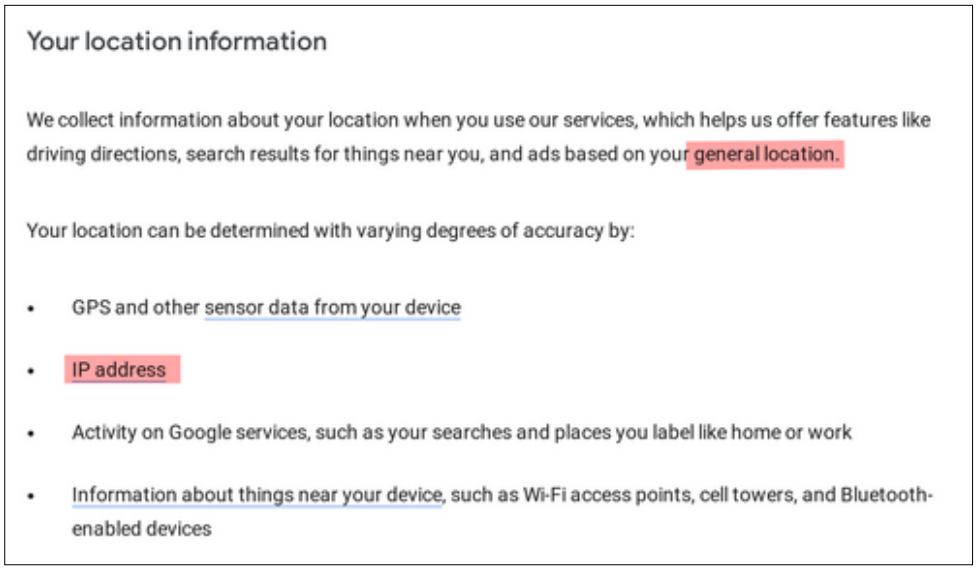
Ad topic	Connection with activities at the same IP adress	Explanation
Google Pixel 7a	Low	
Tango Therapy	Low	
Job Ninja	Medium	One account with the same IP address is looking for a job.
Climate responsible construction	High	One account with the same IP address is working in the energy efficiency sector, sometimes from home.
Job in medical care	Low	One account with the same IP address is looking for a job, but not in this field.
Funny games for you	Low	
Cosmetics	Medium	One account with the same IP address is interested in cosmetics
Garden fence painting	Low	
Money back from your health insurance	Low	
Job Ninja	Medium	Same ad, second time
Kid tooth paste	Low	
Renting an aerial work platform	Low	
Gadget Store	Low	
Job in medical care	Low	Same ad, second time

According to Google, "turning off ad personalization" turns off individual customization in a narrow sense: it only applies to the personal or unique ID of one individual, but not to the targeting of a "general location" (see below screenshot of "Why you're seeing this ad").



Aggregate data as the data collection and ad targeting around GDPR

"General location" may sound unspecific or broad but IP addresses, according to Google, fall under this term. Even though IP addresses shared by several accounts may not be a personal identifier as names or birthdays are, "personalised ads" that target social media accounts of 13- to 17-year-olds become possible via geo-locating where the respective IP address hosts underaged users. Even if the IP addresses get constantly updated, if one account reconnects by personal login data at the new IP address, data collected from the old IP address may still be used to some extent in targeted ads.



Your location information

We collect information about your location when you use our services, which helps us offer features like driving directions, search results for things near you, and ads based on your general location.

Your location can be determined with varying degrees of accuracy by:

- GPS and other sensor data from your device
- IP address
- Activity on Google services, such as your searches and places you label like home or work
- Information about things near your device, such as Wi-Fi access points, cell towers, and Bluetooth-enabled devices

Because Google considers IP addresses as "general location" or "additional context", Google rejects that household tracking data is a relevant consideration under the GDPR. What logically follows is that Google's policies allow household targeting enabled by IP address tracking since it considers this kind of targeting different from targeting users' demographic or personal information, such as during age-based targeting.

