Master Thesis

Rise and Fall of Google's Privacy Sandbox. Why did Google decide to remove third-party cookies, what solution did they propose, and why everything went wrong?

Aalborg University
Electronics and IT

Electronics and IT
Aalborg University
http://www.aau.dk

AALBORG UNIVERSITY
STUDENT REPORT

Title:
Rise and Fall of Google's Privacy Sandbox. Why did Google decide to remove third-party cookies, what solution did they propose, and why everything went wrong?

Theme:
Digital advertisement, internet privacy, Google Privacy Sandbox

Project Period:
Master thesis semester

Project Group:
Mykyta Peschanskyi

Participant(s):
Mykyta Peschanskyi

Supervisor(s):
Jannick Kirk Sørensen

Copies: 1

Page Numbers: ??

Date of Completion:
September 30, 2024

Abstract:

This project analyses the ongoing shift from third-party cookies in digital advertisement and the role of Google's Privacy Sandbox in this shift.

with the author.

Contents

Chapter 1

Introduction

1.1 Motivation

This project aims to analyze the ongoing technological shift in the digital advertising market. Advertisement has been the fueling power of the business, since the creation of the first marketing campaigns back in the early 1900s. Back then, advertisement campaigns were performed using billboards, newspapers, posters, and other tangible means. Since then, the advertising industry has been evolving together with ongoing technological development, quickly adopting new means of reaching audiences. Over time, as the Internet has been becoming more and more widespread, digital advertisement has become an essential part of advertising campaigns. Back in 2019, the internet marketing market size was 319 billion dollars, and it is expected to reach 1,089 billion dollars in 2027. This market creates workplaces, pays taxes, and fuels other sectors of the economy. Free content that we can consume is also often possible due to the revenue that websites get from digital advertisements.

The multi-billion-dollar digital advertisement market is highly reliant on technologies that maintain it. There are a variety of technologies, but one has been significantly widespread– third-party cookies. I have known about this technology since I found out about the foundations of the modern web. Later, when I got a notification from my iPhone saying that I could restrict applications from tracking my data, I was surprised but did not pay much attention. But when I found out that Google was planning to remove third-party cookies completely and substitute them with some "Privacy Sandbox", I realized there was an ongoing shift. I knew that business models websites and brands operate rely on third-party cookies, and I knew that Google is the biggest player in the digital advertisement market. These facts gave me a perception of a fundamental shift, that could potentially cause significant changes in the Internet, causing a lot of consequences for businesses on every level. I discovered a problem that was big enough to be analyzed.

As a student of Innovative Communication Technologies and Entrepreneurship, I am curious

about technologies that facilitate business processes. The case of third-party cookies deprecation and the development of its substitution, Privacy Sandbox, attracts my interest due to the fact that it involves studying the ways that modern digital advertisement works, both from a technological and business point of view. In addition, I want to understand the current shift in digital privacy policies, caused by the adoption of privacy laws, such as GDPR. It is relevant to look at these policies through the lens of digital advertisement, and particularly Privacy Sandbox development because it aims to be a privacy-by-design solution.

1.2 Project Objective

The objective of this project is an analysis of a shift from third-party cookies and the role of Privacy Sandbox in this shift. I want to analyze what led to third-party cookies deprecation, and what are the concerns with their functionality and effectiveness. I want to understand, how participants of the digital advertisement industry react on the shift from third-party cookies. In addition, since the Privacy Sandbox is the technology that has a potential to replace third-party cookies in Chrome, I want to understand, what are the fundamental differences between Privacy Sandbox and third-party cookies, how is the adoption process going, what are the drawbacks and benefits of this technology, and what are the privacy concerns. In addition, I want to examine, how Privacy Sandbox fits into the agenda of digital privacy laws. My research questions will be presented as such:

Rise and Fall of Google's Privacy Sandbox. Why did Google decide to remove third-party cookies, what solution did they propose, and why everything went wrong?

Subquestions:

1. What are the prerequisites for a shift from third-party cookies?
2. How does Privacy Sandbox work, what are advantages and disadvantages?
3. Why Google decided to keep third-party cookies?
4. Beyond Privacy Sandbox. What is the broader situation with third-party cookies?

Chapter 2

Methodology

2.1 Important event that contributed to the Analysis

This project started in March 2024 and continued until the 30th of September 2024. This timeline was filled with the ongoing discussion about Privacy Sandbox, and some of the findings influenced the initial direction of the project. The most significant event that influenced the project was Google's decision to abandon plans to remove third-party cookies(July 27th, 2024). This event significantly changed the path of a project and added new challenges to my analysis.

2.2 Project process

To understand the shift from third-party cookies, I explored different types of cookies and the ways they are used in digital advertisement. To understand privacy problems of this technology, I examined the GDPR and analyzed potential concerns third-party cookies might have with this privacy law. Also, I examined Google's advertisement solutions to understand how third-party cookies are involved in them. For this, I looked at Google's resources that provide technical explanations of these methods. In addition, I wanted to examine to what extent does the digital advertisement industry relies on third-party cookies. For this, I looked at articles from influential industry bodies, such as IAB lab and the Electronic Frontier Foundation, and academic papers. Answering these questions helped me to understand the full picture of the shift from third-party cookies.

For the Privacy Sandbox part, I researched how it works using the official website of this project. I looked into the technical explanation, but I have not concentrated on the technical side of the Privacy Sandbox APIs, because my initial goal was to understand the broader picture, and a deep dive into each API requires a separate project. To gain a comprehensive understanding, I looked into articles and papers, that provide opinions and deep analysis from industry participants, such as big advertisers, publishers, and authorities. Generally, throughout the project, I followed this process:

1. Initial understanding of the technology
2. Reviews of the material, such as articles, blogs, and academic papers. Interview with industry professionals.
3. Formulation of my own critical opinion

2.3 Pivot of the project

This project was inspired by Google's decision to kill third-party cookies in Chrome. My initial goal was to concentrate on Privacy Sandbox, the solution that had to become a substitution. Until July 27th, I was on this path. Then Google announced that they would keep third-party cookies. Even though Google announced that it would keep investing in the development of Privacy Sandbox, it was not in the center of attention anymore. I shifted my research to the analysis of what went wrong with the Privacy Sandbox, and why Google decided to keep third-party cookies. I understood the wider problem with third-party cookies. This problem inspired me to analyze other digital advertisement solutions that are becoming widespread due to problems with third-party cookies. However, these solutions also create privacy and effectiveness concerns, which I decided to analyze.

2.4 Challenges I faced during the project

1. The research questions I raised are broad – I have taken up a challenge to gain an understanding of how the modern digital advertising industry works, its challenges, and perspectives. To answer my research questions, I had to understand how third-party cookies, privacy sandbox, and other technologies work. Also, I had to understand a tendency towards a more private web and the legislation that influences this tendency. In addition, I had to examine the competition in the market. This analysis required a deep understanding of the above-mentioned fields, and inside knowledge from the stakeholders involved in this technological shift.
2. Ongoing adoption and development – Privacy Sandbox is a fresh technology, it only ran through several tests, which were led by Google and a few independent companies. The results of these tests can not be sufficient enough to say to what extent Privacy Sandbox is an effective solution. Google claims that this solution is effective[79], but adTech company Criteo does not agree[66]. It is hard to determine who is right without having alternative views. Conducting tests is very complicated for me as an independent researcher. Also, the ongoing development of technology implies a lack of literature and research about it, which I could use for my analysis
3. Lack of cooperation from the industry stakeholders – Throughout the research, I reached out to members of the advertisement companies based in Denmark. I wanted to hear

their position on third-party cookies deprecation and their view on the future of digital advertisement. I managed to get only one interview, which was extremely helpful for me. I believe that experts have a little incentive to contribute their time to student research. Insights from the companies that are involved in digital advertisement give a valuable understanding of the ongoing situation, and without them, it is hard to create a comprehensive view.

4. Access to the literature – Some articles and research from resources that specialize in digital advertisement are closed and available only after buying a subscription.

Chapter 3

State-of-the-art

3.1 Advertisers

An advertiser [76]is a company or organization that has a goal to promote its products, services, or brand to a specific audience they are focusing on.

Key characteristics of advertisers

- Paid promotion – advertisers pay for promotion of their products and services.
- Marketing goals – Sales increasing, brand recognition building, engagement driving
- Audience targeting – Focus on reaching relevant audience
- Success measurement – tracking the performance of the ads for data-driven decisions

Examples of advertisers

- E-commerce companies
- Retail brands
- Service providers
- Local businesses
- Non-profits and government organizations

Types of advertisers

- Direct-to-Consumer – main clients of these advertisers are individual consumers
- Business-to-Business – main clients of these advertisers are businesses
- Brand advertisers – brands that focus on improving their brand awareness.

The role of advertisers in the digital advertisement

- Media buying – advertisers buy ad spaces on websites, mobile apps, search engines, or social media platforms.
- Creative development – advertisers create visual messages that they consider relevant to their audience and that later are shown on ad spaces they buy.
- Campaign management – advertisers set budgets, duration, and target options for the ad campaign.
- Audience targeting – Filtering the audience based on the parameters that are relevant for their product, service, or brand.
- Performance analysis – Ad performance analysis using different metrics.

3.2 Publishers

A publisher[76] is a digital entity, website, app, or platform that sells advertisement spaces on the resource that belongs to it. Publishers sell spaces in a form of display ads(banners, pop-ups), native ads(ads blended with content), video ads, sponsored content. Publishers want to monetize the content and the audience that is attracted to this content. This approach allows keeping content free for users.

Key characteristics of publishers

- Content distribution – distribution of digital content and ads displaying
- Audience monetization – showing ads to the audience
- Revenue generation – Revenue generation through models like cost-per-click, cost-per-thousand-impressions, cost-per-action.

Examples of Publishers

- News websites
- Social Media platforms
- Video Streaming platforms
- Mobile apps
- Bloggers and content creators

The role of publishers in the digital advertisement

- Ad inventory selling – selling spaces via direct deals or ad networks
- Ads displaying – ensure seamless integration of ads
- Revenue maximization – ad placements optimization
- User experience management – seeking a balance between monetization of ads spaces and positive user experience
- Audience data management – publishers own data records of their users, such as logins, personal information, behavior on their website, and interests.

3.3 Ad Tech industry

AdTech(advertising technology) [7]industry is a set of technologies and platforms that facilitate the buying, selling and delivery of digital advertisement. These technologies and platforms automate the process of linking advertisers with publishers and enable real-time ad serving.

3.3.1 Key Components of the AdTech ecosystem

Demand side – advertisers

Advertisers want to serve ads to their audience and achieve their goals. Advertisers use Demand-Side platforms (DSps) for the automation of the ad-buying process. DSP is a software that allows real-time bidding, specific audience targeting and budget management.

Supply side – publishers

Publishers want to sell spaces on their resources to monetize their content. They use Supply-Side Platforms(SSP) to manage and sell ad spaces. SSPs help publishers maximize revenue, control what ads they place and automate the process of ad space selling.

3.3.2 Ad exchanges and Real-Time Bidding (RTB)

Ad exchanges are platforms that enable operations between SSPs and DSPs. They are marketplaces that allow SSPs and DSPs to trade ad inventory. All operations are happening within milliseconds, during webpage loading process.

Real-Time Bidding (RTB)

RTB is an automated auction[106] through which ad spaces are traded. RTB works in a following way:

- User visits a website – once a user visits a website ad space becomes available
- Ad Impression is Auctioned – available ad space is sent to an ad exchange
- Bidding process – advertisers submit bids for showing ads to a particular user. Bids are based on different factors about a user, such as browsing behavior, demographics, etc.
- Highest bid wins and gets a display time on a webpage
- Ad is displayed in real-time

This process is carried out for milliseconds and it does not influence user experience.

3.3.3 Ad auctions and Bidding process

Bids

Bid [7]is how much an advertiser wants to pay for showing their ad to a user. Bids are placed based on various factors:

- User's value – user browser behavior, interests, consuming habits, demographics.
- Ad placement – how good is an ad space(top of the page, bottom of the page, etc)
- Targeting criteria – precise information about user influence the price

Types of Ad Auction Models

- Secon-Price Auction – higher bidder wins an auction and pays the price of a second-highest bid
- First-Price Auction – higher bidder wins an auction and pays the price they submited.

3.4 First-party and third-party cookies. Privacy concerns about cookies

A cookie [109] is a piece of code that a web server sends to a browser. Web browsers store this code for a specific amount of time, or while a user interacts with a web server. Any future user interaction with a web server will be attached to the relevant cookies. Cookies are used for user-session management, authentication, personalization, and tracking. For example, when a user creates an account on a website, a cookie string that contains relevant information about user's interaction with a website is generated. Later, when a user logs in to a website, a web server recognizes user's account details and users's previous interaction with a website, enabling tailoring of a website's content to user's interests. There are 5 types of cookies:

- Session cookies – Only active while a user interacts with a website. They are deleted after a user ends the interaction.

- Persistent cookies – Remain on the website for a persistent time, usually have an expiration date.
- Authentication cookies – Used for session management and authentication.
- Tracking cookies – Cookies that are generated by tracking services. They record the activity of a user on a website and send this information to a tracking service.
- Zombie cookies – Cookies that appear again, even after they are deleted.

If a cookie is placed by the same domain user is on, they are called first-party cookies. But if cookies are placed by another domain, not the one a user is interactin, they are called third-party cookies [110]. Both third-party and first-party cookies are stored in the web-browser. These cookies track user's interaction with a website and send this information to a third-party domain, that later uses this information for different purposes.

Example of first-party cookies: When you visit tech gear website, the site uses first-party cookies to remember the headphones you added to your cart. If you navigate to other pages or return later, the items remain in your cart. Additionally, the site remembers your preferred currency and language settings for a smoother experience.

