Tyler Bowers
October 15th, 2022

Advertising Espionage

A case study on how digital advertising has changed the way that companies collect and share data.

Introduction

The digital age represents a fundamental change in the way that companies can see potential customers. Online advertising has quickly become the most dominant form of advertising, as its reach is now comparatively unmatched. Digital advertising revenue is predicted to grow from $521B in 2021 to $876B in 2026; a ~%70 increase in just 5 years (Statista, 2022). Its quick evolution has resulted in a business model that closely monitors consumers and that many would consider crossing the line of privacy. The amount of data available shadows traditional marketing techniques. As much as 80% of Google's revenue comes from advertising in 2021 (Alphabet 2022) and Google makes up ~28.6% of this market. Additionally, the top 5 advertisers in the market made up ~67% of the market, refer to the pie chart in appendix 3 for a visual representation of market share. We need to consider and ask the question of just how much control companies should have over our data. If we don't, we risk an age of a privatized big brother. The collection of sensitive consumer data should be regulated due to its manipulation of consumer purchasing habits and lack of transparency to the public.

Summary of Current Advertising Environment

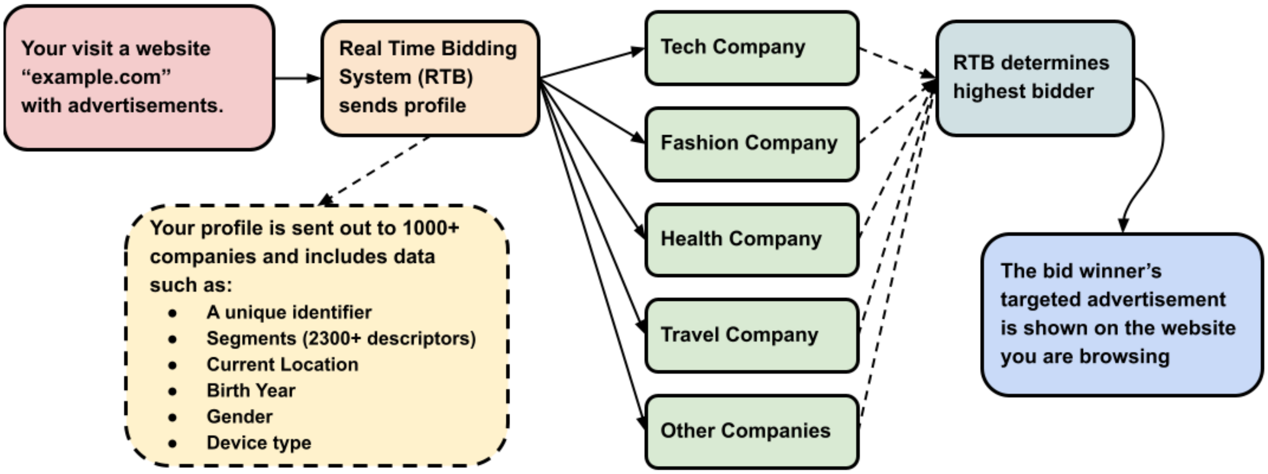
Before the digital age, advertising first came in the form of print media where companies would place ads in the local newspaper and hope that potential customers would see their ads, this was an indirect form of advertising. On the other hand, direct advertising would use the mail to directly communicate with customers, the Sears Roebuck catalog in the late 1800s was one of the first forms of this (Sears, 2012). Though many companies stayed away from this since it was expensive. The analog age came next where advertising took the form of the radio and eventually television. This new medium sparked the "Golden Age of Advertising" (Joshi 2022) where companies revised their advertising and heavily invested in radio/tv time. Many years later the internet arose and as more people adopted the new technology, advertising quickly followed. Post dot-com bubble Yahoo instantiated the pay-per-click model rather than display ads. And when it comes to full online businesses, getting your word out is especially important otherwise, people will just forget that you exist. With the launch of smartphones, digital advertising experienced a significant increase in its reach. Up to this point, it was hard to completely narrow down your target audience, but what if every advertisement could be custom matched to you through an algorithm, this is called *surveillance-based advertising.*

Surveillance advertising is its own new medium that has become the dominant form of advertising today. Surveillance advertising collects personal data to be used as a tracker of your habits. This data allows companies to see trends with your interaction with their ads and allow them to pick you out from the crowd. And no wonder why, having all this data could drive sales beyond what traditional marketing is good at. After all, advertising is not effective if a company cannot reach its target audience.