This stance implies that obtaining consent would not be necessary for compliance with the GDPR where IP addresses are used to target households and individual users—some possibly underage-–in those households. For further background information on aggregated data and how they enable companies to stay GDPR-compliant while targeting clusters of users, please see Appendix II: Further background: The shell game trick of aggregated data.

Furthermore, it raises the question of the consequences of including GPS, Wi-Fi access point signals, and Bluetooth-enabled devices in the "general location" targeting instead of individual ad targeting. This means that locations such as youth centers, classrooms, or school areas could be part of a "general location" even if the individuals at these places are not using the youth centers' or schools' Wi-Fi. For example, when two or three minors in a class are frequent players of a gaming app that advertises using Google Ads, Google may target all the other kids in the class or even the whole school based on their "general location" and will still argue that this isn't targeted advertising just because it did not use the three unique IDs from the minors playing the game in the first place.

As a result, as long as Google is able to "single out" minors as part of a certain household, school, friend gathering, or other general location, the advertisers using Google Ads can effectively target these "general" locations. Further studies should to be done using sock puppet accounts with a school's IP address or using the school's WiFi.

A challenging next step for regulators and legislators will be to draw the line between aggregate group data and context data since Google has already drawn that line for itself. Will device information and language settings be considered context or personal data? Is there a line between geo-location based on IP addresses from context (e.g., Germany-based IP) to personal data (connecting to the classroom Wi-Fi)?

VI

Loophole 4: Distinction between Commercial Content and Ads

Loophole 4: Distinction between Commercial Content and Ads

Marketing practices now engage multiple outlets of monetization beyond official channels of traditional advertisement, and marketers profit from a business practice where it is increasingly difficult to distinguish ads from other social media content. While these practices may not be officially supported by the VLOPs' advertising policies, they nevertheless exist and indirectly drive activities on the platforms and, thereby, increase revenue for the VLOPs and their official partners.

Influencer marketing, for example, includes paid content without content being labelled as advertisement. The audience demographics of verified influencer accounts can be obtained from VLOPs on request, which means advertisers can identify influencers with the largest amount of underaged followers and involve these influencers in unofficial ad campaigns, product placements, and other forms of surreptitious advertising.

Companies like Phylly, a "data gateway to access creator-data directly from the source platforms", can help identify influencers with an above-threshold amount of followers of a specified age group, which can include minors. Below is an example from Phyllo's API documentation showing that capability:


```
"gender_age_distribution": [
  {
    "gender": "FEMALE",
    "age_range": "13-18",
    "value": 12.3[2]
  }
```


It is unclear for which VLOPs exactly Phyllo is able to deliver these follower demographics or whether it can perform these parameter selections in the EU, so further investigations to surface influencer marketing campaigns API use should be conducted.

2 "Value" indicates the percentage value of demographics from the selected group.