Example of third-party cookies: While browsing tech gear website, an external ad network sets a third-party cookie that tracks your visit. Later, as you browse a news site, you see ads for the same headphones, as the cookie has tracked your behavior across different websites to serve targeted ads.

3.5 Usecases that third-party cookies support

Cross-site tracking

Third-party cookies allow user tracking across websites. It allows advertisers to create user profiles that are based on online behavior.

- Tracking of users' behavior across websites
- Identification of a frequently visited website
- Recognizing a user across sessions and devices
- Monitoring of user interaction: clicks, page views, dwell time
- Cross-domain tracking and linking of behavior to the user ID

Behavioral Targeting

Allows delivery of personalized ads based on previous interactions.

- Ads serving based on browsing history
- Recommendation of product based on past searches
- User segmentation based on past behavior
- Tracking of repeat visits to the same website.
- Ad delivery optimization

Personalized advertising

Third-party cookies enable more personalized and tailored ads based on user interest.

- Show ads for products and services the user previously interacted with
- Retarget ads that were previously shown to a user but did not result in a purchase
- Dynamic ad customization
- Ad delivery based on user demographic and behavior

Ad retargeting

Advertisers can target users who previously interacted with their website

- Tracking of users who previously visited a website
- Ad serving across other websites
- Displaying ads for the same products that a user previously interacted with on different websites
- Displaying ads based on items that were left in the cart, but never purchased

Conversion tracking and attribution

Enable measurement of ad campaign success and linking ads and results they achieved.

- Tracking ads that resulted in website visits.
- Conversion measurement, such as purchase, sign-up, download
- Attribution of conversions and interaction that led to them

- Give insights into a customer journey across different touchpoints
- Measurement of ad creatives' effectiveness
- Tracking of sale journey, from interaction with ad to purchase

Audience segmentation

Advertisers can segment their audience into categories.

- Audience segmentation by behavior, interest, demographic
- Segmentation of users into groups like " Football fans", "Luxury buyers", "Budget buyers", etc
- Multi-platform audience segmentation
- Tailoring of ads based on different segments
- Cross-website analysis of user behavior

Frequency Capping

Control of frequency with which the same ad is shown to a user.

- Tracks the amount of time the particular ad is shown to a user
- Sets how many times in a specific timeframe an ad is shown to a user
- Prevents showing the same ads to user repeatedly
- Ad spend optimization
- Ad frequency balancing

Ad fraud prevention

Prevents showing invalid ads and bot attacks.

- Detection of fake clicks or fake impressions
- Identification of suspicious behavior, like bot-actions
- Flags strange patterns in ad interaction
- Saves advertising budget by preventing invalid traffic
- Improves trust between advertisers and publishers

Lookalike modeling

Enables targeting of an audience that has the same characteristics as the existing customers.

- Identification of common patterns among different segments of users
- Identification of users with the same browsing behavior as an existing customer base
- Customer base expansion
- Targeting accuracy improvement
- Boost of returns on ad spend because of targeting of the audience that is more likely to convert.

Multi-touch attribution

Evaluate contribution of multiple ad interactions in the customer journey.

- Cross-channel and cross-device interaction tracking
- Value attribution to each interaction in the user journey
- Evaluating the role of a specific type of ad in influencing conversions
- Ad spend optimization by giving insights into the most effective touchpoint
- Shows data for precise analytics.

Interest-based advertising

Serving ads based on long-term interest and behavior

- User interest tracking based on browsing history
- Creation of interest profiles
- Personalized ads delivery based on hobbies, lifestyle
- Allow building long-term interests with user
- Refine ad targeting

Cross-device tracking

Tracking of users across multiple devices. If user switches between devices, such as desktop, mobile, TV, their profiles remain the same and they are shown the same ads.

- Cross-device activity tracking
- Linking of sessions across devices
- Conversion tracking and attribution across platforms/
- Cohesive ad experience across different devices.

3.5.1 Third-party cookies and data privacy

Privacy concerns with third-party cookies stem from their ability to track users across multiple websites [96], creating detailed profiles of individuals without their explicit consent. These cookies are often used by advertisers to monitor browsing behavior, which can lead to invasive targeted advertising and potential misuse of personal data. Users typically have little visibility into which companies are tracking them and how their data is being used, raising concerns about transparency and control over personal information. Moreover, the aggregation of data from various sources increases the risk of privacy breaches and unauthorized data sharing.

3.5.2 Cookies and GDPR

The General Data Protection Regulation (GDPR) [38] includes provisions that specifically address the use of cookies, often referred to as the "cookie law" [53]. Under GDPR, websites must obtain explicit consent from users before placing non-essential cookies, such as those used for tracking and advertising, on their devices. This means that users must be informed about the types of cookies being used, the data they collect, and the purposes of that data collection. Consent must be freely given, specific, informed, and unambiguous, meaning users should have the option to reject cookies without any negative consequences on their ability to use the site. This regulation aims to enhance user privacy and give individuals greater control over their personal data online.

3.6 Google and third-party cookies

Third-party cookies play a significant role in Google's advertising solutions, enabling the tracking of user behavior across different websites to deliver personalized ads. These cookies help advertisers reach specific audiences based on their browsing history, enhancing ad relevance and effectiveness. Platforms within google's advertisement ecosystem that rely on third-party cookies include:

- Google ads – [41] A platform that allows businesses to create and display ads across Google Search and its partner sites, targeting users based on search queries and intent.
- Google Display Network – [28] A network of over two million websites, videos, and apps where Google Ads can appear, allowing businesses to reach users through banner ads and other visual formats.
- YouTube ads – [3] Advertising options on YouTube that allow businesses to display video ads.
- DoubleClick Campaign Manager – [46] Now part of Google Marketing Platform, it's a tool for managing and tracking digital advertising campaigns across multiple channels and platforms.
- Display and Video 360 – [31] An integrated platform within Google Marketing Platform for planning, buying, and measuring display and video ads across various channels and formats.
- Google Ad Manager – [40] A comprehensive ad management platform that combines Google's ad server and programmatic tools for managing ad inventory and optimizing revenue across various ad networks.
- Google Shopping – [4] A service that allows retailers to display product ads directly in Google Search results, featuring product images, prices, and links to the retailer's website.
- Google Analytics – [37] A web analytics service that tracks and reports website traffic, providing insights into user behavior, conversions, and the effectiveness of marketing campaigns.

3.7 Google Privacy Sandbox

The Privacy Sandbox [43] is a Google initiative that aims to create technologies that both protect user's privacy online and create tools for developers and companies that help them build successful digital businesses. The Privacy Sandbox aims to build new technology that helps keep your information private, enables publishers and developers to keep online content free, and collaborates with the industry to build new internet privacy standards. There are Privacy Sandbox for the Web and Privacy Sandbox on Android. I will concentrate on the Web version.

Privacy Sandbox for the Web [94] aims to create new web standards that will reduce cross-site tracking, but keep content free. Publishers will be able to abandon privacy-invasive technology like third-party cookies and keep getting revenue. Privacy Sandbox for the Web consists of several APIs, each has its own purpose. Currently, there are 9 APIs:

- Private State Tokens API – addresses fraud protection and bot detection issues. Particularly important for establishing trust towards a user, making sure that a user is who they claim to be. Also important for advertisers who do not want to pay for the ads shown to bots.
- Topics API – a solution that directly substitutes third-party cookies. Based on a user's browsing history, a browser creates interest categories and then through API calls shares it with third parties, without revealing the user's browsing data.
- Protected Audience API – a solution that is used for remarketing and custom audience purposes, while restricting third parties from tracking user's browsing behavior. Also, through this API an on-device ad auction is run, that selects the most relevant ads to show to a user, based on user's browsing behavior.
- Attribution Reporting API – used to track the performance of ads. Today performance tracking relies on third-party cookies that track users across websites, thus violating user's privacy. With this API, data for the reports is noised and sent with a delay, preventing cross-site tracking.
- Related Websites Sets – allows limited third-party cookies access for special goals, such as showcasing relationships across sites.
- Shared Storage API – allows making decisions based on cross-site data, without sharing user information.
- Fenced Frames API – securely embed content onto a page without sharing cross-site data.

3.8 Browser fingerprinting

Browser fingerprinting[51] is a comprehensive technique that is used to uniquely identify and track web browsers by harvesting and processing different parameters used by the browser and device. Compared to cookies that store data on a user's device, browser fingerprinting passively gathers a set of data points that combine to create a unique profile of the user's browser.

In its core browser fingerprinting utilize distinct browser and device configurations[1] that are unique due to a combination of software and hardware variations. Browser fingerprints are created when a user visits a website that uses fingerprinting techniques, usually written in JavaScript, that are active while a user interacts with a website. Data points include:

- Operating System: Operating system details, such as Windows, MacOS, mobile platform
- Browser and version: Type of browser and its versions, such as Chrome, Safari or Mozilla
- Screen resolution and color depth: User's screen dimension, number of bits

- Language and Time Zone settings: Preferred language settings and the configured time zone.
- Installed fonts: Fonts installed on the system that are retrieved by the Canvas or Flash APIs
- Browser plugins and extensions: Installed plugins(Flash, Java) and extensions that alter browser behaviour
- MIME types and HTTP headers: media types supported by the system and header information that reveal configurations
- Canvas Fingerprinting: HTML5 Canvas element that renders graphics and captures differences in the way text shapes appear that can vary among devices.
- WebGL fingerprinting: graphic card and driver details gathered from the WebGL API
- AudioContext Fingerprinting: AUdio signals generation and analysis to capture unique aspects of the audio stack
- Touch Support and Device Sensors: Detection of sensors that are supported by the device.

These attributes on its own are not unique, but their combination created by fingerprint processing forms composite identifier that is highly unique. Fingerprinting processing happens by hashing the combination of data points by hash functions like SHA-256 that produce fixed-length output.

Advanced fingerprinting methods may exploit other APIs and characteristics:

- Battery status API: Battery level and status of charging.
- Network information API: Connection type and speed
- Media device enumeration: Data about connection type and speed
- Client hints: HTTP headers that help the server with content optimization and are used by fingerprint methods to collect device information.

In addition, scripts can measure the time the browser takes to perform certain operations. The difference in processing time reveals information of the device's hardware capacity, such as CPU and memory speed.

These attributes are accessible without the user's special permissions. It significantly improves browser fingerprinting effectiveness. Consent is not needed because this data is essential for appropriate content rendering and seamless user experience. For instance, information about screen resolution is used to adjust the site's layout for optimal viewing.

Browser fingerprinting is implemented using libraries and scripts that automate data collection. For example, FingerprintJS[34] collects browser attributes and generates fingerprints without impacting page load time.

When a user visits a website, scripts gather information and send a fingerprint to the server. The server compares this fingerprint with other fingerprints in a database to detect if a user has visited the site before. The server associates the current session with the previous activity.

Browser fingerprints do not store any data on user's device. The stateless nature of this technique challenges detection or prevention[1]. Clearing cookies or private browsing modes does not undermine fingerprint creation and its characteristics.

3.8.1 Examples of fingerprinting solutions

FingerprintJS:[34]

- Open source library for generation of fingerprints using characteristics of device and browser
- FingerprintJS has a commercial version with improved accuracy for the identification of unique users and fraud detection.

ThreatMetrix:[97]

- Device fingerprinting solution for fraud prevention and authentication
- Uses a combination of device intelligence, behavioral analytics, and threat intelligence.

Iovation:[36]

- Device detection and intelligence solutions for web and mobile
- Content delivery optimization and web traffic analysis

SecureAuth:[83]

- Device fingerprinting solutions for improved authentication
- Prevents unauthorized access and reduces identity-related breaches.

InAuth:

- Solutions for mobile intelligence and authentication
- Secures transactions and prevents fraud in mobile environments with the help of browser fingerprinting.

DataDome:[24]

- Device fingerprinting for bot detection and behavioral analysis
- Websites and APIs protection from automated threats.

Imperva Advanced Bot Protection:[8]

- Fingerprinting solutions for malicious bot activity detection and protection
- Website spam and scraping protection

Kasada[52]

- Device and browser fingerprinting for bot mitigation
- Credential stuffing protection

3.9 Universal IDs

Universal ID is an identifier that allows recognition of a user across platforms, websites, and devices[101]. Unlike browser-specific cookies, Universal IDs are server-based and stay consistent across environments. They enable user tracking in a more consistent and privacy-preserving way. Universal IDs incorporate the benefits of third-party cookies, such as ads targeting and effectiveness measurement, but are designed to operate in privacy-first environments.

3.9.1 Different types of Universal IDs

Deterministic IDs

Deterministic IDs is a user identification method for digital advertising[57]. They are based on direct and verifiable data provided by users. They rely on personally identifiable information like emails, phone numbers and login information. They provide highly accurate identification because they are based on actual data provided by a user. Deterministic IDs have the potential to become a popular solution because it is consent-based, highly accurate and enable cross-device tracking.

Probabilistic IDs

Probabilistic IDs is a user identification method that uses statistical modeling and inference[57]. It does not rely on direct data provided by a user but rather relies on non-personally identifiable information like device characteristics, IP addresses, behavioral patterns(browsing history), and location data. This data is used to build profiles and with the help of statistical models, these profiles are given a probability of belonging to a specific user. For example, if user visits a website on a laptop, and later accesses this website from a mobile, probabilistic models can identify the probability of this user being the same person. User does not need to be log in.