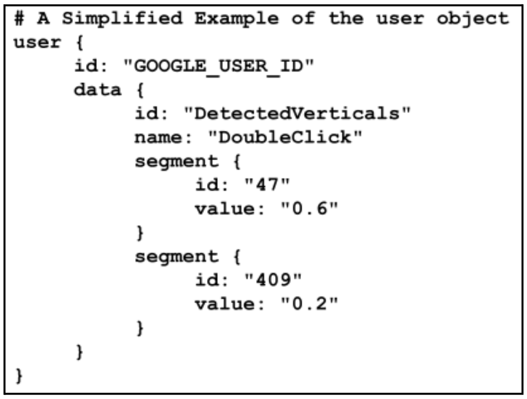
Why do you think that you see ads for products on your phone that you were looking at on your computer just moments ago. Or if you were searching for dog food earlier in the week and now you are seeing ads for dog toys. The process is the same whether you are visiting from a different device or website. Unless you are truly disconnected, you have no way of avoiding being tracked. Advertising's connection to your life is undeniable just as it is to at least 85% of people who own smartphones (Pew Research, 2021). The majority of U.S. Adults are concerned about *how the data is collected* (81%) or *used* (79%) and they believe that they have a *lack of control* (81%) over their own personal data. (Pew Research, 2019). Connecting all of this information about an individual requires a ton of data, so how is it recorded?

How is this Data Collected and Shared?

Both the Interactive Advertising Bureau (IAB), Google and many other companies use a process called "Real Time Bidding" (RTB). Real Time Bidding can be looked at like an auction where "digital advertising inventory is bought and sold" (Google, n.d.) , hence "bidding", and the process takes only a couple hundred milliseconds, hence "real time". When you open a website with Google ads or with OpenRTB ads, then your profile is sent out to the RTB service. Your profile can include information such as your location, current site, gender, device, year of birth, IP address, an ID string and a collection of segments; remember, this data is sent to all of the advertising companies, meaning that they can all see this data. A study estimated that on average your “online activity and location [is] exposed 747 times every day” (ICCL, 2022) and in Europe the number per day is on average 376 times. The most disturbing part of the data sent is the segment object since there are more than 2300 possible values that it can hold, these are used to uniquely target certain customers or specific markets. The importance of segments in RTB cannot be understated since they lead to “increased advertiser-audience match quality, and in turn increased value per-clicks and bid prices from advertisers” (Quin et al., 2016). The process of real time bidding is simple, it starts when you open a website that contains ads with RTB. Your profile is then sent to the bidding market where companies check your profile (segments) to see if it has elements that match what they are looking for, they then enter a bid amount based on the strength of the match to their model by using an algorithm. If their bid wins then their ad gets displayed on the website that you are currently visiting. Here is a visualization the process that happens in less than a second:


Your visit a website “example.com” with advertisements.
Real Time Bidding System (RTB) sends profile
Your profile is sent out to 1000+ companies and includes data such as:
• A unique identifier
• Segments (2300+ descriptors)
• Current Location
• Birth Year
• Gender
• Device type
Tech Company
Fashion Company
Health Company
Travel Company
Other Companies
RTB determines highest bidder
The bid winner’s targeted advertisement is shown on the website you are browsing

So what are the “segments” and what is their importance? The openRTB 2.6 documentation describes the segment in section 3.2.22 as “key-value pairs that convey specific units of data. The parent data object is a collection of such values from a given data provider” (OpenRTB 2021). The data object is contained within the user object (3.2.20) that contains information such as a unique identifier for each individual. Even using a VPN (or even TOR) cannot protect you if you are signed into your account since your unique identifier is carried with your account. The data object within the user object contains an id, name, value, and ext. The id and name are both specific to the data provider, so if it is Google then the data provider would be “DoubleClick” (an advertisement company acquired by google in 2008) this would also be known as the supply-side platform (SSP). The value part is what contains the segments. A segment will contain an id and a value, the id integer corresponds to a category such as (47) “Autos & Vehicles” or even as far as (409) “Right-Wing Politics”. You can find all of the official ids for Google[1] or for IAB[2] as well as sorted versions of these that highlight the odd ids by Brave Browser[3] [4] online. Appendix 1 includes a list of interesting categories that people could be grouped into. The value included with the id is the strength of this measurement which is used in tandem with the advertiser’s models to set the bid amount.



```
# A Simplified Example of the user object
user {
     id: "GOOGLE_USER_ID"
     data {
          id: "DetectedVerticals"
          name: "DoubleClick"
          segment {
               id: "47"
               value: "0.6"
          }
          segment {
               id: "409"
               value: "0.2"
          }
     }
}
```

The strength (value) of these segments are generated by “cookie-based big data analysis” (Quin et al., 2016). So for example, Magnite’s privacy policy states that “when you visit a Digital Media Property that uses our technology, we collect certain information about you and your device” (Magnite 2022). They do note that they can’t fully identify a person (i.e. your name) but they do collect many identifiers that can single you out and track you with a uid (unique identifier). The data that they collect can be the topics of what you are looking at, your activity on the website (dates & times, search keywords, general location), browser information (type, language, or history), and device information (such as IP address, device characteristics, or the ISP you are visiting from). There are many more areas of information collected that can be found in Magnite’s privacy policy[5].