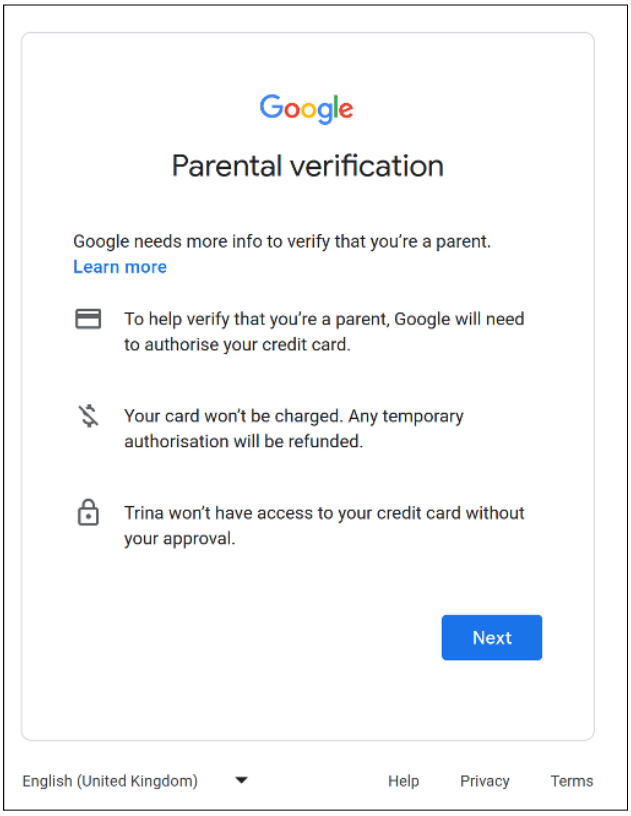
VII

Loophole 5: Age Propagation between Apps

Loophole 5: Age Propagation between Apps

Age propagation involves the age information given based on consent to one app or platform being propagated into ad managers or third parties using VLOPs' ad SDKs in their apps without further request for explicit consent. We found that, in the case of Google, login data from Google Android accounts is propagated to the Google Ad SDK and all third parties using the SDK in their apps. In the case of Meta, there is no evident age propagation between Meta accounts and its ad SDK.

If a user aged 13 tries to create an account, Google asks for the account details of the parents and authorises the account by phone number and Google account of the parent. Additionally, the parents must share their credit card details with Google to create the Google Account (see screenshot from the sign-on process below). This rigid check may lead to account creation with a falsified age to circumvent credit card verification, which makes enforcement actions on the VLOPs' handling of underaged accounts difficult.



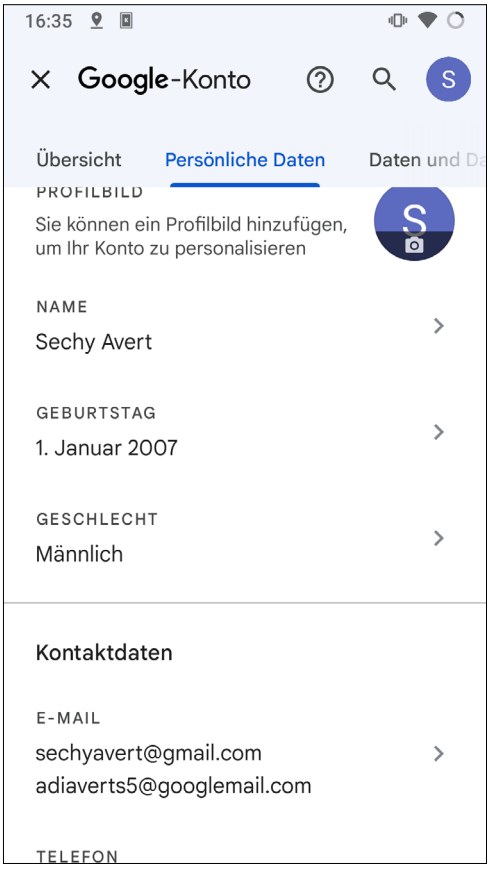
However, creating an account for a 16-year-old individual is possible without parental verification. The Android account can subsequently install and use several third-party apps that contain the Google Ad Mob SDK:

