Clicking into Exposure: Uncovering Privacy Risks of Google Click Identifier in YouTube Ads

Ha Dao
Max Planck Institute for Informatics
hadao@mpi-inf.mpg.de

Abhishek Shinde
Saarland University
absh00002@stud.uni-saarland.de

Sana Athar
Max Planck Institute for Informatics
sathar@mpi-inf.mpg.de

Devashish Gosain
Indian Institute of Technology Bombay
dgosain@cse.iitb.ac.in

Abstract

YouTube is one of the largest video platforms on the web, with Google Ads deeply integrated into the viewing experience. While users may expect some level of tracking during ad delivery, the extent and mechanics of Google Ads tracking on YouTube, particularly the tracking behaviors triggered by user interactions with ads, remain underexplored. To address this gap, for the first time, we develop *YT-AdTrack*, a fully automated framework that measures tracking initiated by YouTube ads across 430 top-trending videos, three widely used browsers, and six geographic locations. In our *baseline* measurement campaign, *YT-AdTrack* strategically accepts cookie banners on YouTube, interacts with displayed ads, and subsequently accepts cookie banners on advertiser landing pages to capture downstream tracking behavior.

Our findings show that *every* ad click consistently carries a unique Google Click Identifier, `gclid`, which is propagated through redirection chains and ultimately embedded in the advertiser's landing page. We further observe that 64 (out of 76) advertisers persist this identifier as a first-party cookie, thereby transforming a short-lived click token into a durable user identifier. In addition, `gclid` values frequently leak across parties from advertisers, exposing them to both Google-controlled services and external third-party ad networks, which exacerbates the tracking nexus by extending well beyond standard conversion measurement. Strikingly, even when cookie banners are rejected, ad interactions remain consistently tagged: 55.4% of advertisers store `gclid` as a cookie, and 18.9% enable auto-tagging, which allows Google to directly persist the identifier. This demonstrates that banner rejection does not safeguard users from `gclid`-based tracking.

We find these behaviors to be consistent across browsers, with advertisers persisting the identifier in 76.4–84.2% of cases and Google directly storing it in over two-thirds of interactions. Similarly, across six geographic locations, `gclid`-based tracking persists, with advertisers storing it in 72.5–88.5% of cases and Google's auto-tagging active in all locations. Overall, our analysis reveals that a single ad click can initiate durable cross-site tracking that persists across various banner choices, browser environments, and regional contexts.

Proceedings on Privacy Enhancing Technologies 2026(2), 92–107

https://doi.org/10.56553/popets-2026-0038

Keywords

Google Click Identifier, gclid, Tracking Cookies, Web Tracking, Cookie Banner, Navigational Tracking, Cross-Site Tracking

1 INTRODUCTION

Online advertising fuels much of today's web ecosystem, enabling free access to content and services. At the core of this ecosystem lies ad attribution, the process of linking user interactions with advertisements (e.g., clicks) to subsequent actions (e.g., purchases). To perform attribution, platforms have historically relied on identifiers such as third-party cookies or mobile advertising IDs. However, the tightening of privacy regulations (e.g., GDPR [1], CCPA [2]) and growing browser-level restrictions (e.g., Safari's ITP [60], Chrome's cookie phaseout [20]) have eroded the viability of these traditional identifiers. In response, large platforms, including Google and Meta, have introduced new mechanisms for attribution that embed identifiers directly within ad click URLs.

As the dominant player in both search and video advertising, Google employs an identifier, Google Click Identifier (`gclid`), across its advertising products, including YouTube. Every time a user clicks on a Google-served ad, the advertiser's landing page URL is appended with a `gclid` parameter (see Figure 1). According to Google's documentation, the `gclid` serves as a pseudonymous token enabling advertisers to track conversions. For advertisers, this design provides a convenient way to measure ad campaign effectiveness. For Google, however, every `gclid` is inherently connected to its broader advertising infrastructure, including user accounts, devices, and ad delivery systems.