[1] Google’s Segments: https://developers.google.com/authorized-buyers/rtb/downloads/publisher-verticals

[2] IAB’s Segments: https://www.iab.com/wp-content/uploads/2017/11/IAB_Tech_Lab_Content_Taxonomy_V2_Final_2017-11.xlsx

[3] Brave browser’s marked up version of Google’s Segments: https://brave.com/static-assets/files/Google-publisher-verticals-marked-up.pdf

[4] Brave browser’s marked up version of IAB’s Segments: https://brave.com/static-assets/files/IAB-taxonomy-v2-marked-up.pdf

[5] Magnite’s privacy policy: https://www.magnite.com/legal/advertising-technology-privacy-policy/

So who is all this data shared to? The main companies that the data is shared with are partners of the companies that place ads on websites. The largest of these companies that use RTB are Google (DoubleClick), PubMatic, Magnite, BidSwitch, Xandr and the list continues (ICCL 2022). Each one of these companies has partners that they share data with using RTB. Only a few of them disclose their partners: Xandr (Microsoft) shares data with up to 2050 companies (Xandr 2022). Google only discloses companies based in the "European Economic Area (EEA) and UK" to be compliant with GDPR (General Data Protection Regulation), meaning that they share data with at least 1071 companies, the Irish Council for Civil Liberties (ICCL) estimated that Google shares data with ~4700 companies in the US. The data recipients could be local or "sent to firms across the globe, including to Russia and China" (ICCL 2022). Many would consider this a serious breach of privacy since the user has no control and little knowledge of all their data being shared. All of this data is used to send highly tailored and targeted advertisements back to websites based on your own advertising profile.

Negative Effects of Surveillance Advertising

While most of real-time bidding data is just general categories (though some may find any data collection of this type a breach of privacy) there are several negative effects that RTB can have on consumers. Two reasons against RTB (or reasons to regulate it) are that the data can be used for manipulation and that it lacks transparency/ privacy for users of RTB-based sites.

Manipulation can be performed on certain groups of individuals with certain characteristics that match each other. Surveillance advertising allows companies to sift through subjects and narrow them down based on a weighted algorithm. Normal advertising would only be able to place ads in locations that are generalized such as cooking product ads after a cooking show on tv. RTB allows a company to extend its reach and further narrow down a specific target audience. Manipulation's effects are certainly issues for vulnerable customers. Some examples of exploiting vulnerable people could include marketing beauty products to people with low self images, a category for this in Google's segments is #437 /Health/Mental Health or marketing dieting products or gym memberships to the overweight which could use the segment

#818 /Health/Health Conditions/Obesity. While it is probably not the intention, many of these categories could allow these manipulative ads through. Additionally, some of the segment categories could go against Google's own policy. Google's "personalized advertising content policy principles" (Google 2022) notes several categories that restrict the type of ads that can be shown but they still provide the categories of data. Some examples of this are categories #409 and 410 (right & left wing politics) which go against "Political affiliation in personalized advertising" and categories #862-869 (Religion & Belief) which conflict with their rules of "Religious belief in personalized advertising". Appendix 2 contains an extended list of segments that provide data for types of advertisements that would not follow Google's content policy. Again, why provide the data for it if that type of ads aren't allowed? Manipulation using RTB could be akin to automated exploitation of consumer vulnerabilities for profit.

Lack of transparency is inherently hard to find since consumers knowing about the amount of data collected on them would be scary. The information collected about you is held by the advertising facilitators and a bit by the browser. With Google you can request data on your profile[6]. In particular, the section that stores all of your history can be downloaded in the "My Activity" selection, it includes your history for all google products. Yes, this includes all of your browser history. If you thought that you can just delete it in browser settings then you are wrong. Google actually stores all of your browser history, when you "delete" it in your browser you are actually just clearing the local instance. This data also contains history for youtube searches, image searches, and 26 other items. My history went back to 2013 and was 311 MB in size, my google search history was 149MB alone and remember that that is text data. It is true that Google does disclose that they collect this data but not that many people really know this since they don't read the terms of service. We have reached an age where we can have privacy but consent is dead because people are bombarded with requests to agree with terms of service and privacy policies. Google as well as other advertisers can generate segments based on this information which is then sold to companies via RTB. This data is then used for research and to provide personalized ads for an individual. If privacy is known as the freedom from intrusion, then the way that Google

[6] https://takeout.google.com/

handles this data could be considered a massive breach of personal privacy. There is also an issue with where the data is sent. A report by the ICCL notes that: “Europeans and U.S. Internet users’ private data is sent to firms across the globe, including to Russia and China, without any means of controlling what is then done with the data.” (ICCL, 2022). Sending all of this information about consumer habits to international countries is a security risk since it could give them ways of influencing public opinion though targeted advertisements. To many people as well as the ICCL this amount of data sharing could be considered “the biggest data breach” (ICCL, 2022).