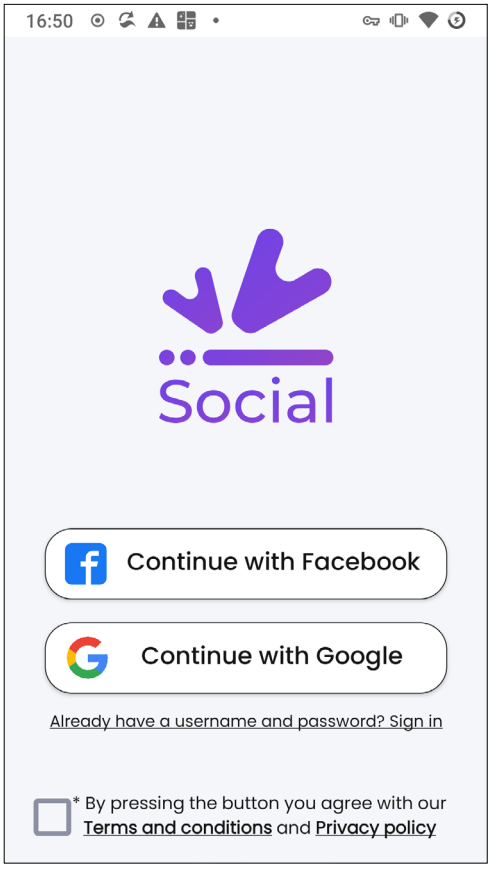
- Mathe Wiki (de.lakdev.mathewiki).
- Kleines Klavier (com.lemon.baby.piano.kids)
- Freestyle (com.lyricspiration.freestyle)

In this case, the age and targeting settings in Google Ads are automatically propagated to the SDK in the third-party apps, which poses a risk of the underaged Google accounts being targeted. This is especially risky when Google Ads cannot block ads if the third-party app developers do not set age restrictions but, instead, simply create custom target groups based on the age information propagated from the underaged Google accounts.

For Facebook, we searched for an app meeting the following requirements: 1) uses Facebook Login functionality, 2) does not have its own age check, 3) serves ads, and 4) does not have too many ad SDKs included so it is more likely to be served ads from Meta.

However, this combination is uncommon and the search abilities at Exodus Privacy still do not allow for a combination of settings (e.g., Facebook Login SDK and a low amount of other SDKs). Grivvy Social is the only app that meets all four criteria.





The 16-year-old Facebook sock puppet account is used for login, and consent to the Terms and Conditions and Privacy Policy per GDPR is given. The Grivvy Social app uses several monetization SDKs that auction ad space in the app, one of which is the Meta Audience Network. Unfortunately, we did not observe any ads coming from the Meta Audience Network.[3] This is likely because Grivvy Social integrates numerous ad parameters from so many partners that advertisers from Facebook were not winning any auctions.

3 An ad-related request was recorded from Meta's Ad Network SDK after we logged into the 16-year-old sock puppet account but it could be interpreted as an ad auction request. The recorded request and server response are included in Appendix III - Meta Ad Network SDK request in case further interest arises on this point.

VIII

Loophole 6: Dark Patterns in Age Verification by Third-Parties Using VLOPs' Ad SDKs

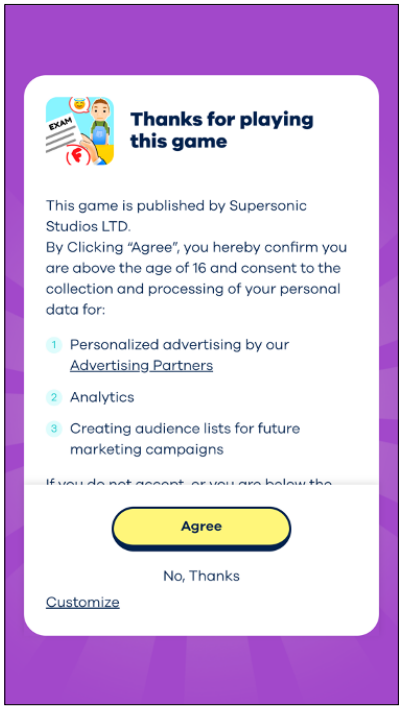
Loophole 6: Dark Patterns in Age Verification by Third-Parties Using VLOPs' Ad SDKs