Examples of Probabilistic IDs

Tapad Cross-Device graph:

- A probabilistic identity resolution platform
- Process multiple data points that include device types, IP addresses, and browsing behavior to understand the connection between devices
- Allows advertisers to target the same user across devices, without PII

Adbrain be Trade Desk:

- Probabilistic cross-device identification
- Matches devices to users using machine learning and behavioral data.
- Achieve delivery of consistent messaging across device

Crosswise by Oracle Data Cloud:

- A cross-device identity graph based on probabilistic methods.
- Creates anonymous user profiles based on statistical probability.
- Used for cross-device targeting and measurement

Zeotap ID+:

- Identity solutions that combine deterministic and probabilistic data
- Gathers data signals through partnerships and uses AI to improve matching accuracy
- Used for ad targeting and measurement

Lotame Panorama ID:

- Global privacy-compliant identity solution
- Creates identity graph based on non-PII data and probabilistic modeling
- Maintanes addressability on cookieless environments

ID5 Universal IDs:

- Shared identity infrastructure for digital advertisement
- Creates and shares user IDs based on probabilistic methods
- Enables effective targeting and personalization in cookieless environments.

Examples of deterministic IDs

Unified ID 2.0:

- Open source framework developed by The Trade Desk and managed by IAB Tech Lab
- Uses hashed and encrypted email addresses provided by users.
- Allows advertisers and publishers to recognize users across platforms

LiveRamp Identity Link:

- Identity resolution service that connects offline and online data
- Uses anonymized and linked to the same device PII like emails, and phone numbers.
- Unified view of the customer for personalized marketing across channels

Google Publisher Provided Identifiers

- Allows publishers to send their own identifiers to Google Ad Manager
- Assigns unique and persistent identifier to logged-in user.
- Used for frequency capping, audience segmentation and targeting in environments with restricted third-party cookies

Adobe Experience Platform Identity Service:

- Identity management across devices and channels
- Creates persistent profile based on customer-provided identifiers
- Allows personalized experience and consistent messaging across touchpoints

Chapter 4

Analysis

4.1 Prerequisites for a shift from third-party cookies

Google started planning the substitution of third-party cookies in early 2020[15], initially announcing to finish it in 2022, and later extended to 2024. This shift was influenced by increasing privacy concerns and pressure from European regulatory bodies like GDPR. Also, other major browsers like Safari and Firefox already restricted third-party cookies[105], making Google lose the battle for privacy. These actions led to the development of alternative solutions, that would provide a sufficient level of privacy while replacing the functionality and effectiveness of third-party cookies.

For ages, third-party cookies have been an essential part of digital advertisement, making it possible for advertisers to track users across multiple websites and create detailed profiles based on their online behavior. This functionality enabled precise ad targeting and personalized content serving, making ads more relevant for users and effective for advertisers. Apart from targeting, third-party cookies enable frequency capping(preventing showing the same ad multiple times), retargeting(targeting users that already visited a website), and attribution(statistics about the performance of an ad).

Demand for third-party cookies is created by the industry's will to advance ad relevance and reduce ad ineffectiveness. Without third-party cookies, advertisers effortlessly tried to reach the intended audience, and marketing campaigns were less effective, increasing costs both for advertisers and users. These cookies are a cornerstone of the internet economy, they are used by publishers as a way to monetize their content, thus making it free for consumers.

However, non-consented user tracking and profile creation caused serious privacy concerns[96]. Users were usually unaware of the way their data used and who it is shared with. Also, data aggregation from different sources increases the risk of privacy breaches and unauthorized data sharing. Third-party cookies are usually associated with the next issues:

- **Cross-site tracking and profiling** – Companies can monitor user behavior across different websites, often without user's consent and knowledge. These cookies are usually placed by third parties, such as ad networks or data brokers, not the website itself. While users surf the web, cookies monitor this activity and collect information on browsing habits and preferences, assembling data into detailed profiles. These profiles usually contain sensitive information about individuals, such as medical data, religious information, and personal life data. The problem lies in the little user awareness[96] about the underlying processes applied to their data and it's further exploitation.

- **Lack of transparency and consent** – Among the integral issues with third-party cookies is the lack of transparency[96]. Users have little or no idea that their data is being collected and traded around the internet. GDPR-like privacy laws demand explicit consent for data collection, but usually consent boxes just trick users into accepting all cookies, without providing sufficient explanation about underlying processes. This practice creates an illusion of legitimate and informed consent, when in fact it is just a banner game.

- **Data sharing and exploitation** – The data harvested through third-party cookies is often sold or shared with third-party entities, for example, advertisers, marketers, and data brokers. Later this data is used for purposes that the user never gives consent to, such as targeting advertisements, political manipulations, or price discrimination[96]. In addition, third-party cookies concentrate a high amount of data in the hands of centralized data management platforms, creating a bigger risk of data exploitation and misuse. The case with Facebook and Cambridge Analytica is a perfect example.

- **Risk of data breaches and security issues** – Concentration of large amounts of data in the hands of centralized data brokers or data management platforms creates a higher risk of data breaches and cyberattacks[96]. Attackers can get access to personal data, harming users across multiple platforms. Furthermore, data brokers usually store data in jurisdictions with weak privacy policies, thus increasing security risks. For example, in 2018 Marriott Hotel suffered an attack that caused data leakage of over 500 million guests. The vulnerability was partly caused by third-party services that had access to this data, making it vulnerable to attackers.

- **Erosion of privacy and trust** – As users are becoming more aware of their actions towards their data, the trust levels in technologies drop. This creates higher levels of skepticism and even abandoning some services.

4.2 Legislative response to third-party cookies

In GDPR, cookies are directly only mentioned once, in [78] Recital 30: "Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency

identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them." Cookies are qualified as personal data and therefore must comply with GDPR[53]. It means that companies can process their user's personal data only after they give consent, or if companies have a legitimate interest [108].

Much wider cookies are addressed In the ePrivacy Directive[32], which is also known as a "Cookie law" because after this law came into force, websites were required to ask for user's consent through pop-ups. According to EPD and GDPR, the one who processes personal data must:

1. Receive user's consent for any cookies except strictly necessary
2. Accurately and specifically inform about the type of data that is tracked and the purpose of tracking in plain language.
3. Document and store user's consent.
4. Allow user's access to service even in case of denial from cookies.
5. Enable users to easily withdraw their consent.

The ePrivacy Directive [32] came into power in 2009. Soon it must be replaced by ePrivacy Regulation [93]. EPR will have EPD as its core but will address issues with new technologies, including user tracking by third parties. It is still being created, and the last update is August 29, 2024, that canceled a requirement to remove persistent cookies after 12 months.

4.3 Google and third-party cookies

As we can see, privacy regulations do not ban third-party cookies. Privacy regulations require clear communication with users about the fact that they are being tracked and consent to be tracked. Other than that, third-party cookies as a technology is not banned. So why did Google decide to end support of cookies?

Google first announced plans to get rid of cookies in 2020[16], saying that they would eventually fully end their support. I believe that this is a response to an industry trend for a more private web. In 2017, Apple implemented Intelligent Tracking Prevention[100], a technology that prevents third-party tracking and restricts third-party cookies. Firefox implemented Enhanced Tracking Protection, a technology that allows users to block cookies and access from third-party trackers. Chrome has 67%[26] of a market share, making it the biggest player in the market, but suddenly it started losing a battle for privacy to the competitors. The context of this battle is the desire of major browsers to transform privacy on the web and their bet on increasing users' awareness regarding privacy. Those who lead this battle will get more users onboard.

The Webkit, browsers engine used in Apple's Safari and web browsers on IOS and IpadOS have their Tracking Prevention Policy that describes tracking practices they use[105]. It states that Webkit prevents tracking practices that are harmful to users because they exploit user's privacy without their consent and ability to control it[100]. Webkit states that they prevent covert tracking, all cross-site tracking, stateful tracking, covert stateful tracking, navigational tracking, and fingerprinting or stateful tracking. They also promise to prevent all tracking mechanisms that are currently unknown. If any party tries to bypass tracking prevention, they promise to add restrictions. This policy is inspired by Mozilla's anti-tracking policy.

While being among the three most popular browsers, Mozilla, Safari, and Chrome have completely different business models. Safari is a part of Apple's ecosystem, that focuses on selling hardware and services, like Apple Music, iCloud, and AppStore. Apple's business model is not reliant on advertisement, and they try to position themselves as a privacy-first company. That is why they emphasize on intelligent tracking protection[100] and try to prevent third-party cookies. These actions create a competitive advantage, potentially attracting users to Apple's ecosystem.

Mozilla's Firefox is non-profit and operates through Mozilla Foundation, which focuses on open-source development, user privacy, and the open web[35]. They generate money through partnerships and donations and do not rely on data collection and advertisement.

Unlike Mozilla and Apple, Google's business model heavily relies on advertisement and data collection[30]. Google harvests huge amounts of data through its services, including Chrome, with the goal to later use it for targeted advertisement. Third-party cookies are an essential technology that facilitates this process. 80%[30] of Google's profits come from advertisements. Google managed to gain huge chunk of a market thanks to its advertisement technologies, such as Google Ads, YouTube ads and others, that rely on third-party cookies. Hence, Google heavily relies on third-party cookies, and removing them would significantly undermine Google's revenue streams. This fact explains, why Google was so slow with the implementation of cookieless advertisement methods.

4.4 Industry's reliance on third-party cookies

However, the tendency towards a more private web made google work towards cookieless solutions. Taking Google's dominance in the market, a transition from third-party cookies not only creates a threat for Google's revenue streams but also for businesses that rely on advertisement tools Google offers. As for 2024, Chrome is used by 3.45 billion users worldwide, taking up to 63.87 percent of the browser market share[26]. More than 84% of companies are going to use Google Ads in 2024[80]. Google's services are especially convenient for small and medium companies, that do not have unlimited marketing budgets. Vast amount of data Google collects via third-party cookies allows precise ad serving, based on user behavior and interests. These

allow small and medium companies, that do not have access to sufficient amounts of first-party data, to promote their products and services.

The transition from third-party cookies creates inconveniences for businesses because it requires time and resources to learn and master cookieless advertisement. However, cookieless advertisement techniques are less effective than good-old third-party cookies, which have been around for years and pervade the majority of the web. Advertisers may see significant drops in the results of their advertisement campaigns, and suddenly their ROIs(return on investment) can drop significantly[81]. That is why some companies have started preparing for the shift from third-party cookies since 2020[68]. They started experiments with different cookieless strategies, such as first-party data strategies, server-side tracking, cookieless IDs, data clean rooms and others.

Google faces a dilemma: There are advertisers, who are their clients, and they like third-party cookies, and there are users, who are also their clients, and they do not like cookies. How do you find balance? Initially in 2020[16], Google announced that they would shift from third-party cookies in 2022. They announced it and started the development of alternative solutions, that would satisfy the industry and help Google remain at the top of the Internet advertisement business. That is when they began working on The Privacy Sandbox.

4.5 Development of The Privacy Sandbox

Google's announcement of third-party cookies removal marked a significant shift in the digital advertisement industry. The initiative was met with a wide range of reactions from advertisers, publishers, ad tech companies, and regulators. In this section, I will concentrate on reviewing opinions about The Privacy Sandbox by those who are directly or indirectly affected by it.

4.5.1 Reaction from Advertisers

There are different types of advertisers in the market. Some are small brands, that spend precious resources on ad targeting and rely on Google's algorithms with the hope that they will reach targeted audiences and generate sales. In this case, they rely on Google's precision and power. Additionally, there are big brands, that despite having deep pockets with monstrous marketing budgets, have access to first-party data, that they generate from interaction with their users. These facts significantly influence the damage that removal of third-party cookies potentially causes for brands. Experts suggest brands[50]bet on first-party data as a solution to cookieless advertisement. However, small businesses rarely generate large datasets of this data, hence these solutions does not work for them. According to statistics[11], small and medium businesses make up a major chunk of many countries' economies. Generally, the Privacy Sandbox initiative was

met with a high degree of skepticism and concerns from advertisers[54]. However, some emphasized[111] potential improvement of privacy, while the majority were worried about their ability to target ads, measure their performance, and execute personalized marketing strategies.

One of the main concerns that experts express[23] is the increasing dominance and potential monopoly of Google. This is the topic that I will return to during my analysis because this issue arises more and more as Google is rolling out the privacy Sandbox. The problem for advertisers lies in over-reliance on Google's solutions. Now, advertisers can choose different Adtech providers, that have different solutions based on third-party cookies. But when Google bans them, they will only be able to use the Privacy Sandbox and other cookieless solutions, that are yet to come.

Another significant concern is the doubts[54] over how well Privacy Sandbox will replace third-party cookies functionality in targeting accuracy they used to. APIs proposed by Privacy Sandbox, such as Topics[99] and Protected Audience[75] do not directly replace third-party cookies. It results in concerns from advertisers[66] that these solutions will not provide a sufficient level of granularity and targeting efficiency, especially in retargeting and audience prospecting use cases. Some advertisers[48] had an opportunity to test these APIs, but results were limited and solutions were described as incomplete as they could not satisfy the full range of advertisers needs.[48]

In addition, another problem is effective attribution[49]. Attribution means the ability of advertisers to see the performance of their ads. For example, when a user clicks on the link, advertisers get this data into their Google Ads. It allows advertisers to get feedback about the effectiveness of ads and optimize them. Now Google Ads offers a wide range of metrics that allow advertisers to make precise data-driven decisions. But as for now, Privacy Sandbox does not provide enough metrics that allow flexible decision-making. Privacy-centric design of Attribution Reporting API does not allow tracking every single interaction on the advertiser's website, thus advertisers will have to adapt to the limited amount of metrics attributed to their ads.[49]

However, Advertisers also expressed optimism[111] regarding the shift towards the Privacy Sandbox. They appreciated the time that Google gave advertisers and other industry players to adopt cookieless technologies[111]. Others pointed out that this shift will make advertisers use more user-centric and meaningful approaches for advertisement.