Potential Solutions

Real time bidding has brought up many issues with the privacy of consumer data, especially in the areas where it can have negative effects. A total ban is not necessarily needed, rather, some form of regulation should be used to disallow the collection of some types of data. There is currently no single law that protects against data collection in the US, rather there is a collection of laws at the federal and state level that protect privacy rights. The Federal Trade Commission Act only has a small section for false advertising, nothing in the document relates to data privacy and advertising. Other laws like FERPA, HIPAA, COPPA are for family educational privacy, health insurance privacy, and children’s online privacy, there are no laws protecting online data collection, tracking and data sharing.

The European Union does have laws that protect data privacy. Known as “General Data Protection Regulation” or GDPR, this regulation’s aim was to unionize data privacy laws in the EU and the idea was that personal data privacy should be regarded as a basic human right. Since its initialization its has handed out over 1400 fines totaling more than € 2,000,000,000 with many of the largest fines sent to Amazon, Meta, WhatsApp, and Google (GDPR Enforcement Tracker). It has seven key principles that affect the processing of personal data: “lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality (security), accountability” (Information Commissioner Office [ICO], 2018). A simplification for each one of these principles can be found in appendix 4. Some of the most important parts of these main points are “data minimisation” where only necessary data should be collected, and “storage limitation” where personal data should only be kept for as long as it needs to be. These could both conflict with the amount of data that Google keeps and for how long they keep it.

Of course, the story in the US is much different as there are no current laws that protect data collection and data sharing rights. However there was a bill recently introduced in both the House and Senate that is advocating for a complete ban on surveillance advertising (Banning Surveillance Advertising Act [BSAA], 2022). This bill would “restrict online advertising that targets an individual, internet-connected device, or group of individuals or devices based on personal information” (BSAA). An important section of this document is that it would disallow providing an advertiser / third party with a “unique identifier that may be used to identify an individual or a connected device” (BSAA). This would effectively eliminate the ability of an external party to single out an individual. Any violation of this act would be “treated as a violation of a rule defining an unfair or deceptive act or practice under section 18(a)(1)(B) of the Federal Trade Commission Act”. While this bill does bring the idea of data privacy to the surface it might be a bit too egregious. A complete ban could have unintended consequences as it could cause serious damage to the $500B+ industry (Statista, 2022). Many of the biggest companies in the US depend on this type of advertising for a majority of their profit, i.e. we don't have to pay for any of Google's services. There is also an issue with its effect on commerce; if companies cannot as effectively reach their target audience then there will also likely be a hit on ad engagement therefore decreasing purchases. Due to these facts alone, it is extremely doubtful that the bill will pass. It would be much better to take an approach more like GDPR where there are restrictions and transparency requirements rather than an outright ban.

Conclusion

The digital age has allowed data collection on an unmatched scale. Previously companies relied on ads that could only be placed in general areas that would have a broad reach. Surveillance-based advertising allows companies to easily read out and precisely market to groups of individuals through expansive data collection which many would consider a serious breach of privacy. Real-time bidding changes the way that advertising companies can see their target audience, it allows them to single out an individual based on a unique identifier and segment data. Segment data separates users into categories, or segments, based on information that has been collected on them over time; for Google alone there are more than 2300 different segments some of which give data for ads that Google doesn’t allow themselves. There is one recently introduced bill in the House of Representatives and Senate that aims for an outright ban on surveillance-based advertising (Banning Surveillance Advertising Act of 2022). However, a complete ban could have unintended consequences so it might be in best interest to take an approach more like the European Union. The EU passed GDPR, a regulation that promotes transparent and safe handling of private data. Since then more than 1400 fines have been issued for GDPR noncompliance (GDPR Enforcement Tracker). While the amount of tracking will likely not get much worse, it's important to ask how much privacy do we want to keep?