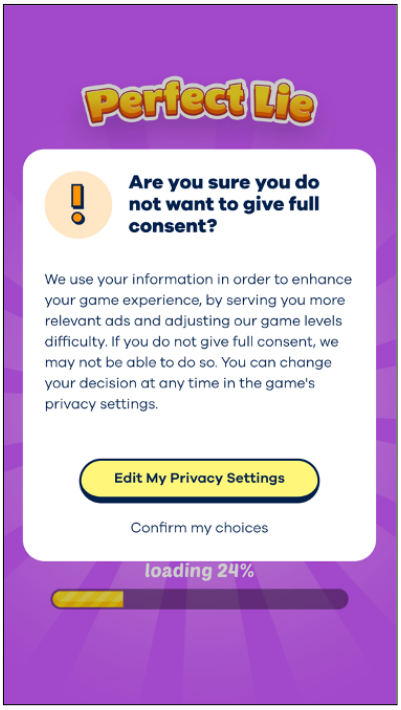
In our separate research piece on the risk of dark patterns—"An Evaluation of Understandability of Very Large Online Platforms for Young Users, Including Dark Patterns"—we investigated the presence of manipulative dark patterns during the new account creation process for four VLOPS. According to the typology, there are six major dark patterns:

1. Inferring consent by clicking next;
2. Obscuring important details;
3. Presenting options that may not be in a user's best interests as a 'better user experience';
4. Visual promotion of options that are in a platform's best interests, while demoting options that are in the users' best interests;
5. Presenting options that are in users' best interests as temporary;
6. Click twice for no, but only once for yes.

In this study on ad targeting of minors, we focused on the age verification process of third-party partners that use VLOPs' ad SDKs. Most age checks in the audit of third-party partners of VLOPs' ad SDKs used elaborate dark patterns. A typical example is from the gaming app Perfect Lie (com.funcell.perfectlie):

- **Obscuring important details:** The age question is buried in the texts with other consent questions; the heading "Thanks for playing this game" does not clarify what the user is agreeing to by clicking the "agree" button, and the text is too long to be visible without scrolling down.
- **Visual promotion of options that are in a platform's best interests, while demotion of options that are in users' best interests:** The "Agree" button to giving consent is in large yellow highlighted button, while "No, Thanks" is less prominent.
- **Click twice for no, but only once for yes:** After denying consent by selecting the smaller button "No, Thanks", the user is prompted to "reconsider" with the "Edit My Privacy Settings" prominently displayed. This means to not give consent for using age information for advertising and analytics, the user has to choose both times the less prominent choices in the pop-up window.





The problem with such dark patterns in the case of underaged users is that they can easily gloss over these consent details in favor of quickly creating an account so that they can experience the game. The design of these dark patterns enables third-party tools to use VLOPs ad SDKs to circumvent the platforms' non-targeting of underaged users by creating a loophole for their own ad practices (e.g., custom target group based on the underaged users who consented to personalised advertising) with so-called "consent."