4.5.2 Reaction from Publishers

Publishers rely on third-party cookies in order to effectively sell advertisement inventory on their websites. Publishers expressed significant concerns about the effectiveness of Google's Privacy Sandbox, especially around latency issues[55] that can severely impact revenue generation. Latency[84] in this case is the amount of time it takes to perform ad auction and eventually serve ads to a user. Primarily, this concern originates from the Protected Audience API(PAAPI)

within the Privacy Sandbox, because this API will be used for targeted advertisement when third-party cookies will be removed. Early tests showed that PAAPI causes a significant delay during ad auctions, causing an increase in response time by 1500 milliseconds (1.5 seconds), which is considered a significant response time[84]. This delay caused lower ad viewability rates that dropped from standard 70% to 39%[84]. This significantly reduces available ad inventory and creates a direct threat to publishers' ad revenue because it reduces the chances of ads being displayed.[84]

In addition, latency issues cause lower yield and slower delivery times[55], further degrading the effectiveness of the solution. Publishers are afraid[55] that these bottlenecks will reduce the number of ad impressions and eventually decrease monetization of a website. Publishers want to have more controls[55] and reporting capabilities inside The Privacy Sandbox, that will allow them to better track and manage ad performance.[73]

This technological shift is particularly harmful for smaller publishers that rely on advertisement revenue to sustain their operations. I assume that significant drops in revenue will lead to catastrophic consequences for them, because, unlike big publishers, they do not have large resources to survive this shift.

4.5.3 Reaction from regulators and industry bodies

Feedback on Google's Privacy Sandbox from industry bodies and regulators has been diverse, ranging from careful optimism to significant concern. The shift from third-party cookies and their replacement with Privacy Sandbox APIs poses a major change in the digital advertising landscape, and different stakeholders expressed their opinions about potential consequences for privacy, competition, and transparency.

Regulators have expressed[47] worries about competitive issues with the Privacy Sandbox. In January 2021, the United Kingdom's Competition and Markets Authority (CMA)[47] initiated an investigation caused by industry stakeholders' complaints about the Privacy Sandbox. They claimed that the Sandbox could damage competition by giving Google greater control over digital advertisement because it would bound the possibility of ad tech companies and publishers to have access to user data independently. The CMA's investigation was part of a regulatory plan to examine Googe's superiority in the digital advertisement market. Regulators expressed concerns that Privacy Sandbox implementation could result in consolidation of market power in Google's hands because it would both design standards and control access to user data in the new system.[47]

In addition, the CMA partnered with the UK's privacy watchdog, the Information Commissioner's Office, in order to ensure the balance between competition and user privacy in the new standards. Regulators recognized[20] Google's privacy initiatives, but they also pointed out the

need for transparency and supervision to ensure that Google's system does not damage competition. Since then, Google has agreed to work with CMA to ensure that the Privacy Sandbox development promotes both privacy and competition.[20]

4.5.4 Feedback from the World Wide Web Consortium(W3C)

W3C is an international community that develops web standards that have been a part of discussions around the Privacy Sandbox. W3C says that they appreciate Google's focus on privacy, but at the same time, they express concerns[5] about the lack of inclusivity in the way that Google makes decisions. Standards community members emphasized that Google's approach centralizes too much power in their hands, thus limiting the diversity of solutions that address online privacy and tracking issues.

Specifically, The W3C Technical Architecture Group raised concerns about Federated Learning of Cohorts, which is currently called Topics API. This solution groups users into behavioral cohorts for targeted advertisement. TAG welcomed[82] the idea of moving towards privacy-preserving methods but criticized cohort-based tracking for the potential risk of user tracking and exposure of sensitive personal characteristics. The group emphasized[82] the necessary careful review for potential unintended consequences.

4.5.5 Feedback from privacy advocates

Privacy advocates consider Privacy Sandbox as a right step but questioned its ability to fully address user privacy concerns. Organizations such as the Electronic Frontier Foundation criticize Google's approach, especially the lack of transparency regarding the way user's data will be handled. The EFF has raised questions about the potential discrimination caused by cohort-based tracking and exploitation based on sensitive attributes such as race, gender, or sexual orientation.[19]

The EFF's concerns were especially solid regarding the original FLoC proposal[33], which as they say could still expose users to tracking even if the data was anonymized. They are concerned whether the privacy protections built into FLoC would be reliable enough to prevent misuse by malicious actors, such as combining cohort data with other identifiers to track individuals across websites. The EFF's position[19] has been that the move away from third-party cookies is positive, the Privacy Sandbox may not be enough to protect users from tracking by large corporations.

4.5.6 Industry Body responses: The interactive Advertising Bureau(IAB)

The Interactive Advertising Bureau is a trade group that stands for advertisers, agencies, and publishers. It has taken an alert but constructive position about Privacy Sandbox. The IAB's primary concern[71] lies in the potential historical shift in the advertising landscape, especially

for smaller publishers and ad tech companies that are reliant on third-party cookies for ad targeting and performance tracking. The IAB has appealed to Google to make sure that Privacy Sandbox solutions give the same level of efficiency as third-party cookies for personalized ad delivery.[71]

The IAB Tech Lab has been actively testing Privacy Sandbox APIs[102]. The goal of these tests was to assess their performance and ensure that they addressed the needs of the digital advertising community. The IAB supports Google's initiative to move towards a more privacy-friendly web. However, they pointed out[102] the importance of ensuring that these shifts do not disproportionately damage certain segments of the industry, such as small and independent publishers. The IAB emphasized the need for a dialogue between Google and the industry to tackle concerns about the impact on revenue and data transparency.

4.5.7 Concerns from the European Union

EU looks at the Privacy Sandbox through the lens of GDPR. Since GDPR sets strict standards for how companies must collect and process personal data, regulators have questioned[88] whether the Sandbox complies with these regulations. One of the main problems is that cohort-based methods can still be called personal data according to GDPR because they involve grouping users according to their browsing history.

The European Data Protection Board (EDPB), an EU body that oversees GDPR enforcement, has expressed concerns[88] about the Privacy Sandbox's ability to create decent transparency and data control for users. I believe, their concerns are caused by the fact that aggregated data could still be used to indirectly identify individuals, hence it does not comply with GDPR's requirements. This uncertainty most likely will make Google work closer with regulators to ensure that Privacy Sandbox is compliant with GDPR and other privacy laws.

4.5.8 Collaborative efforts for the development of the Privacy Sandbox

During the development of The Privacy Sabdbox Google Collaborated with a wide range of industry players, including advertisers, publishers, ad tech companies, browser developers, and regulatory bodies. Google tries to satisfy all industry players, which is why they try to gather expert opinions around the market.

1. Involvement of advertisers – Big advertisers are involved in the collaboration[79]. These brands use targeted advertising for their marketing strategies. I think big brands want to be sure that new solutions will satisfy their advertising use cases. They are working with Google and provide their expertise in using targeted advertising solutions, providing feedback on how well new solutions achieve the results previously achieved by third-party cookies.

2. Involvement of publishers – Big publishers rely on third-party cookies to support their ads revenues, making them a vital part of this collaboration. They expressed concerns[79] that the shift towards Privacy Sandbox tools might drop their ad revenue. The reason behind their participation in tests is to ensure the new solutions will enable them to maintain profitability.

3. Involvement of Ad Tech Companies – Criteo, Magnite, Trade Desk, and other companies that develop advertising solutions, are vital for the ecosystem. They develop the technologies for programmatic advertising, such as real-time bidding. Technologies that these companies develop are based on third-party cookies. Removing them means also removing these technologies.[65]

4. Involvement of browser developers – Mozilla and Safari are pioneers in third-party cookies replacement. Cookieless technologies that Safari uses were inspired by Mozilla. Google tries to gain their experience, and also make sure that new technologies will be compatible throughout multiple platforms and browsers.

5. Involvement of regulatory bodies – regulatory bodies such as the UK's Competition and Markets Authority is actively involved in testing The Privacy Sandbox. They want to make sure that new solutions are compliant with GDPR and competition laws. These bodies want to preserve user's privacy and market competition.[77]

4.5.9 How does the collaboration work?

The collaboration is done by public feedback and transparency. Proposals are released by Google through the World Wide Web Consortium[69]. Then Google invites industry stakeholders to participate in discussions, trials, and feedback sessions. Using this forum, companies can assess Google's proposals and give detailed feedback about their functionality and effectiveness.

For instance, in this way, Google released Federated Learning of Cohorts(FLoC), the technology that groups users based on their browsing behavior without revealing individual identities. However, companies involved in testing and privacy advocates, such as Brave[87]and DuckDuckGo[29] expressed concerns that this technology does not protect users from fingerprinting and still enables it. Thanks to this feedback, FLoC was replaced by Topics API, which allows targeting based on general topics of interest, not on the browsing history.

4.5.10 Why are companies involved?

Removal of third-party cookies causes a significant disruption to the digital advertising landscape. This removal threatens business models that have been here for years, that relied on digital ad targeting and measurement. Collaboration with Google allows all the parties involved to shape the development of the new tools and helps to ensure that new solutions will align with their needs[27].

For example, adTech firms participate in the development, trying to secure their spot in the cookieless advertising landscape by lobbying their views. To avoid monopolistic concerns, Google enables integration with different ad tech platforms in their proposals like FLEDGE.[98]

4.5.11 Results of the collaboration

The collaborative efforts have resulted in significant changes in Google's proposals. To be specific, Topics API and Protected Audience API have been redeveloped through multiple rounds of tests and feedback from the above-listed involved parties. For instance, initially, tests of Topics API were promising, but later concerns about its ability to perform at scale without compromising user privacy remained. In addition, ad tech companies have been able to test Protected Audience API, by running simulations of it they have helped Google improve its ability to balance privacy and performance.

4.6 New birth of third-party cookies in Chrome

After years of threats to phase out third party cookies and countless tests of cookieless solutions, on July 22, 2024, Google introduced "A new path for Privacy Sandbox on the Web".[18] In essence, Google decided to keep allowing third-party cookies and abandoned plans to remove them in Chrome and all their products. Google has been threatening the industry with these plans for 4 years, in the timeline below I show the milestones on its way. That has led to the wide industry response, that I have analyzed in the chapters above. Some companies remained silent and careless, but some were preparing for this shift[85], by developing first-party strategies and investing in privacy-preserving solutions. Now Google says: "We are proposing an updated approach that elevates user choice. Instead of deprecating third-party cookies, we would introduce a new experience in Chrome that lets people make an informed choice that applies across their web browsing, and they'd be able to adjust that choice at any time. We're discussing this new path with regulators, and will engage with the industry as we roll this out."[18] This decision came after multiple postponements of the final deprecation of third-party cookies and the rollout of Privacy Sandbox.

4.6.1 The timeline of Privacy Sandbox development and announcements of third-party cookies deprecation in Chrome

1. In January 2020 Google first announced that they would deprecate third-party cookies support in Chrome.[16]

2. In January 2020 Google first announced that they would deprecate third-party cookies support in Chrome within two years. Google decided to go a different path than other major browsers. Instead of blocking third-party cookies, they decided to develop Privacy Sandbox to preserve existing business models and satisfy users' privacy demands.[39]

3. In July 2022 Google further delayed the adoption of Privacy Sandbox and the full phase-out of third-party cookies. They shifted the delivery of Privacy Sandbox APIs to early to mid-2023. The full phase-out of third-party cookies was estimated to happen in early 2024[17]

4. In December 2023 Google announced that on January 4th, 2023 they would start testing Tracking Protection. This feature limits website access to third-party cookies by default. In this announcement, they proclaimed the full phase-out of third-party cookies in the second half of 2024.

5. In January 2024 Google restricted third-party cookies for 1% of users. They planned to restrict them for 100% of users from the third quarter of 2024.[68]

6. In July 2024 Google abandoned plans to remove third-party cookies in Chrome.[16]

As we can see from the timeline, Google stressed the digital advertisement industry several times, causing uncertainty about whether they would postpone deprecation or not. According to Google, they had problems with API testing and issues with the United Kingdom's Competition and Market Authority (CMA). In my opinion, Google's initial plan to phase out third-party cookies until 2022 was too optimistic. Of course, Google has almost unlimited resources to develop, test and implement privacy-preserving APIs. However, other players of this post-cookies game were not willing to engage in tests. I assume this is because of the low number of test participants. Only 43 AdTech companies did direct integrations with Protected Audience API and only 12 publishers were interested in early adoption.[112] These companies are the biggest players in the AdTech market, and these publishers are big newspapers and marketplaces. I assume that they have budgets and resources to test and implement Google's new initiatives. But, third-party cookies would not only be phased out for major players but for every single Chrome user. Google's guidelines for tests are complex and require technical knowledge[95]. When Google announced third-party cookies deprecation they had plans to make it privacy-preserving while still allowing publishers and advertisers to deliver ads. I believe that after tests, the Privacy Sandbox team understood, that without more thorough development and deeper feedback from the industry, they would not be able to achieve initial goals.

In addition, Google has attracted the attention of the UK's monopoly regulator, CMA[47]. CMA planned to "The investigation will assess whether the proposals could cause advertising spending to become even more concentrated on Google's ecosystem at the expense of its competitors. It follows complaints of anticompetitive behavior and requests for the Competition and Markets Authority (CMA) to ensure that Google develops its proposals in a way that does not distort competition."[21]. Apparently, other authorities than CMA have not expressed any interest in Privacy Sandbox.

4.7 What went wrong with Privacy Sandbox

I have already mentioned the problems Google had with authorities and feedback from the industry. These obstacles made Privacy Sandbox developers shift the rollout and deprecation of third-party cookies. Obstacles have been arising since the beginning of the development. What were these obstacles, and were they the reason why Google eventually gave up on the idea of deprecating third-party cookies? In the next chapter, I will analyze deeper the obstacles Google had and try to understand the real reason behind Google's idea to keep third-party cookies.