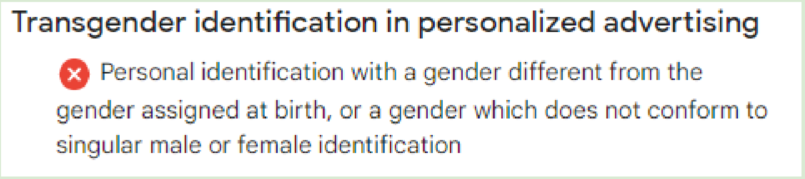
Appendix 1: List of Interesting and potentially dangerous categories

- Full List: https://developers.google.com/authorized-buyers/rtb/downloads/publisher-verticals
- There are many more than shown on this list.

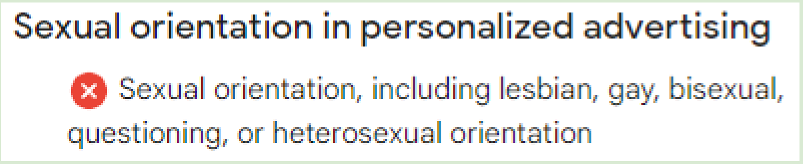
- 257 /Health/Substance Abuse
- 409 /News/Politics/Right-Wing Politics
- 410 /News/Politics/Left-Wing Politics
- 420 /Health/Health Conditions/Skin Conditions
- 429 /Health/Health Conditions/Cancer
- 437 /Health/Mental Health
- 571 /Health/Health Conditions/Eating Disorders
- 623 /Health/Aging & Geriatrics
- 639 /Health/Mental Health/Anxiety & Stress
- 640 /Health/Mental Health/Depression
- 818 /Health/Health Conditions/Obesity
- 819 /Health/Health Conditions/Pain Management
- 975 /People & Society/Religion & Belief/Skeptics & Non-Believers
- 976 /People & Society/Social Issues & Advocacy/Reproductive Rights
- 1127 /People & Society/Social Issues & Advocacy/Poverty & Hunger
- 1220 /Beauty & Fitness/Cosmetic Procedures
- 1235 /Health/Substance Abuse/Steroids & Performance-Enhancing Drugs
- 1236 /Health/Reproductive Health/Sexual Enhancement
- 1237 /Health/Substance Abuse/Smoking & Smoking Cessation
- 1238 /Health/Alternative & Natural Medicine/Cleansing & Detoxification
- 1239 /Health/Alternative & Natural Medicine/Acupuncture & Chinese Medicine
- 1251 /People & Society/Religion & Belief/Scientology
- 1262 /Health/Health Conditions/Infectious Diseases/Parasites & Parasitic Diseases
- 1434 /Finance/Credit & Lending/Debt Collection & Repossession
- 1437 /Finance/Credit & Lending/Loans/Personal Loans/Short-Term Loans & Cash Advances

Appendix 2: List of segment categories that potentially go against Google's own policy

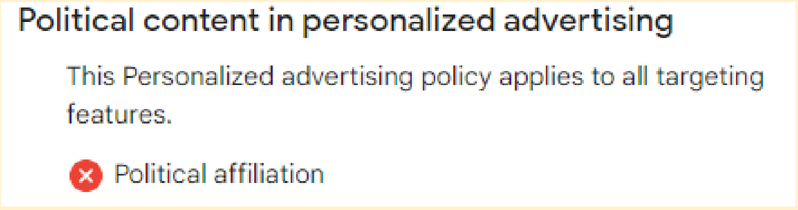
- Full List: https://developers.google.com/authorized-buyers/rtb/downloads/publisher-verticals
- This list could potentially not be complete.
- Screenshots are of Google's own policy.
    - https://support.google.com/adspolicy/answer/143465

- Legal restrictions
    - 946 /Health/Public Health/Toxic Substances & Poisoning
- Identity and belief [Religion | Gender/Sexual orientation | Politics | Race]
    - 113 /People & Society/Ethnic & Identity Groups/Lesbian, Gay, Bisexual & Transgender
    - 1301 /People & Society/Social Issues & Advocacy/Same-Sex Marriage
        - 

          Transgender identification in personalized advertising

          ☒ Personal identification with a gender different from the gender assigned at birth, or a gender which does not conform to singular male or female identification
        - 

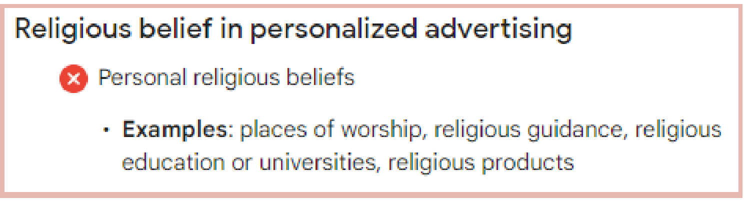
          Sexual orientation in personalized advertising

          ☒ Sexual orientation, including lesbian, gay, bisexual, questioning, or heterosexual orientation
    - 409 /News/Politics/Right-Wing Politics
    - 410 /News/Politics/Left-Wing Politics
        - 

          Political content in personalized advertising

          This Personalized advertising policy applies to all targeting features.