X

Appendix I: TikTok Collection of Duration of App Use

Appendix I: TikTok Collection of Duration of App Use

[API_Monitor]
{
"category": "JSON",
"class": "org.json.JSONObject",
"method": "put",
"args": "[\"stats_list\",\"<instance: java.lang.Object, $className: org.json.JSONArray>\"]",
"returnValue": "{\"stats_list\":[{\"ad_sdk_version\":\"5.3.0.4\",\"app_version\":\"1.0.71\",\"timestamp\":1694076340,\"conn_type\":1,\"appid\":\"8085960\",\"device_info\":{\"os\":1,\"model\":\"SM-G900F\",\"vendor\":\"samsung\",\"package_name\":\"com.tree.idle.catsnackbar\",\"ua\":\"Mozilla\/5.0 (Linux; Android 11; SM-G900F Build\/RQ3A.211001.001; wv) AppleWebKit\/537.36 (KHTML, like Gecko) Version\/4.0 Chrome\/113.0.5672.163 Mobile Safari\/537.36\",\"gaid\":\"\"},\"type\":\"general_label\",\"error_code\":0,\"event_extra\":\"{\\\"starttime\\\":1694074071,\\\"endtime\\\":1694076340,\\\"start_type\\\":1}\",\"duration\":\"2269\"},{\"ad_sdk_version\":\"5.3.0.4\",\"app_version\":\"1.0.71\",\"timestamp\":1694075838,\"conn_type\":1,\"appid\":\"8085960\",\"device_info\":{\"os\":1,\"model\":\"SM-G900F\",\"vendor\":\"samsung\",\"package_name\":\"com.tree.idle.catsnackbar\",\"ua\":\"Mozilla\/5.0 (Linux; Android 11; SM-G900F Build\/RQ3A.211001.001; wv) AppleWebKit\/537.36 (KHTML, like Gecko) Version\/4.0 Chrome\/113.0.5672.163 Mobile Safari\/537.36\",\"gaid\":\"\"},\"type\":\"settings_request\",\"error_code\":0,\"event_extra\":\"{\\\"result\\\":1,\\\"http_code\\\":200,\\\"request_size\\\":1103,\\\"response_size\\\":6883,\\\"total_time\\\":1811,\\\"is_hit_cache\\\":1,\\\"abtest_ver\\\":\\\"71503311\\\"}\"},{\"ad_sdk_version\":\"5.3.0.4\",\"app_version\":\"1.0.71\",\"timestamp\":1694079440,\"conn_type\":1,\"appid\":\"8085960\",\"device_info\":{\"os\":1,\"model\":\"SM-G900F\",\"vendor\":\"samsung\",\"package_name\":\"com.tree.idle.catsnackbar\",\"ua\":\"Mozilla\/5.0 (Linux; Android 11; SM-G900F Build\/RQ3A.211001.001; wv) AppleWebKit\/537.36 (KHTML, like Gecko) Version\/4.0 Chrome\/113.0.5672.163 Mobile Safari\/537.36\",\"gaid\":\"\"},\"type\":\"settings_request\",\"error_code\":0,\"event_extra\":\"{\\\"result\\\":1,\\\"http_code\\\":200,\\\"request_size\\\":1098,\\\"response_size\\\":6883,\\\"total_time\\\":1839,\\\"is_hit_cache\\\":1,\\\"abtest_ver\\\":\\\"71503311\\\"}\"}]}",
"calledFrom": "com.bytedance.sdk.openadsdk.c.a.j.b(OverSeaEventUploadImpl.java:8)"
}

XI

Appendix II: Further Background: The Shell Game Trick of Aggregated Data

Appendix II: Further Background: The Shell Game Trick of Aggregated Data

"Aggregated" or "group" data is a clever trick similar to the shell game. To confuse legislators and authorities, companies like Google or Deutsche Post mix the data of one individual with n others. This way the meaningfulness of the data could be watered down. What is overseen by many DPOs in this personal data shell game is that the strong tie between the individual and the new statistical behavioral data of the group remains intact.

In theory, the mixing can be done randomly. Then the behavioural data of one specific group will quickly approximate the average patterns from all other groups that have been built from an available dataset of individuals. While this method may have some privacy advantages, the connection with the properties of the full dataset (e.g. neighbourhood, nationality) also stays intact and will still be classified as personal data in case the goal of the data processing is to "single out" an individual from, for instance, individuals outside of the dataset (see Recital 26 GDPR). As this random mixing does not provide any advantage over demographic targeting, it is not used in targeting advertising.

What ad targeting relies on instead, while still not very common, is to group individuals that are similar to each other in some form. For example, the Deutsche Post circumvented the Data Protection Office by using household clusters called microcells: The behavioral patterns of one individual are clustered with ~6.6 other households from the same building or surrounding houses. For example, if an incoming data point states that one individual just bought a specific car brand, Deutsche Post can move this information to the microcell level. The ~ 6.6 households of a microcell are then addressable by letterbox advertising as "likely owners" of this car brand. Socioeconomically, the individuals inside these small clusters still have a strong similarity, which stays meaningful enough to have a better targeting value than a spray-and-pray campaign. Needless to say, Deutsche Post still knows which individuals are in the microcell, otherwise, it could not post letters.