In case of fundamental technological shifts and new initiatives, it is useful to look at the reactions of industry bodies. Privacy Sandbox development and third-party cookies deprecation is exactly this kind of shift. Organizations like World Wide Web Consortium and Electronic Frontier Foundation help shape the Internet. In the case of the Privacy Sandbox, the leading organization is the IAB tech lab[44]. IAB tech lab is a non-profit research and development consortium that produces and helps implement technical standards and solutions. The goal of the Tech Lab is "reduction of the friction associated with the digital advertisement and marketing supply chain while contributing to the safe growth of an industry." The Tech Lab made a report, called "Privacy Sandbox Fit Gap Analysis for Digital Advertisement". They have a dedicated "Privacy Sandbox Task Force"[70], a group that brings industry participants to assess the implications of Privacy Sandbox and works closely with Privacy Sandbox developers to provide consolidated feedback. This group consists of various players across the digital advertisement industry.

In the report[72], IAB Tech Lab concentrated on the assessment of fundamental common everyday use cases and implied business impact. They focused on Protected Audience API and Attribution Reporting API. In my opinion, this is a wise choice of APIs to concentrate on, because they cover the most important use cases that digital advertisement relies on: audience management, auction management, metrics measurement, and ad rendering. In addition, I would also concentrate on Topics API, because it raised privacy concerns across the industry[60]. These privacy concerns originate in potentially invasive ways of using user's browsing data to create topics of interest.

Privacy Sandbox Task Force assessed 45 main usecases and shared issues they found with Privacy Sandbox developers. Among other issues, the most important ones are:

1. Fragmented documentation – It is hard to understand how APIs work when technical documentation is poorly organized, spread across multiple sources, and unclear. It complicates implementation and troubleshooting of the system. Consequently, it is hard to adapt Privacy Sandbox to organization needs. Documentation must be clear, easily accessible, and well organized[72].

2. Lack of consideration for commercial requirements – Chrome acts as an active participant

in financial transactions and delivery of goods. Financial transactions are ad auctions and delivery of goods is ad serving. Currently, Google does not explain how will they maintain contractual relationships with advertisers, publishers, and technology partners. If Google does not meet legal requirements it may result in penalties and loss of trust[72].

3. Absence of third-party audits – Privacy Sandbox does not allow third-party audits. This is an essential part that allows to assess if the ad transaction is fraud-free. Without these audits, advertisement transactions are vulnerable to threats[72].
4. Lack of standard industry accreditation – Privacy Sandbox lacks accreditations, such as MRC accreditation. The possession of accreditation shows data quality, accuracy and trust[72].

4.7.1 Industry readiness to the shift from third-party cookies

When I look into challenges Google had with Privacy Sandbox development and implementation, it is necessary to understand the level of the industry's awareness about potential third-party cookies removal. Do companies make any steps towards cookieless advertisement, or only major adTech companies and publishers are concerned with that? Are there any performance problems with third-party cookies solutions, or do they satisfy companies that rely on them? It is important to answer these questions to understand why Google failed to remove cookies. Maybe Privacy Sandbox, except for having technical problems, does not fit into the current technological agenda, and the industry is simply not ready for these changes.

One of the problems with third-party cookies that the industry faces is signal loss[63]. Signal loss in digital advertisement is the process of reduction or elimination of data signals that advertisers and adTech companies rely on to serve personalized ads, target specific audiences, measure campaign effectiveness and trace conversions. Signal loss happens because of a combination of factors, such as regulatory changes, technological shifts, and evolving user awareness.

Privacy regulations require websites to ask for explicit user consent for data processing, which more and more users do not give[86]. It significantly limits advertisers' ability to collect personal information and leads to reductions of data signals. In addition, browsers and platforms implement privacy-enhancing technologies. For example, Safari[105] and Mozilla block third-party cookies, and Apple's App Tracking Transparency[100] requires mobile developers to ask for consent before tracking users across apps and websites. In addition, users widely adopt AdBlockers, Privacy extensions, and Privacy-focused browsers like Brawe or DuckDuckGo. These tools block data collection mechanisms and contribute to signal loss. AdBlockers alone are used by almost one billion users worldwide, and since 2012 the number of adBlockers users increased 21 times[62].

Signal loss is a significant problem for companies that want to do sustainable advertising. This problem forces more and more advertisers to adopt first-party data strategies, contextual advertisement, or cookieless technologies. Surveys say that due to this problem, 31% of marketers and

advertisers are preparing alternative[91] strategies. This would be a great time for a solution like Privacy Sandbox. It would eliminate the problem of signal loss because third-party cookies would not exist anymore, and all the advertisers would forget about this specific problem. However, even this significant problem has not stimulated Google to finalize Sandbox and roll it out.

Despite the fact that more and more companies are turning to privacy-preserving cookieless solutions, it might not be the case for Denmark. I interviewed Jacob Knobel, CEO of Datapult[25]. Jacob has multiple years of experience in programmatic advertisement and a deep knowledge of the Danish advertisement industry. In his opinion, small and medium companies that use digital advertisement strategies based on third-party cookies will not shift towards privacy-preserving solutions until they start losing significant amount of profits or until they will be forced to do it. As of now, these companies are settled with third-party cookies-based advertisements. Most likely, the high switching costs of cookieless technologies imply that companies with limited resources are discouraged from testing or developing new solutions.

On the one hand, the industry feels problems with loss of signals that cause losses and lower effectiveness of marketing campaigns. But on the other hand, we see companies that ignore ongoing shifts. Here the question of industry readiness arises. In my opinion, the industry can not be one hundred percent ready for the shift. Historically, the mass adoption of new technologies happened gradually, with pioneers and those who were forced to shift. The ongoing case with mass adoption of cookieless technologies shows that a significant amount of companies are adopting new technologies and investing in cookieless solutions. But, in my opinion, there will always be a fraction that does not care, as long as their ads are shown and they see profits. In this case, Google's deprecation of third-party cookies would be the milestone that would make every player in this industry shift towards privacy-preserving solutions. However, Google decided to wait.

4.8 Reactions on Google's decision to retain cookies

Google decision to retain cookies came out of the blue and created wide range of responses around the web. Some players of the industry breathed a sigh of relief and went on with their third-party cookie advertisement strategies. Some were frustrated. Below, I will analyze responses from industry bodies and companies.

4.8.1 World Wide Web consortium

W3C expressed concerns and disappointment about Google's decision to no longer deprecate third-party cookies. They pointed out that third-party cookies are harmful to the web due to the fact that they enable user tracking across multiple sites, which violates privacy. In their opinion, even though they are essential for such use cases as login or shopping cart, they are usually used for surveillance and ad targeting without user consent. In addition, they pointed

out ongoing regulatory concerns[45] about third-party cookies and the negative societal impacts of data collection and micro-targeting, particularly in political cases.

W3C has been taking part in the development of Privacy Sandbox[2]. For several years W3C's Technical Architecture Group has been involved with the Sandbox team to develop better alternatives to third-party cookies. They claim to achieve substantial progress together, and this decision undermines these collaborative efforts to develop privacy-preserving advertisement methods.

W3C expresses concerns that this decision will be catastrophic for the goal of enhancing user privacy on the web. In the end, they hope that Google will reverse this decision and continue the way toward eliminating third-party cookies.

In my opinion, the W3C is an industry body that focuses on making the web better and improving user privacy[104], while they may not fully realize the economic consequences of third-party cookies deprecation. Their analysis concentrates mostly on the technical, privacy, and regulatory aspects, ignoring the financial impact on the digital advertising industry. I believe that there is a need for a balanced approach, that considers the needs of all players across the industry, this approach can lead to more sufficient and sustainable solutions.

4.8.2 Response from regulators

The UK's Information Commissioner's Office (ICO) was frustrated about Google's decision[45]. They stated that "From the start of Google's Sandbox project in 2019, it has been our view that blocking third-party cookies would be a positive step for consumers" and "Our ambition to support the creation of a more privacy-friendly internet continues. Despite Google's decision, we continue to encourage the digital advertising industry to move to more private alternatives to third-party cookies - and not to resort to more opaque forms of tracking"

The UK's Competition and Markets Authority is pleased[9] with Google's new approach, which basically introduces a user-choice prompt that allows users to decide if they want to keep third-party cookies or not. According to CMA, this approach is right because it has the user's consent as its main principle.

The main task for Google and all industry players right now is to design a choice architecture that adjusts to everyone's interests. For example, Dave Lee from Bloomberg expressed his concerns about the complexity of this potential architecture[58]. According to him, if choice screens are too challenging for users to accept, or too easy to decline, it might be dissatisfying for advertisers, and this can be considered as anti-competitive intentions.

An example of this case is Chrome's current choice for "ad topics"[59]. When a user opens

Chrome, this message pops up:"Turn on an ad privacy feature. Ad topics help sites show you relevant ads while protecting your browsing history and identity. Chrome can note topics of interest based on your recent browsing history. Later, a site you visit can ask Chrome for relevant topics to personalize the ads you see. You can see ad topics in settings and block the ones you don't want to be shared with sites. Chrome also auto-deletes ad topics that are older than 4 weeks."

This way of phrasing raised concerns, saying that it is potentially misleading. For example, Max Schems, Honorary Chairman of NOYB said[42]:"Google has simply lied to its users. People thought they were agreeing to a privacy feature, but were tricked into accepting Google's first-party ad tracking. Consent has to be informed, transparent, and fair to be legal. Google has done the exact opposite."

In my opinion, giving users a choice is the right way, but it may not be the best way to go. The majority of users are unaware of third-party cookies and the implications of their usage. In this case, regulators can try to implement the default solution that will satisfy both competition and consumers. They can try to require Google to develop a solution that blocks third-party cookies by default, like Apple or Mozilla use.

4.8.3 Response from adTech companies

Another opinion about Google's decision to retain cookies comes from George London, CEO of adTech company Upwave. George has been involved in Privacy Sandbox development process where he collaborated with W3C. George says that he "witnessed a masterclass in corporate hubris".

In his opinion, Google not only wanted to make the web more private and secure for users but also tried to win the race against Apple, which has been attacking Google about its weak privacy positions[12]. Before, I already mentioned that there is an ongoing battle between Google and Apple on being more privacy-oriented. In addition, George states that preventing cross-site tracking does not create privacy for users. In his opinion "The core problem was that Google's definition of privacy was philosophically bankrupt. It ignores key common-sense aspects of privacy, such as the notion that users' expectations vary depending on what information they're sharing and with whom. Or that harm comes from how data is used, not how it's collected."

In addition, George says that Google's actions made industry players search for alternatives[67], that may be less privacy-friendly. For example, it can be identifiers based on address or phone number.

As a way forward, George suggests developing a multistakeholder initiative, that will be led by regulators. This initiative must include a comprehensive consensus-building process, a flex-

ible and dynamic definition of privacy, based on philosophical norms, and pragmatic data use rules.

In my opinion, calling Google's definition of privacy "philosophically bankrupt" is oversimplification. It is true that not allowing cross-site tracking does not comprehensively protect user privacy, but Google aimed efforts to find a balance between user privacy and advertising ecosystem needs. Underestimations of these efforts overlook the complexities of web standards and create potential unintended consequences of rapid changes, for example for small publishers that rely on revenue from advertising.

4.9 What is next?

The decision to retain third-party cookies came after multiple attempts to roll out Privacy Sandbox. However, technical problems and regulatory burdens made Google to put it on hold. There was too much at stake, both for Google and the industry. Privacy Sandbox was met with too much criticism, saying that it is not effective and sustainable enough to fully substitute third-party cookies. On June 27th, 2024, a month before Google published its decision, Criteo made its final report about Privacy Sandbox. Criteo is a giant in adTech market and the biggest external company that was involved throughout the development and test of Privacy Sandbox. They said that Privacy Sandbox was not ready, but it could be a good alternative that can work with third-party cookies. They declare that if Privacy Sandbox had been implemented in that current state, publishers would have seen their ad revenue drop by 60 percent[81]

In addition, the regulatory burden was too heavy. UK's Competition and Market Authority was stepping on Google's toes throughout the process of development. In my opinion, the fact that they were pleased with the decision to keep cookies and slow down on Sandbox development, says that they were not going to reduce the pressure on Google[10]. As for now, it seems like this regulator is satisfied with the new user-centric approach, that " lets people make an informed choice that applies across their web browsing, and they'd be able to adjust that choice at any time". It seems like Google decided to choose a path, in which they first seek the regulator's blessing, rather than the industry's or users' blessing. Following this approach, they are planning to give extra choice to consumers, following the fact that this user-centric approach would definitely satisfy regulators. However, answering the question I raised in the chapter "Industry readiness to shift from third-party cookies", the industry is definitely ready for new solutions, that would replace third-party cookies that are getting less and less effective.

In the light of dramatic signal loss from third-party cookies that I explained in the chapter "Industry readiness to shift from third-party cookies", the decision to retain third-party cookies seems irrational. However, I assume that Google knows the business and has a clear strategic understanding of the market. In my opinion, a new approach that elevates user's choice is a temporary solution. With this solution, they satisfied regulators. Now they can continue the

development of Privacy Sandbox, which finally will become sufficient enough to roll it out. When it is ready, Google will have multiple products, both for third-party cookies and one that works without them. It means that users that do not consent to be tracked by third-party cookies, will be targeted using Privacy Sandbox.