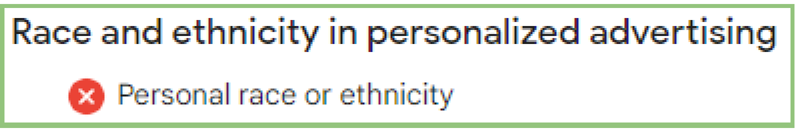
          ☒ Political affiliation
    - 101 /People & Society/Religion & Belief/Spirituality
    - 1251 /People & Society/Religion & Belief/Scientology
    - 1258 /People & Society/Religion & Belief/Pagan & Esoteric Traditions
    - 862 /People & Society/Religion & Belief/Buddhism
    - 864 /People & Society/Religion & Belief/Christianity
    - 866 /People & Society/Religion & Belief/Hinduism
    - 868 /People & Society/Religion & Belief/Islam
    - 869 /People & Society/Religion & Belief/Judaism
    - 975 /People & Society/Religion & Belief/Skeptics & Non-Believers

        - 

          Religious belief in personalized advertising

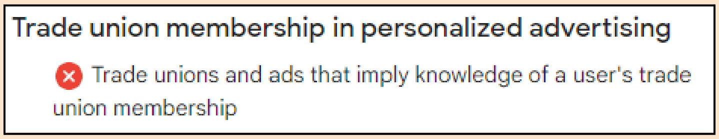
          ⊗ Personal religious beliefs

          - **Examples**: places of worship, religious guidance, religious education or universities, religious products

    - 171 /People & Society/Ethnic & Identity Groups/Indigenous Peoples/Native Americans
    - 547 /People & Society/Ethnic & Identity Groups/Africans & Diaspora/African-Americans
    - 548 /People & Society/Ethnic & Identity Groups/Latinos & LatinAmericans
    - 549 /People & Society/Ethnic & Identity Groups/Asians & Diaspora/East Asians & Diaspora
    - 550 /People & Society/Ethnic & Identity Groups/Jewish Culture
    - 556 /People & Society/Ethnic & Identity Groups/Arabs & Middle Easterners
    - 579 /People & Society/Ethnic & Identity Groups/Africans & Diaspora
    - 580 /People & Society/Ethnic & Identity Groups/Asians & Diaspora/Southeast Asians & Pacific Islanders
    - 681 /People & Society/Ethnic & Identity Groups/Indigenous Peoples
    - 682 /People & Society/Ethnic & Identity Groups/Eastern Europeans
    - 683 /People & Society/Ethnic & Identity Groups/Western Europeans
    - 1257 /People & Society/Ethnic & Identity Groups/Asians & Diaspora
        - 

          Race and ethnicity in personalized advertising

          ⊗ Personal race or ethnicity

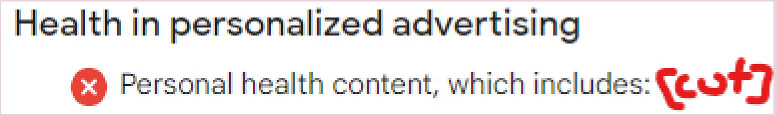
    - 1121 /People & Society/Social Issues & Advocacy/Work & Labor Issues/Unions & Labor Movement
        - 

          Trade union membership in personalized advertising

          ⊗ Trade unions and ads that imply knowledge of a user's trade union membership

    - 976 /People & Society/Social Issues & Advocacy/Reproductive Rights
    - 1280 /People & Society/Social Issues & Advocacy/Human Rights & Liberties
- Personal Hardships [Health | Finance]
    - 420 /Health/Health Conditions/Skin Conditions
    - 429 /Health/Health Conditions/Cancer
    - 437 /Health/Mental Health
    - 571 /Health/Health Conditions/Eating Disorders

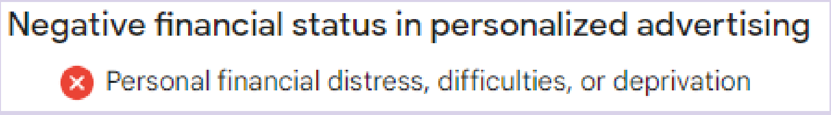
  - 623 /Health/Aging & Geriatrics
  - 639 /Health/Mental Health/Anxiety & Stress
  - 640 /Health/Mental Health/Depression
  - 818 /Health/Health Conditions/Obesity
  - 819 /Health/Health Conditions/Pain Management



Health in personalized advertising

☒ Personal health content, which includes: [cut]