The efforts of several Google Privacy Sandbox proposals like FLEDGE, FloC and Topics API were even more focused on building meaningful groups: The goal is always to group people with as much similarity as possible, based on similar behaviors or interests.

This trick should not make any legally meaningful difference, even if it is helping companies circumvent existing regulations: In direct targeting, a company ties the label "bought a car" to one individual. In group or aggregated data it ties the label "probably bought a car" to one individual. As long as it is possible to single out an individual from others who "didn't probably buy a car," it should qualify as personal data.

XII

Appendix III: Meta Ad Network SDK request

Appendix III: Meta Ad Network SDK request

POST https://www.facebook.com/adnw_sync2 HTTP/1.1
Content-Type: application/x-www-form-urlencoded;charset=UTF-8
Accept-Charset: UTF-8
user-agent: Dalvik/2.1.0 (Linux; U; Android 11; SM-G900F Build/RQ3A.211001.001) [FBAN/AudienceNetworkForAndroid;FBSN/Android;FBSV/11;FBAB/com.givvysocial;FBAV/9.8;FBBV/87;FBVS/6.12.0;FBLC/deu]
Host: www.facebook.com
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 3067

URLEncoded form

payload:
{"request":{"prefetch_urls":"fill","bidder_token_info":"fill","feature_config":"update"},"bundles":{"feature_config":{"fingerprint":null}},"context":{"COPPA":"false","APPBUILD":"87","ID_CACHE_TS_MS":"-1","KG_RESTRICTED":"false","RTF_FB_APP_VERSION":"445612530","VALPARAMS":"{\"is_emu\":\"false\",\"apk_size\":\"30198401\",\"timezone_offset\":\"3600000\",\"app_started_reason\":\"LAUNCHER_FOUND_API21\",\"is_debuggable\":\"false\",\"debug_value\":\"N\\\\VA\",\"build_type\":\"N\\\\VA\"}","UNITY":"false","APPNAME":"Givvy Social","SESSION_TIME":"1696257958.591","REQUEST_TIME":"1696258561.051","CARRIER":"","SDK_CAPABILITY":"[3,4,5,7,11,16,17,18]","CLIENT_REQUEST_ID":"88fc7eef-830e-4556-be69-c58721c809fb","DENSITY":"3.0","AD_REPORTING_CONFIG_LAST_UPDATE_TIME":"0","SCREEN_HEIGHT":"640","SDK_VERSION":"6.12.0","SDK":"android","OSVERS":"11","ANALOG":"{\"total_memory\":\"1785765888\",\"accelerometer_y\":\"0.49799395\",\"rotation_x\":\"-0.01917476\",\"accelerometer_x\":\"-0.02813187\",\"accelerometer_z\":\"9.346365\",\"charging\":\"1\",\"available_memory\":\"404131840\",\"rotation_z\":\"-0.03089267\",\"rotation_y\":\"-0.007456851\",\"battery\":\"75.0\",\"free_space\":\"2585120768\"}","ASHAS":"f9129bf15552b9afe463f94ad6819cad34197df2;","IDFA":"","ATTRIBUTION_ID":"","RTF_FB_APP_INSTALLED":"true","APPVERS":"9.8","DATA_PROCESSING_OPTIONS_COUNTRY":"null","INSTALLER":"com.android.vending","DATA_PROCESSING_OPTIONS_STATE":"null","CAPPED_IDS":"[]","ACCESSIBILITY_ENABLED":"false","HAS_EXOPLAYER":"true","AFP":"29549a939d0a004b24bb008cae571d26","PLACEMENT_ID":"","MAKE":"samsung","TEMPLATE_ID":"0","SCREEN_WIDTH":"360","ID_SOURCE":"NO_GMS","APP_MIN_SDK_VERSION":"21","OS":"Android","DATA_PROCESSING_OPTIONS":"null","ROOTED":"1","MODEL":"SM-G900F","FUNNEL_CORE_EVENTS":"4101,4146,4127,4106,4123,4104,4411,4412,4410","FUNNEL_LOGGED":"false","BUNDLE":"com.givvysocial","LOCALE":"deu","NETWORK_TYPE":"1","IDFA_FLAG":"0","SESSION_ID":"856f0539-e100-4162-97a7-c590e536a1d4"}}