Nevertheless, as of now, those users that do not consent to cookies, or use adBlockers, or those that use Safari and Mozilla can not be targeted with the solutions Google currently has. The problem with third-party cookies' ineffectiveness remains, and it is getting bigger. Although Google announced that they would keep developing Privacy Sandbox, they did not give any timelines or promises about it. This means that Google currently can not provide a solution for third-party cookies, which are rapidly losing effectiveness. Companies that use these solutions, will continue seeing drops in the effectiveness of their ad campaigns. There is a trend in the industry, that third-party cookies are outdated, first of all for the reason of their decreasing effectiveness. Now, companies are shifting towards solutions that do not use third-party cookies. For instance, solutions that use first-party data, or context-based solutions. In addition, intent-based solutions, AI-based solutions, or solutions that use publishers signals. Smart advertisers and publishers have already observed this trend, and are actively preparing and testing new solutions[89]. In my opinion, for years, the advertising industry was third-party cookies-centered. This was a sufficient solution that performed well. Now, this era is gone, and companies are developing and exploring new solutions. There are a variety of different solutions, that satisfy different use cases and industries[89]. Questions that I am raising now are: What is the set of solutions that will replace third-party cookies? How effective are they? Can we predict the solution that will dominate the market as third-party cookies did?

4.10 Browser Fingerprinting

Third-party cookies are the most popular marketing technology used for ad targeting and user tracking. However, there is also a wide range of technologies that can be used for this purpose. As signals from third-party cookies get less and less relevant, advertisers are turning to more persistent technologies. One of these technologies is browser fingerprinting. Browser fingerprinting tackles the main problems of third-party cookies: the need for consent and blocking by major browsers.

Here is a comparison of third-party cookies and browser fingerprinting, the comparison is based on functionality, effectiveness, and the level of privacy:

Use cases supported by third-party cookies:

- Ad targeting and personalization
- Retargeting

- Measurement and analytics
- Frequency capping

Use cases supported by browser fingerprinting:

- User recognition
- Ad targeting
- Fraud detection
- Bypassing cookies restrictions

Advantages of third-party cookies:

- Widespread adoption
- Relatively simple to implement or manage
- Gather precise user data overtime

Disadvantages of third-party cookies:

- Signal loss
- Requires consent

Advantages of browser fingerprinting:

- Resilience to deletion
- Do not require to be stored locally on user's device
- Can be used for fraud detection and security measures

Disadvantages of browser fingerprinting:

- Considered as very intrusive, due to lack of user consent mechanism and ability to opt-out.
- Regulatory risks – conflict with data protection law.

Browser fingerprinting solutions for advertisement are on the rise now[13]. Unlike third-party cookies, browser fingerprinting is much more persistent and more resilient to ad blockers, browser restrictions, and user opt-outs. First of all, browser fingerprinting can be used in Safari and Mozilla. This fact makes this solution highly relevant for advertisers because Safari users make up the most valuable audience. With browser fingerprints, it is hard for users to remain unknown, even if a user denied cookies, uses adBlockers, or surfing the web via Safari or Mozilla. Fingerprints allow very precise ad targeting because they collect a vast amount of data about user's device and browser settings. The combination of different data points creates a unique

identifier, that will correspond only to one user. This unique identifier allows precise ad targeting, tailored to specific interests and settings. 75% of desktop devices can be identified, and only 1 in every 19000 browser fingerprints can be the same as from your device[1]. Another advantage of browser fingerprints is cross-device and cross-browser performance. In the case of cookies, each device has its own set of cookies. But in the case of fingerprints, identifiers allow recognizing the user on another device, or browser. It allows plenty of use cases for ad targeting and personalization.

4.10.1 Privacy concerns about browser fingerprinting

Browser fingerprints raise significant privacy concerns for the reason that this method allows covert tracking of users across the web without them being aware of it or giving consent. Browser fingerprints are different from third-party cookies because users cannot just delete browser fingerprints from a device. This allows companies to track users persistently, even if users try to enhance their privacy by clearing cookies or using private browsing. The inability to prevent and control this tracking impairs users' autonomy and control over their personal data.

In addition, browser fingerprints gather extensive data, that includes sensitive information about users, such as system configuration and usage patterns. This way of extensive profiling infringes on individuals' privacy and increases the risk of data exploitation for malicious purposes, including identity theft and cyberattacks. According to GDPR, the processing of personal data requires explicit and informed consent from the user. Device fingerprint is considered personal data, hence it can not be created without the user's consent[14]. However, websites never ask for consent to create a browser fingerprint. Companies that create a fingerprint and exploit it without user's consent violate GDPR

Privacy issues that browser fingerprinting poses are inflamed by the lack of transparency. Users are usually unaware of the ongoing collection, profiling, sharing, and trading of their personal data between third parties. The undercover data collection destroys trust and violates the principles of fairness and lawfulness of data protection laws. The European Data Protection Board has highlighted that browser fingerprinting without consent can be justified only if its usage is essential for the service to be provided, but it is rarely the case in online advertisements[103]. Also, the Electronic Frontier Foundation raises awareness for stricter regulations and the creation of measures that protect users from unwanted fingerprinting[22].

In addition, browser fingerprinting can create a threat to online anonymity, which is essential to activists, journalists, or whistleblowers who operate in repressive countries. Popular anonymity-enhancing tools like VPNs can be bypassed by sophisticated fingerprinting techniques, creating a threat of surveillance and dehumanization[61].

4.10.2 Effectiveness of browser fingerprinting

Browser fingerprinting is effective due to its resilience to widespread privacy measures. Third-party cookies can be deleted or denied, but fingerprints are significantly more complex to bypass. Even if browsing data is cleared and user switches on private browsing, unique device fingerprints remain the same, allowing continuous tracking. This research analyzed the uniqueness of the high volume of browser fingerprints. According to it, 99% of browsers can be identified based on the fingerprint[56].

This fact is adopted by advertisers to perform ad targeting and personalization. Analysis of browsing habits and preferences allows advertisers to deliver more relevant ads, thereby increasing engagement and conversion rates. Fingerprinting also enables frequency capping and attribution modeling, which is used to prevent showing the same ad and for tracking users across different sites and sessions.

Currently, a solution that would prevent fingerprinting without significantly harming user experience and web functionality does not exist. The nature of browser fingerprinting exploits functionality that browsers provide to websites for correct functioning, which is why it is so hard to prevent. Parameters like screen resolution, language settings, and installed plugins are necessary for appropriate web page rendering. Attempts to limit access to this information can lead to broken websites and poor user experience. The Electronic Frontier Foundation states that blocking all fingerprint features is impossible without ”breaking the web”[22].

In addition, even though Mozilla[35] and Safari offer Enhanced tracking protection, they are insufficient enough and can be circumvented. Mechanisms behind these browsers limit the information shared with websites, but advanced fingerprinting techniques can identify users based on other available data points. Apple also acknowledges that effective protection against fingerprinting is impossible without affecting usability[105].

Fingerprinting techniques are rapidly evolving. When anti-fingerprinting techniques prevent the collection of some data points, trackers find another attribute or make a more sufficient combination of existing ones. For example, canvas fingerprinting uses HTML5 to uniquely generate image that is based on user's graphic rendering capabilities. Even though GDPR considers browser fingerprints as personal data and requires consent for its creation, enforcement is complicated because of the invisible creation of fingerprints. Users are most likely unaware of fingerprint creation, and companies are not transparent about the fingerprinting techniques that are used on their websites.

The widespread adoption of browser fingerprinting undermines efforts of an ongoing war with third-party cookies. As cookies are getting less and less effective, advertisers switch[15] to browser fingerprinting because it is an effective and flexible solution. However, unlike consent-based third-party cookies, users do not even known that they are being tracked. Coupled with

the fact that regulators do not work towards the elimination of this problem, browser fingerprints are a privacy nightmare. The industry is rapidly going towards a cookieless future, but this future does not look bright if invasive tracking mechanisms take the scene instead of bad-old cookies. Financial incentives that fingerprint techniques contain do not stimulate the elimination of these practices. In my opinion, advertisers may consider fingerprinting as a safe harbor, and start building their advertisement strategies around it. Privacy-preserving advertisement techniques are in the initial stages of development and adoption, unlike fingerprinting which has been available for years and has numerous solutions with proven effectiveness. Enhanced Tracking Protection in Safari browser eliminated the problem of third-party cookies. I think, only this kind of solution and strict legal penalties can incentivize advertisers to abandon these solutions. Unfortunately, as I mentioned before, currently there is no comprehensive solution that would eliminate fingerprinting. Development of this solution is a challenging task, that can be considered as future work for this thesis.

4.11 Universal IDs

Universal ID is another solution that can substitute third-party cookies. In this section, I will analyze how it works, what are different types of Universal IDs, and what are privacy and effectiveness concerns about this solution.

4.11.1 How Universal IDs work

There are two types of Universal IDs: Deterministic and Probabilistic.

Deterministic IDs

1. Data collection: The first step is user authentication. A user logs into a website or app by providing credentials like a phone number or email address. After that, the platform that uses Deterministic IDs[6] asks a user for consent and in case of a positive answer, securely collects this information.

2. Data Hashing and Encryption: The next step is hashing. Credentials are processed using cryptographic hash functions like SHA-256[92] that convert credentials into fixed-size strings that are impossible to reverse-engineer. Then, to enhance security unique salts are added. In addition, extra encryption may be applied to protect data during transmission and storage.

3. ID Generation: Hashed and encrypted data makes up a unique and anonymized identifier. To ensure interoperability, participating platforms use standardized identifiers.

4. Identity graph construction: Deterministic ID [114]links devices and platforms users log into using the same credentials. When a user logs in using another device or platform, updates are diffused across the network, hence keeping data synchronized.

5. Data activation: IDs are then used by advertisers and publishers to deliver personalized content and ads. Deterministic IDs also enable measurement and attribution across channels.

Probabilistic IDs

1. Data collection: Probabilistic IDs use non Personally Identifiable Information such as device type, operating system, browser version, IP address, time zone, language settings, and browser patterns. In addition, it collects timestamps, page views, clicks, etc.
2. Feature extraction and normalization: Data is standardized and significant data points are found for accurate user identification.
3. Statistical modeling: In order to find patterns, algorithms that search for patterns and correlations in collected data points are applied[64]. Then, matching accuracy is improved by applying machine learning. Then, according to the likelihood that different data signals belong to the same user, the algorithm assigns probability scores to potential matches.
4. ID Generation: Clusters of data points that represent a probable user profile associated with a unique identifier[64]. This ID is dynamically updated as new data becomes available.
5. Data Activation: Then probabilistic IDs are grouped into audience segments for targeting.

4.11.2 Effectiveness of Universal IDs in different scenarious

Deterministic IDs

Deterministic IDs are effective in logged-in environments due to high accuracy and cross-device tracking[113]. High accuracy is achieved by using consistent credentials that ensure precise identification. Accurate mapping of user behavior across devices is possible due to the same credentials that link multiple devices. In addition, Deterministic IDs allow precise personalization and targeting[90]. Customized experience is achieved by enabling the delivery of personalized content that is based on verified user preferences. Effective retargeting campaigns allow reaching out to users who have previously interacted with specific products or services[90]. However, there are certain limitations of Deterministic IDs. They are less effective when dealing with anonymous traffic because in this case ID cannot be generated for users that do not log in or provide personal information.

Probabilistic IDs

Probabilistic IDs are much more effective in non-logged-in environments[74]. Probabilistic IDs do not require explicit identifiers, hence it covers a much broader audience. It links devices based

on behavioral and technical patterns. In addition, probabilistic IDs allow higher scalability and can be used much broader, targeting users that are not reachable by deterministic methods[74]. Also, when data is not available, it can be substituted by statistical algorithms. However, the accuracy of probabilistic IDs is much lower due to data that is generated by statistical algorithms and machine learning models[90]. Also, it possesses measurement challenges due to the probabilistic nature of data.

User experience improvement

Universal IDs improve user experience:

1. Consistency across devices: Users' preferences are recognized across devices that give them enhanced experience[107]. Personalized content increases user satisfaction and loyalty.

2. Reduced Ad fatigue: Effective frequency capping prevents showing the same ads to users repeatedly, hence improving user experience.

3. Data-driven insights: Comprehensive analytics gives deeper insights into consumer behavior[107]. This results in more relevant ads shown to users. In the long run, users may be more willing to give consent to be tracked. For years, third-party cookie-based strategies were showing irrelevant ads to users, increasing their annoyance.

4. Enhanced segmentation: allows tailoring marketing efforts to specific segments for improved campaigns

Despite the increasing popularity of Universal ID solutions, there are certain limitations that may slow down the adoption of these methods. These solutions significantly rely on data quality and availability[90]. Data signals with low quality and quantity lower effectiveness and reduce accuracy. Additionally, these solutions may be technically complex due to resource intensity and algorithmic limitations[90]. Integration of Universal IDs requires technical expertise and resources, which may be challenging for smaller organizations. Machine learning models behind probabilistic solutions need constant tuning and can not perform well in every scenario. Moreover, a lack of standardization creates interoperability issues and adoption barriers[90]. There are a lot of solutions on the market that do not follow industry-wide standards. Competing interests among stakeholders of these solutions impede widespread adoption.

Privacy limitations of Universal IDs

Universal IDs promise effective ad targeting while respecting user privacy. It may be the case of deterministic IDs, because they require user consent to be created, and companies that create these identifiers share what data they use and for which purposes. In this case, privacy may be in question during the storage phase, when it is in danger of security breaches. Since this IDs are stored on the company server, data breaches may create significant problems.

However, probabilistic IDs may not be as privacy-preserving as deterministic. If we look at the way probabilistic IDs are created, it looks suspiciously like the fingerprinting technique that I described in the previous chapter. Just as fingerprints, probabilistic IDs do not require consent to be created. Just like fingerprints, it uses browser-specific data. The difference is the statistical and machine learning algorithms that Universal IDs use. It sounds like a magic box that data goes through and suddenly it allows more precise ad targeting. I could not find any due diligence of probabilistic ID solutions that would validate that IDs are created in a privacy-preserving way. Even though this solution is still being developed, I assume that authorities who are busy with the judgment of Privacy Sandbox should take action to evaluate the Probabilistic IDs solution. I believe that while authorities are focused on the Privacy Sandbox, they overlook emerging solutions that do not comply with any of the laws.