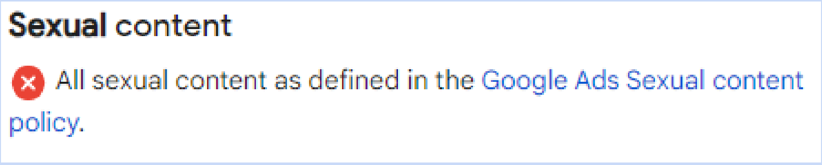
  - 1127 /People & Society/Social Issues & Advocacy/Poverty & Hunger
  - 1220 /Beauty & Fitness/Cosmetic Procedures
  - 1235 /Health/Substance Abuse/Steroids & Performance-Enhancing Drugs
  - 1237 /Health/Substance Abuse/Smoking & Smoking Cessation
  - 1238 /Health/Alternative & Natural Medicine/Cleansing & Detoxification
  - 1239 /Health/Alternative & Natural Medicine/Acupuncture & Chinese Medicine
  - 1262 /Health/Health Conditions/Infectious Diseases/Parasites & Parasitic Diseases
  - 1434 /Finance/Credit & Lending/Debt Collection & Repossession
  - 1437 /Finance/Credit & Lending/Loans/Personal Loans/Short-Term Loans & Cash Advances



Negative financial status in personalized advertising

☒ Personal financial distress, difficulties, or deprivation

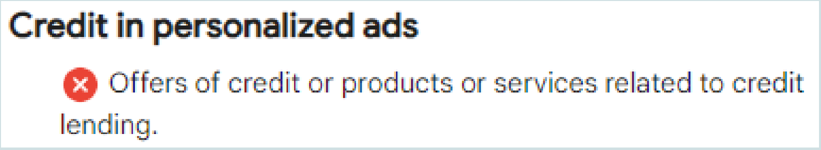
- Sexual Intrests
  - 1236 /Health/Reproductive Health/Sexual Enhancement



Sexual content

☒ All sexual content as defined in the Google Ads Sexual content policy.

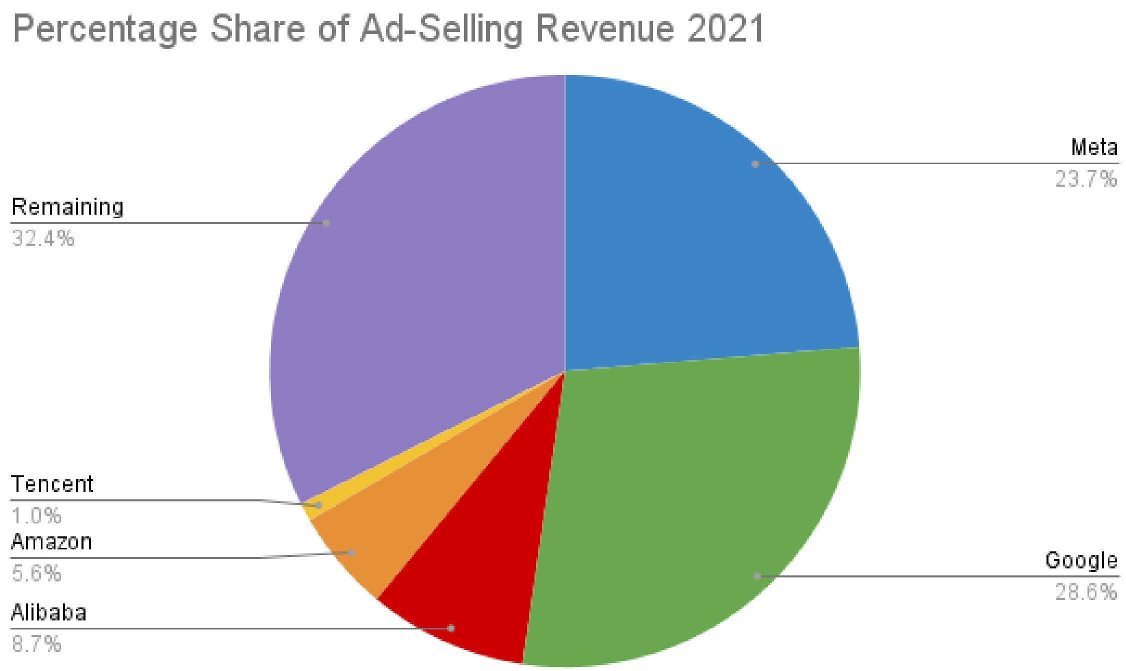
- Access to Opportunities
  - 1434 /Finance/Credit & Lending/Debt Collection & Repossession
  - 1437 /Finance/Credit & Lending/Loans/Personal Loans/Short-Term Loans & Cash Advances



Credit in personalized ads

☒ Offers of credit or products or services related to credit lending.