Prior work has focused on advertising and conversion contexts: TrafficGuard [58] highlights its role in conversion tracking and campaign optimization, while Nimbata [39] notes its integration with CRM systems[1] to improve lead attribution. Beyond advertising, recent research has identified a broader trend toward UID smuggling, where unique identifiers are embedded in URLs to preserve cross-site linkage despite cookie restrictions [3, 10, 17, 36, 44]. Yet, the specific behavior of `gclid` within complex web-based advertising environments, such as YouTube, remains largely unexplored.

Thus, in this paper, we present a first systematic analysis of `gclid`-based tracking in the YouTube web-based advertising ecosystem. We introduce *YT-AdTrack*, a novel framework that automatically detects and interacts with advertisements on YouTube. The framework collects cookies and network traffic during ad clicks,

[1]CRM: Customer Relationship Management software for managing customer interactions.

enabling a systematic analysis of the privacy risks associated with Google's click-based advertising in the YouTube ecosystem. By gathering 430 trending videos across seven countries using the YouTube Data API, we conduct four measurement campaigns: (i) a *baseline* run that accepts cookie banners on YouTube and the advertiser landing page, (ii) a *rejection* run that declines them, (iii) a *multi-browser* run using Chrome, Firefox, and Edge, and (iv) a *multi-vantage points* run from different locations with signed-in Google accounts. These experiments enable us to analyze how ad clicks expose the `gclid` identifier and to evaluate the influence of cookie banner interactions, browser choice, and geographic location on tracking behaviors (§ 4).

Overall, our main findings can be summarized as follows:

- We find that every ad interaction on YouTube covertly embeds a unique `gclid`, which is not only stored by advertisers as a long-lived cookie, but also propagated through Google's infrastructure and unexpectedly further leaked to 133 third-party domains embedded on advertiser sites. As a result, a single ad click can expose the click identifier to Google, Meta, Microsoft, and other ad tech firms, extending the reach of this identifier far beyond its intended role in conversion measurement (§ 5.1).
- Regarding the effect of banner interaction, we see that rejecting banners does not reduce `gclid`-based tracking, with all 568 ad interactions still tagged; moreover, around 55.4% of advertisers (41 out of 74) stored the `gclid` as a first-party cookie, and 14 advertisers enabled auto-tagging that allowed `googleadservices.com` to directly persist the identifier as a cookie (§ 5.2).
- When examining how different browsers impact the propagation of `gclid` following an ad interaction, we observe that, similar to Chrome, the identifier consistently accompanies ad interactions across Edge and Firefox. Advertisers persisting `gclid` as a first-party cookie in 76.4% of cases on Edge (120 out of 157) and 79.4% on Firefox (143 out of 180), while Google itself also directly stored the identifier in over two-thirds of cases in both browsers (§ 5.3).
- Under the signed-in account configuration, `gclid` tagging consistently accompanies ad interactions. Using six geographic locations, we also find that `gclid`-based tracking remained consistent, with nearly every ad click carrying the identifier, advertisers persisting it as a first-party cookie in 72.5–88.5% of cases (lowest in Germany, highest in the USA - New York, and Google's auto-tagging mechanism directly setting the identifier as a cookie at all vantage points (§ 5.4).

Finally, we discuss the expected and observed handling of `gclid`, its relation to GDPR consent boundaries, possible defenses at the browser and network levels, and the ethical considerations and limitations of our study (§ 6).

2 BACKGROUND

In this section, we provide background on the Google Click Identifier and define key terms that will be used throughout the paper.

2.1 Google Click Identifier (`gclid`)

Google Ads is Google's online advertising platform that enables advertisers to display targeted ads across search results, YouTube, and partner websites, using real-time bidding and detailed user data for personalization and measurement [52]. Through this ecosystem, advertisers can target specific audiences and monitor the effectiveness of their campaigns across different services. The Google Click Identifier (`gclid`) is a URL parameter automatically appended to the destination URLs of Google Ads when auto-tagging[2] is enabled.