Chapter 5

Discussion

5.1 Reflections

Analysis of a technology that is being developed is challenging. Google announced that they would keep third-party cookies and instead of Privacy Sandbox, the elevated user experience would be implemented. They have not elaborated on how this new solution will look. It happened two months ago, and still, there is no elaboration. I believe soon they will introduce the elevated user experience they are talking about. If I knew what this solution looked like, that would create valuable input for my project. it is a missing peace that could explain Google's plans for a nearest future.

5.2 Future work

For future work, I would concentrate more on Browser Fingerprinting and Universal IDs. Browser Fingerprinting is extremely invasive, and the fact that currently there is no effective, user-friendly solution against it creates a potential for research. In addition, it will be interesting to create an analysis with the title ''post third-party cookies digital advertising" where after several years of digital advertising evolution, and a full shift from third-party cookies, I would look into the new technological landscape of the industry.

Chapter 6

Conclusion

Digital advertisement is a vibrant technological field that is driven by the hunt for consumer's attention. Nowadays, attention is one of the most valuable assets, and companies continuously improve services and products, in order to deserve a piece of it. Now users have a great variety of products and services to choose from. As more and more companies are using digital channels to reach their audience, competition is getting tougher. The higher the competition, the higher the price for attention. Digital advertisement is getting more expensive, and companies are trying to maximize the effectiveness of their advertising strategies. In addition to increasing costs users, taught by decades of data exploitation and lack of privacy, are becoming more privacy-aware and demanding companies to respect their privacy.

The combination of the above-listed factors resulted in a fundamental technological shift in the digital advertising market. The privacy factor led to decreasing efficiency of existing technologies and marked development of new technologies that would satisfy demands of users and businesses. But fundamental changes do not happen overnight and require joint work of all stakeholders to achieve a better future.

Throughout this project, I managed to analyze the whole cycle of the fundamental shift in digital advertisement market. I looked at this shift through the prism of Privacy Sandbox and third-party cookies. From the beginning of the project I was curious to discover what led to plans about third-party cookies deprecation, and how would the industry survive these changes. Then I found out about the Privacy Sandbox. I managed to understand how it works, analyzed its advantages and disadvantages and its place in the modern digital advertisement market. My project became more challenging when Google decided to make the 180-degree turn and keep third-party cookies, while putting Privacy Sandbox on the shelf as an alternative solution. This pivot was a new challenge for my project. I decided to discover, what led to the decision to keep cookies and how this decision fits into the evolving privacy agenda of the digital advertisement market.

I managed to find out that Privacy Sandbox was not ready to substitute third-party cookies that had been here for years. It showed me, how strong was the influence of this technology, and how hard was to substitute it. However, the progress that started is irreversible, and third-party cookies will slowly die. Advertisers and publishers have to find new solutions. **I realized, that currently there is no one-fit-all solution, and stakeholders most likely will have to incorporate a set of solutions to successfully get user's attention.**That is why I decided to touch upon alternative solutions that currently exist on the market.

Fundamental shifts take time, and I believe that Privacy Sandbox is not the only rise and fall we will see. One thing is certain– third-party cookies will be gone, and changes that are currently happening in the digital advertisement market are creating opportunities for new technologies to rise.

Bibliography

[1] URL: https://medium.com/slido-dev-blog/we-collected-500-000-browser-fingerprints-here-is-what-we-found-82c319464dc9#:~:text=74%25%20of%20desktop%20devices%20can,collected%20on%20iPhones%20were%20unique.

[2] .

[3] YouTube. *Online Video Advertising Campaigns – YouTube Advertising*. YouTube, 2019. URL: https://www.youtube.com/ads/.

[4] *About Shopping campaigns and Shopping ads - Google Ads Help*. support.google.com. URL: https://support.google.com/google-ads/answer/2454022?hl=en.

[5] AdExchanger. *W3C feedback*. AdExchanger, Nov. 2020. URL: https://www.adexchanger.com/data-driven-thinking/what-the-floc-dont-be-a-sheep/ (visited on 09/13/2024).

[6] admin. *Tech Lab Update on UID2.0*. Iabtechlab.com, Feb. 2022. URL: https://iabtechlab.com/tech-lab-update-on-uid2-0/ (visited on 09/28/2024).

[7] Amazon Ads. *What is AdTech? A Beginner's Guide | Amazon Ads*. Amazon Ads, July 2021. URL: https://advertising.amazon.com/library/guides/what-is-adtech#:~:text=Adtech%20helps%20advertisers%20and%20agencies (visited on 09/30/2024).

[8] *Advanced Bot Protection | Bot Management Market Leader | Imperva*. Products, Apr. 2024. URL: https://www.imperva.com/products/advanced-bot-protection/ (visited on 09/25/2024).

[9] Competition and. *Investigation into Google's 'Privacy Sandbox' browser changes*. GOV.UK, Jan. 2021. URL: https://www.gov.uk/cma-cases/investigation-into-googles-privacy-sandbox-browser-changes#full-publication-update-history (visited on 09/24/2024).

[10] Competition and. *Investigation into Google's 'Privacy Sandbox' browser changes*. GOV.UK, Jan. 2021. URL: https://www.gov.uk/cma-cases/investigation-into-googles-privacy-sandbox-browser-changes#full-publication-update-history.

[11] *Archive:Statistics on small and medium-sized enterprises*. ec.europa.eu. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Statistics_on_small_and_medium-sized_enterprises&oldid=262219.

[12] Andrew Blustein. *Apple Has Finally Implemented Its Privacy Overhaul, Here's What You Need to Know*. Adweek.com, Apr. 2021. URL: https://www.adweek.com/programmatic/apple-has-finally-implemented-its-privacy-overhaul-heres-what-you-need-to-know/ (visited on 09/24/2024).

[13] BrowserScan. *The Rise of Browser Fingerprinting: A New Era of Ad Targeting*. Browserscan.net, July 2023. URL: https://www.browserscan.net/blog/rise-of-browser-fingerprinting/ (visited on 09/26/2024).

[14] Bill Budington. *The GDPR and Browser Fingerprinting: How It Changes the Game for the Sneakiest Web Trackers*. Electronic Frontier Foundation, June 2018. URL: https://www.eff.org/deeplinks/2018/06/gdpr-and-browser-fingerprinting-how-it-changes-game-sneakiest-web-trackers.

[15] *Building a more private web: A path towards making third party cookies obsolete*. Chromium Blog, Jan. 2020. URL: https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html.

[16] *Building a more private web: A path towards making third party cookies obsolete*. Chromium Blog, Jan. 2020. URL: https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html.

[17] CafeMedia. *Google delays the removal of third-party cookies until 2024 - CafeMedia*. CafeMedia, July 2022. URL: https://cafemedia.com/google-delays-the-removal-of-third-party-cookies-until-2024/ (visited on 09/29/2024).

[18] Anthony Chavez. *A new path for Privacy Sandbox on the web*. Privacy Sandbox, July 2024. URL: https://privacysandbox.com/news/privacy-sandbox-update/ (visited on 09/15/2024).

[19] Thomas Claburn. *EFF urges Chrome users to get out of the Privacy Sandbox*. www.theregister.com. URL: https://www.theregister.com/2023/09/30/eff_chrome_google_sandbox/.

[20] *CMA and ICO turn up the heat on Google's Privacy Sandbox*. Media Makers Meet | What's new in media, May 2024. URL: https://mediamakersmeet.com/cma-and-ico-turn-up-the-heat-on-googles-privacy-sandbox/ (visited on 09/13/2024).

[21] *CMA to investigate Google's 'Privacy Sandbox' browser changes*. GOV.UK. URL: https://www.gov.uk/government/news/cma-to-investigate-google-s-privacy-sandbox-browser-changes.

[22] *Cover Your Tracks*. coveryourtracks.eff.org. URL: https://coveryourtracks.eff.org/.

[23] CPI. *Smaller Ad-Tech Firms Voice Concerns Over Google's Privacy Sandbox Amid Regulatory Scrutiny | PYMNTS.com*. PYMNTS.com, Sept. 2024. URL: https://www.pymnts.com/cpi-posts/smaller-ad-tech-firms-voice-concerns-over-googles-privacy-sandbox-amid-regulatory-scrutiny/ (visited on 09/19/2024).

[24] datadome. *Data Dome, Inc | DISC Training Certification | Business Assessments*. Data Dome, Nov. 2023. URL: https://datadome.com/ (visited on 09/25/2024).

[25] *Datapult*. Datapult.dk, 2024. URL: https://datapult.dk/ (visited on 09/21/2024).

[26] Brian Dean. *Google Chrome Statistics for 2021*. Backlinko, Mar. 2021. URL: https://backlinko.com/chrome-users.

[27] Chrome for Developers. *Privacy Sandbox: A view into industry's feedback*. YouTube, Mar. 2023. URL: https://www.youtube.com/watch?v=5t83ebP71Yw (visited on 09/29/2024).

[28] *Display Network: Definition - Google Ads Help*. support.google.com. URL: https://support.google.com/google-ads/answer/117120?hl=en.

[29] Dax the duck. *Use DuckDuckGo Extension to Block FLoC, Google's New Tracking Method in Chrome*. Spread Privacy, Apr. 2021. URL: https://spreadprivacy.com/block-floc-with-duckduckgo/ (visited on 09/14/2024).

[30] Yassin El Hardouz. *The Empire Of Google: A Successful Revenue Model*. www.linkedin.com, Sept. 2023. URL: https://www.linkedin.com/pulse/empire-google-successful-revenue-model-yassin-el-hardouz/.

[31] *End to End Campaign Management - Google Display Video 360*. Google Marketing Platform. URL: https://marketingplatform.google.com/about/display-video-360/.

[32] *EUR-Lex - 32002L0058 - EN - EUR-Lex*. Europa.eu, 2021. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058.

[33] *Federated Learning of Cohorts (FLoC) - The Privacy Sandbox*. Privacy Sandbox, 2024. URL: https://privacysandbox.com/intl/en_us/proposals/floc/ (visited on 09/19/2024).

[34] *Fingerprint*. Fingerprint, 2024. URL: https://fingerprintjs.com/ (visited on 09/25/2024).

[35] *Firefox Privacy Notice*. Mozilla, Oct. 2019. URL: https://www.mozilla.org/en-US/privacy/firefox/.

[36] *Fraud Detection Prevention Solutions - Advanced Multifactor Authentication Solutions*. TransUnion. URL: https://www.iovation.com/.

[37] *[GA4] Enroll in Analytics Academy courses on Skillshop - Analytics Help*. Google.com, 2019. URL: https://support.google.com/analytics/answer/15068052#zippy=.

[38] GDPR. *General data protection regulation (GDPR)*. General Data Protection Regulation (GDPR), 2018. URL: https://gdpr-info.eu/.

[39] Vinay Goel. *An updated timeline for Privacy Sandbox milestones*. Google, June 2021. URL: https://blog.google/products/chrome/updated-timeline-privacy-sandbox-milestones/.

[40] *Google Ad Manager - Integrated Advertising Management Platform*. Google.com, 2019. URL: https://admanager.google.com/home/.

[41] *Google Ads – få nye kunder, og øg salget vha. onlineannoncering*. Google Ads, 2024. URL: https://ads.google.com/intl/da_dk/start/overview-ha/?subid=dk-da-ha-aw-bk-c-bau (visited on 08/26/2024).

[42] *Google Sandbox: Online tracking instead of privacy*. noyb.eu, 2024. URL: https://noyb.eu/en/google-sandbox-online-tracking-instead-privacy (visited on 09/24/2024).

[43] *How We're Protecting Your Online Privacy - The Privacy Sandbox*. Privacy Sandbox, 2024. URL: https://privacysandbox.com/intl/en_us/open-web/ (visited on 09/04/2024).

[44] *IAB website*. iabtechlab.com. URL: https://iabtechlab.com/.

[45] *ICO statement in response to Google announcing it will no longer block third-party cookies in Chrome*. Ico.org.uk, July 2024. URL: https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2024/07/ico-statement-in-response-to-google-announcing-it-will-no-longer-block-third-party-cookies/ (visited on 09/24/2024).

[46] *Introducing Google Marketing Platform - Campaign Manager 360 Help*. Google.com, 2019. URL: https://support.google.com/campaignmanager/answer/9015629?hl=en (visited on 08/26/2024).

[47] *Investigation into Google's 'Privacy Sandbox' browser changes*. GOV.UK. URL: https://www.gov.uk/cma-cases/investigation-into-googles-privacy-sandbox-browser-changes.

[48] Josh Isaac. *Google Privacy Sandbox: The Impact On Advertisers And Publishers - Next Millennium Media*. Next Millennium Media, Feb. 2024. URL: https://nextmillennium.io/blog/google-privacy-sandbox-the-impact-on-advertisers-and-publishers/ (visited on 09/09/2024).

[49] jiamin. *Three things we need to do as an industry to make the Privacy Sandbox work for Advertisers - GroupM*. GroupM, Aug. 2024. URL: https://www.groupm.com/three-things-we-need-to-do-as-an-industry-to-make-the-privacy-sandbox-work-for-advertisers/ (visited on 09/09/2024).

[50] Kristin Jones. *The Importance of First-Party Data in a Cookieless World | Porch Group Media*. Porchgroupmedia.com, 2024. URL: https://porchgroupmedia.com/blog/the-importance-of-first-party-data-in-a-cookieless-world/ (visited on 09/19/2024).