Appendix 3: Pie Chart of Advertising revenue 2021 (Statista, 2022)



Appendix 4: Simplification of seven key principles of GDPR. (ICO, 2018)

- “Lawfulness, fairness and transparency”
  - Processes of data processing must be disclosed and easily accessible to the average user.
- “Purpose limitation”
  - Data cannot be reused for anything other than its original intention.
- “Data minimisation”
  - Determine what information you need and only collect that amount.
  - Organizations should not overreach in collection.
- “Accuracy”
  - Data kept must be up to date and accurate (no typos)
- “Storage limitation”
  - Personal data should only be kept for as long as it is necessary.
- “Integrity and confidentiality (security)”
  - Appropriate measures should be taken so that personal information is protected from hackers.
  - Breaches must be disclosed within 72 hours.
- “Accountability”
  - Programmers or any others handling sensitive data must be aware and properly trained to be GDPR compliant.

References

Alphabet . (2022, February 1). YEAR IN REVIEW 2021 . 2021 Alphabet Annual Report. Retrieved October 14, 2022, from https://abc.xyz/investor/static/pdf/2021Q4_alphabet_earnings_release.pdf Page 6 of FORM 10-K.

Banning Surveillance Advertising Act of 2022 (2022). bill.

GDPR Enforcement Tracker. List of GDPR fines. (n.d.). Retrieved October 15, 2022, from https://www.enforcementtracker.com/

Google. (2022). Personalized Advertising - advertising policies help. Google. Retrieved October 13, 2022, from https://support.google.com/adspolicy/answer/143465

Google. (n.d.). *Introduction to real-time bidding (RTB) - authorized buyers help.* Google. Retrieved October 11, 2022, from *https://support.google.com/authorizedbuyers/answer/6136272*

H.R.6416 - 117th Congress (2021-2022): Banning surveillance advertising ... (n.d.). Retrieved October 11, 2022, from https://www.congress.gov/bill/117th-congress/house-bill/6416

History of the Sears Catalog. Sears Archives . (2012, March 21). Retrieved October 11, 2022, from http://searsarchives.com/catalogs/history.htm

ICCL. (2022, May 15). *ICCL report on the scale of real-time bidding data broadcasts in the U.S. and Europe*. Irish Council for Civil Liberties. Retrieved October 13, 2022, from https://www.iccl.ie/digital-data/iccl-report-on-the-scale-of-real-time-bidding-data-broadcasts-in-the-u-s-and-europe/

Information Commissioner Office. (2018). The principles. Information Commissioner Office. Retrieved October 14, 2022, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

Joshi, S. (2022, January 31). *History of advertising 101: What you need to know*. G2 Articles. Retrieved October 11, 2022, from https://www.g2.com/articles/history-of-advertising

Magnite. Advertising Technology Privacy policy. Magnite. (2022, September 13). Retrieved October 13, 2022, from https://www.magnite.com/legal/advertising-technology-privacy-policy/

OpenRTB version 2 - IAB tech lab. (2021). Retrieved October 12, 2022, from https://iabtechlab.com/wp-content/uploads/2022/04/OpenRTB-2-6_FINAL.pdf

Pew Research Center. (2019, November 12). *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*. Pew Research Center: Internet, Science & Tech. Retrieved October 10, 2022, from https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/pi_2019-11-14_privacy_0-02/

Pew Research Center. (2022, October 7). *Mobile fact sheet*. Pew Research Center: Internet, Science & Tech. Retrieved October 10, 2022, from https://www.pewresearch.org/internet/fact-sheet/mobile/

Qin, R., Yuan, Y., II, J., & Wang, F.-Y. (2017, February 9). *Optimizing the segmentation granularity for RTB advertising markets with a two-stage resale model*. IEEE Xplore. Retrieved October 12, 2022, from https://ieeexplore.ieee.org/document/7844403

RTB evidence. Brave Browser. (2018). Retrieved October 11, 2022, from https://brave.com/rtb-evidence/

Statista Research Department. (2022, June). Digital ad spend worldwide 2026. Statista. Retrieved October 13, 2022, from https://www.statista.com/statistics/237974/online-advertising-spending-worldwide/

Statista Research Department. (2022, March 9). Digital ad revenue share by company 2023. Statista. Retrieved October 15, 2022, from https://www.statista.com/statistics/290629/digital-ad-revenue-share-of-major-ad-selling-companies-worldwide/

Xandr. (2022, July 6). Third-Party Providers. Xandr Documentation Center. Retrieved October 13, 2022, from https://docs.xandr.com/bundle/service-policies/page/third-party-providers.html#ThirdPartyProviders-Ad-serverPartners