Server Response

HTTP/1.1 200 OK
Vary: Accept-Encoding
Content-Encoding: gzip
report-to: {"max_age":259200,"endpoints":[{"url":"https:\/\/www.facebook.com\/ajax\/browser_error_reports\/"}]}, {"max_age":3600,"endpoints":[{"url":"https:\/\/www.facebook.com\/ajax\/browser_error_reports\/"}],"group":"network-errors"}
content-security-policy: default-src data: blob: 'self' https://.fbsbx.com 'unsafe-inline' *.facebook.com *.fbcdn.net 'unsafe-eval';script-src *.facebook.com *.fbcdn.net 'unsafe-inline' blob: data: 'self' 'unsafe-eval';style-src *.fbcdn.net data: *.facebook.com 'unsafe-inline';connect-src *.facebook.com facebook.com *.fbcdn.net wss://*.facebook.com:* wss://*.fbcdn.net attachment.fbsbx.com blob: *.cdninstagram.com 'self' android-webview-video-poster: http://localhost:3103 wss://gateway.facebook.com wss://edge-chat.facebook.com wss://snaptu-d.facebook.com wss://kaios-d.facebook.com/ *.fbsbx.com;font-src data: *.facebook.com *.fbcdn.net *.fbsbx.com;img-src android-webview-video-poster: *.fbcdn.net *.facebook.com data: https://*.fbsbx.com facebook.com *.cdninstagram.com fbsbx.com fbcdn.net blob: *.oculuscdn.com;media-src *.cdninstagram.com blob: *.fbcdn.net *.fbsbx.com www.facebook.com *.facebook.com data:;frame-src *.facebook.com *.fbsbx.com fbsbx.com data: *.fbcdn.net;worker-src blob: *.facebook.com data:;block-all-mixed-content;upgrade-insecure-requests;report-uri https://www.facebook.com/csp/reporting/?m=c&minimize=0;*
document-policy: force-load-at-top
permissions-policy: accelerometer=(), ambient-light-sensor=(), bluetooth=(), camera=(self), geolocation=(self), gyroscope=(), hid=(), idle-detection=(), magnetometer=(), microphone=(self), midi=(), payment=(), screen-wake-lock=(), serial=(), usb=()
cross-origin-resource-policy: same-origin
nel: {"report_to":"network-errors","max_age":3600,"failure_fraction":0.01}
cross-origin-opener-policy: same-origin-allow-popups
Pragma: no-cache
Cache-Control: private, no-cache, no-store, must-revalidate
Expires: Sat, 01 Jan 2000 00:00:00 GMT
X-Content-Type-Options: nosniff
X-XSS-Protection: 0
X-Frame-Options: DENY
Strict-Transport-Security: max-age=15552000; preload
Content-Type: text/html; charset="utf-8"
X-FB-Debug:
NgNeT3e+FpIoEcxkFFZqsqILgTHp/SR8aZfzZmCnkBI9fg4UmMBT5kuaz3ocQcgimt3ZBHH/tVZ21Jl0BGMkYw==
Date: Mon, 02 Oct 2023 14:56:00 GMT
Alt-Svc: h3=":443"; ma=86400
Transfer-Encoding: chunked
Connection: keep-alive
[decoded gzip] XML

{"response":{"prefetch_urls":"keep","bidder_token_info":"keep","feature_config":"full"},"bundles":{"feature_config":{"data":{"feature_config":{"adnw_modules_sync_enabled":"false","adnw_modules_no_pii_sync_enabled":"false","adnw_enable_sync":"false","adnw_sync_after_ad_load":"false"}},"fingerprint":null}},"refresh":{"target_refresh_s":300}}