The `gclid` uniquely identifies each ad click, facilitating the tracking and attribution of user interactions across Google Ads and linked platforms, such as Google Analytics [19]. The `gclid` enables precise measurement of conversions, including both online and offline events, by linking user actions back to specific ad campaigns and keywords. This functionality is used for advertisers to evaluate the effectiveness of their advertising efforts and refine their strategies accordingly.

Figure 1 shows how `gclid` operates in the attribution process. When a user clicks on a Google Ad, the advertiser's landing page loads with a unique `gclid` parameter appended to the URL. This identifier is then stored by the advertiser's website as a first-party cookie, typically via the Google Ads conversion linker tag in `gtag.js` or Google Tag Manager, ensuring it persists across the user's browsing session. Suppose the advertiser uses Google Ads or Marketing Platform tags (e.g., conversion tag, remarketing tag, or conversion linker). In that case, these scripts also copy the `gclid` into a cookie associated with `googleadservices.com`. If the user subsequently performs a conversion action (e.g., completing a purchase), the advertiser's site records this event along with the stored `gclid` and transmits it back to Google Ads. Google then uses the `gclid` to link the recorded conversion to the specific ad click that initiated the user's visit, thereby completing the attribution loop.

2.2 Term Definitions

We first define some frequently used terms in this paper:

- **URL path**: the sequence of complete URLs observed from the initial request (originator) to the destination, including all intermediate redirectors (e.g., `a.com/x/y?UID=123` → `b.com/x/y?UID=123`).
- **Domain path**: the sequence of domains corresponding to each step of the same *URL path* (e.g., `a.com` → `b.com`).
- **Redirector**: any intermediate domain in the *URL path* that forwards the request to another location, typically via an HTTP redirect (e.g., `redirector.com/redirect?UID=123`).

3 RELATED WORK

Web tracking techniques have undergone significant evolution, adapting to and often circumventing emerging privacy mechanisms [6]. Traditionally, browsers used a shared cookie jar model. In this model, cookies set by third-party domains, such as advertising networks or analytics services, could be accessed whenever those domains were embedded on any site. This facilitated pervasive and often non-consensual cross-site tracking [18], raising significant privacy concerns. To mitigate this, some browsers initially introduced third-party cookie blocking [5, 34, 60]. However, this approach was found to have limitations against more evasive tracking techniques, such as navigational tracking [29, 44], fingerprinting [27, 28, 38], and CNAME cloaking [11, 14].

[2]Auto-tagging is a setting in the Google Ads account. When enabled, it adds a `gclid` to the end of the landing page URL, just before any part that starts with a # (called URL fragment).

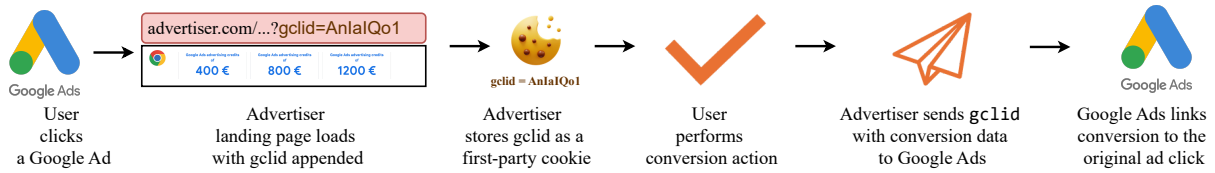


Figure 1: Workflow of how `gclid` is used in the attribution process. A conversion action is a specific user activity that is valuable to an advertiser, such as making a purchase, filling out a form, downloading an app, or visiting a specific page.

3.1 Navigational Tracking

Trackers increasingly exploit navigational and redirect-based tracking, leveraging user navigation flows and intermediate hops to identify users across sites. By embedding identifiers within URLs or inserting intermediate redirect chains, these mechanisms often bypass storage-based defenses. A notable variant, known as bounce tracking, involves redirecting users through tracker-controlled domains that set first-party cookies to persist identifiers across sites even when third-party cookies are blocked [29]. Redirect-based tracking has been extensively examined for its role in phishing and malicious redirection attacks [9, 40, 48, 59], while bounce tracking has been studied for its capacity to enable cross-site user re-identification despite client-side mitigations [41, 42, 49]. Koop et al. [29] conducted a comprehensive study on bounce tracking and found that 11.6% of Alexa top 50k websites use redirectors capable of storing first-party tracking cookies, even when third-party cookies are blocked. Similarly, Brave researchers [50, 51] analyzed how websites and trackers use HTTP redirects to track users, often in ways that are invisible to users, eluding most privacy tools.