[51] Tamas Kadar. *What is Browser Fingerprinting How Does it Work?* SEON, May 2020. URL: https://seon.io/resources/browser-fingerprinting/.

[52] Kasada. *Kasada | Protection from Automated Threats | Bot Mitigation*. Kasada. URL: https://www.kasada.io/.

[53] Richie Koch. *Cookies, the GDPR, and the ePrivacy Directive*. GDPR.eu, May 2019. URL: https://gdpr.eu/cookies/.

[54] Daniel Konstantinovic. *Privacy Sandbox testers raise concerns about latency and signal loss*. EMARKETER, July 2024. URL: https://www.emarketer.com/content/privacy-sandbox-testers-signal-loss-latency-cookies (visited on 09/19/2024).

[55] Daniel Konstantinovic. *Privacy Sandbox testers raise concerns about latency and signal loss*. EMARKETER, July 2024. URL: https://www.emarketer.com/content/privacy-sandbox-testers-signal-loss-latency-cookies.

[56] Pierre Laperdrix et al. "Browser Fingerprinting". In: *ACM Transactions on the Web* 14 (Apr. 2020), pp. 1–33. DOI: 10.1145/3386040. URL: https://arxiv.org/pdf/1905.01051.pdf.

[57] Brian LaRue. *What Are Deterministic and Probabilistic IDs?* AdMonsters, Feb. 2018. URL: https://www.admonsters.com/ad-ops-decoder-what-are-deterministic-and-probabilistic-ids/#:~:text=Probabilistic%20identifiers%20use%20a%20wide (visited on 09/29/2024).

[58] Dave Lee. *The Cookie Won't Crumble No Matter How Hard Google Tries*. Bloomberg.com, July 2024. URL: https://www.bloomberg.com/opinion/articles/2024-07-26/the-cookie-won-t-crumble-no-matter-how-hard-google-tries?srnd=opinion&embedded-checkout=true (visited on 09/24/2024).

[59] *Manage your ad privacy in Chrome - Google Chrome Help*. Google.com, 2019. URL: https://support.google.com/chrome/answer/13355898?hl=en#zippy=%2Cmanage-ad-topics (visited on 09/24/2024).

[60] *Memo -IAB France's competition concerns over Privacy Sandbox's newly released API Topics*. URL: https://www.alliancedigitale.org/wp-content/uploads/2024/03/IAB-France-Memo_Topics-API.pdf (visited on 09/21/2024).

[61] Arvind Narayanan and Dillon Reisman. *The Princeton Web Transparency and Accountability Project*. URL: https://www.cs.princeton.edu/~arvindn/publications/webtap-chapter.pdf.

[62] *Number of Ad Block Users Worldwide (2024)*. Exploding Topics, June 2024. URL: https://explodingtopics.com/blog/ad-block-users.

[63] *Overcoming signal loss in advertising | illumin*. illumin, May 2024. URL: https://illumin.com/insights/blog/overcoming-signal-loss-in-advertising/ (visited on 09/21/2024).

[64] *Panorama Identity - Lotame*. Lotame, July 2024. URL: https://www.lotame.com/panorama-identity/ (visited on 09/28/2024).

[65] Todd Parsons. *Privacy Sandbox Testing Results Show Shortfalls to Meet CMA Requirements | Criteo*. Criteo, June 2024. URL: https://www.criteo.com/blog/privacy-sandbox-testing-results-show-shortfalls-to-meet-cma-requirements/ (visited on 09/14/2024).

[66] Todd Parsons. *The Bottom Line of Privacy Sandbox Testing: What You Need to Know | Criteo*. Criteo, Mar. 2024. URL: https://www.criteo.com/blog/the-bottom-line-of-privacy-sandbox-testing-what-you-need-to-know/ (visited on 09/19/2024).

[67] Catherine Perloff. *Buyers Are Wasting Money on Alt IDs While Cookies Still Persist*. Adweek.com, Apr. 2024. URL: https://www.adweek.com/programmatic/buyers-are-wasting-money-on-alt-ids-while-cookies-still-persist/ (visited on 09/24/2024).

[68] *Preparing for the end of third-party cookies | Privacy Sandbox*. Google for Developers. URL: https://developers.google.com/privacy-sandbox/blog/cookie-countdown-2023oct.

[69] *Privacy*. W3C. URL: https://www.w3.org/mission/privacy/.

[70] *Privacy Sandbox*. Iabtechlab.com, July 2024. URL: https://iabtechlab.com/standards/privacysandbox/ (visited on 09/21/2024).

[71] *Privacy Sandbox Fit Gap Analysis for Digital Advertising*. URL: https://iabtechlab.com/wp-content/uploads/2024/02/Privacy-Sandbox-Fit-Gap-Analysis-PUBLIC-COMMENT-RELEASE.pdf (visited on 09/13/2024).

[72] *Privacy Sandbox Fit Gap Analysis for Digital Advertising*. URL: https://iabtechlab.com/wp-content/uploads/2024/02/Privacy-Sandbox-Fit-Gap-Analysis-PUBLIC-COMMENT-RELEASE.pdf.

[73] *Privacy Sandbox Latency Issues Will Affect Publishers*. Pubmag.ru, 2024. URL: http://pubmag.ru/en/adexchanger-privacy-sandbox-latency-issues-publishers-impact/ (visited on 09/13/2024).

[74] *Probabilistic vs deterministic: Which method should you be using for identity resolution?* www.mparticle.com. URL: https://www.mparticle.com/blog/probabilistic-vs-deterministic/.

[75] *Protected Audience API overview*. Google for Developers, 2022. URL: https://developers.google.com/privacy-sandbox/private-advertising/protected-audience (visited on 09/19/2024).

[76] *Publishers vs Advertisers: What's the difference?* www.adbutler.com. URL: https://www.adbutler.com/blog/article/publishers-vs-advertisers-differences-explained.

[77] *Quantitative testing of Google's Privacy Sandbox technologies -seeking input from affected firms and others on the CMA's proposals*. 2022. URL: https://assets.publishing.service.gov.uk/media/6363b00de90e0705a8c3544d/CMA_Experiments_note.pdf (visited on 09/14/2024).

[78] *Recital 30 - Online identifiers for profiling and identification*. GDPR.eu, Nov. 2018. URL: https://gdpr.eu/recital-30-online-identifiers-for-profiling-and-identification/.

[79] *Results from Privacy Sandbox APIs testing - Google Ad Manager Help*. Google.com, 2019. URL: https://support.google.com/admanager/answer/15189422?hl=en (visited on 09/14/2024).

[80] Daniel Ruby. *111 Google Ads Statistics For 2023 (Revenue, Data Trends)*. DemandSage, Mar. 2023. URL: https://www.demandsage.com/google-ads-statistics/.

[81] Allison Schiff. *Criteo: The Privacy Sandbox Is NOT Ready Yet, But Could Be If Google Makes Certain Changes Soon*. AdExchanger, June 2024. URL: https://www.adexchanger.com/privacy/criteo-the-privacy-sandbox-is-not-ready-yet-but-could-be-if-google-makes-certain-changes-soon/.

[82] Allison Schiff. *Influential W3C Working Group Calls Privacy Sandbox Proposal 'Harmful'*. AdExchanger, Apr. 2021. URL: https://www.adexchanger.com/privacy/influential-w3c-working-group-calls-privacy-sandbox-proposal-harmful/ (visited on 09/19/2024).

[83] *SecureAuth - Workforce and Customer Identity Access Management*. SecureAuth, Aug. 2024. URL: https://www.secureauth.com/ (visited on 09/25/2024).

[84] Rebecca Sentance. *Google's Privacy Sandbox: What are the latest concerns?* Econsultancy, July 2024. URL: https://econsultancy.com/google-privacy-sandbox-concerns-third-party-cookies/.

[85] *Shifting from 3rd party cookies to another identity solution in the U.S. 2020*. Statista. URL: https://www.statista.com/statistics/1222326/third-party-cookies-identity-solution-usa/.

[86] Shreya. *Internet Cookie Statistics: Key Trends and Insights*. CookieYes, Sept. 2023. URL: https://www.cookieyes.com/blog/internet-cookie-statistics/.

[87] Brave Software. *Why Brave Disables FLoC*. Brave, Apr. 2021. URL: https://brave.com/blog/why-brave-disables-floc/ (visited on 09/14/2024).

[88] Richard Speed. *Google's Privacy Sandbox more like a privacy mirage, campaigners claim*. Theregister.com, June 2024. URL: https://www.theregister.com/2024/06/13/noyb_gdpr_privacy_sandbox/ (visited on 09/13/2024).

[89] Aimee Newell Tarín. *Cookie Deprecation is Dead: What Should the Industry Do Now? - ExchangeWire.com*. Exchangewire.com, 2024. URL: https://www.exchangewire.com/blog/2024/07/24/cookie-deprecation-is-dead-what-should-the-industry-do-now/ (visited on 09/24/2024).

[90] Rob Taylor. *Alternative IDs may hold the key to cookieless advertising's future*. Criteo, Mar. 2024. URL: https://www.criteo.com/blog/alternative-ids-the-future-of-cookieless-advertising/.

[91] Teads. *New Study Finds Only 32% Of Global Publishers Are Actively Preparing For The Cookieless Future*. Teads, May 2024. URL: https://www.teads.com/2024-publisher-cookie-prepartation/ (visited on 09/21/2024).

[92] National Institute of Standards and Technology. *Secure Hash Standard (SHS)*. csrc.nist.gov, Aug. 2015. URL: https://csrc.nist.gov/pubs/fips/180-4/upd1/final.

[93] *The European ePrivacy Regulation*. www.european-eprivacy-regulation.com. URL: https://www.european-eprivacy-regulation.com/.

[94] *The Privacy Sandbox: Technology for a More Private Web*. privacysandbox.com. URL: https://privacysandbox.com/.

[95] *Third-party cookies*. Google for Developers, 2024. URL: https://developers.google.com/privacy-sandbox/cookies (visited on 09/16/2024).

[96] *Third-Party Cookies and Their Impact on Privacy | Cardlytics*. www.cardlytics.com. URL: https://www.cardlytics.com/blog/third-party-cookies-and-their-impact-on-privacy.

[97] *ThreatMetrix - Cybersecurity Risk Management | LexisNexis Risk Solutions*. LexisNexis Risk Solutions, 2024. URL: https://risk.lexisnexis.com/global/en/products/threatmetrix?utm_campaign=bsgmif20.fremeaops.tmxweb&utm_medium=vanityurl&utm_source=pdf&utm_content=threatmetrixwebpage (visited on 09/25/2024).

[98] Trey Titone. *What is FLEDGE? Google FLEDGE Explained*. Ad Tech Explained, Mar. 2021. URL: https://adtechexplained.com/fledge-explained/ (visited on 09/14/2024).

[99] *Topics API: Relevant Ads without Cookies - The Privacy Sandbox*. Privacy Sandbox, 2021. URL: https://privacysandbox.com/intl/en_us/proposals/topics/ (visited on 09/19/2024).

[100] *Tracking Prevention Policy*. WebKit, Aug. 2019. URL: https://webkit.org/tracking-prevention-policy/.

[101] *Universal ID - definition*. Clearcode, 2022. URL: https://clearcode.cc/glossary/universal-id/#:~:text=A%20universal%20ID%20is%20a (visited on 09/29/2024).

[102] *Unpacking the IAB Tech Lab's Privacy Sandbox Analysis: A Call to Action for the Digital Ad Industry - AlgoriX*. AlgoriX, Mar. 2024. URL: https://www.algorix.co/unpacking-the-iab-tech-labs-privacy-sandbox-analysis-a-call-to-action-for-the-digital-ad-industry/ (visited on 09/13/2024).

[103] Usercentrics. *European Data Protection Board guidelines for consent*. Usercentrics.com, 2024. URL: https://usercentrics.com/knowledge-hub/edpb-guidelines-for-consent/.

[104] *Web Platform Design Principles*. W3.org, July 2024. URL: https://www.w3.org/TR/design-principles/#leave-the-web-better (visited on 09/24/2024).

[105] *WebKit*. WebKit. URL: https://webkit.org/.

[106] *What are Ad Auctions? The Definitive Guide*. Kevel.com, 2024. URL: https://www.kevel.com/blog/ad-auctions.

[107] *What are Universal ID solutions, and how do they work? | Didomi*. Didomi.io, 2024. URL: https://www.didomi.io/blog/universal-id-solutions (visited on 09/28/2024).

[108] *What does 'grounds of legitimate interest' mean?* commission.europa.eu. URL: https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_en.

[109] *What is a Cookie?* SearchSoftwareQuality. URL: https://www.techtarget.com/searchsoftwarequality/definition/cookie.

[110] *What is a Third-Party Cookie?* WhatIs.com. URL: https://www.techtarget.com/whatis/definition/third-party-cookie.

[111] *Why Privacy Sandbox is a Good Paradigm Shift for Consumers*. Metarouter.io, 2024. URL: https://www.metarouter.io/post/why-privacy-sandbox-is-a-good-paradigm-shift-for-consumers (visited on 09/19/2024).

[112] WICG. *turtledove/fledge-tester-list.md at main · WICG/turtledove*. GitHub, 2020. URL: https://github.com/WICG/turtledove/blob/main/fledge-tester-list.md (visited on 09/16/2024).

[113] Maciej Zawadziński. *Deterministic and Probabilistic Matching: How Do They Work? - Clearcode Blog*. Clearcode | Custom AdTech and MarTech Development, Dec. 2016. URL: https://clearcode.cc/blog/deterministic-probabilistic-matching/.

[114] *"IdentityLink" is Now RampID™*. LiveRamp, May 2021. URL: https://liveramp.com/blog/identitylink-now-rampid/.