While bounce tracking is increasingly constrained by partitioned storage in modern browsers, trackers have adapted through UID smuggling, which embeds unique identifiers (UIDs) into URLs (query parameters) to maintain linkage across otherwise isolated contexts. Chouaki et al. [10] found that even privacy-focused search engines (DuckDuckGo, StartPage, Qwant) engage in navigational tracking after ad clicks, often exceeding traditional engines (Google, Bing), in post-click data flows. Randall et al. [44] further found UID smuggling on 8.1% of unique URL paths, likely driven by affiliate and attribution markets seeking to maintain conversion visibility despite cookie blocking. Munir et al. [36] measured the ubiquity of link decoration for tracking and proposed PURL, a sanitization approach, highlighting that decorated links on top sites routinely carry identifiers and sensitive data.

Recent research has extended these findings to platform-specific identifiers. Prior work by Bekos et al. [3] showed that Facebook's `fbclid`, when combined with the Facebook Pixel, enables persistent tracking of users across websites and over time by linking earlier browsing activity to Facebook accounts. More recently, El Fraihi et al. [17] examined how `fbclid` serves as the basis for the first-party `_fbc` cookie, which—together with Meta's server-side Conversions API—improves user matching between client- and server-side events. Their measurements show that Meta's Conversions API can associate 34–51% of website visitors with user profiles using coarse identifiers such as IP address, user-agent, and geolocation, effectively bypassing browser-based tracking protections.

In contrast, `gclid` operates within Google's advertising ecosystem and primarily relies on client-side propagation and storage mechanisms integrated into web-based ad delivery. Both `fbclid` and `gclid` are platform-based click identifiers appended as a query parameter to track outbound user clicks and support ad conversion attribution. Although they share similar functions, their technical implementations and privacy implications differ substantially, particularly in how they persist and propagate across web contexts. While `fbclid` has been studied extensively in the context of Meta's tracking infrastructure, the behavior and privacy implications of `gclid` are not yet well understood. Our work extends this line of research by presenting the first systematic, in-depth analysis of `gclid`-based navigational tracking via YouTube ads. Unlike previous studies that have mainly focused on bounce tracking, UID smuggling, social click IDs, or server-side APIs in general web environments, we examine how a conversion-measurement identifier like `gclid`—originally intended for attribution—persists and propagates beyond consent boundaries. This reveals how advertising infrastructure can transform legitimate analytics mechanisms into resilient tracking vectors, raising new questions about consent enforcement and data exposure in Google's advertising ecosystem.

3.2 YouTube's Advertising Ecosystem

YouTube's advertising ecosystem is intricately designed to leverage user data for targeted advertising and content recommendations. It displays a range of ad formats, including skippable and non-skippable in-stream ads, bumper ads, overlay ads, and display ads [61], which can appear before, during, or alongside videos. These ads are primarily managed through Google Ads, enabling advertisers to target users based on demographics, interests, watch history, and other behavioral signals. YouTube's monetization model is heavily reliant on user engagement metrics, such as ad impressions, watch time, and click-through rates, as well as whether users skip ads, which directly influences advertiser bidding and creator revenue. In 2024, YouTube generated nearly $36 billion in ad revenue, making it one of the largest digital advertising platforms globally, second only to Google Search [26].

YouTube plays a crucial role in Google's advertising system because it combines a massive audience with seamless integration into Google Ads. Through Google Ads, advertisers can run video campaigns directly on YouTube, tapping into Google's rich data on user interests, demographics, and behaviors to fine-tune their targeting [47]. This integration and the resulting flow of ad clicks (and associated `gclid` values) make YouTube a key node in Google's end-to-end attribution pipeline—allowing advertisers to track how

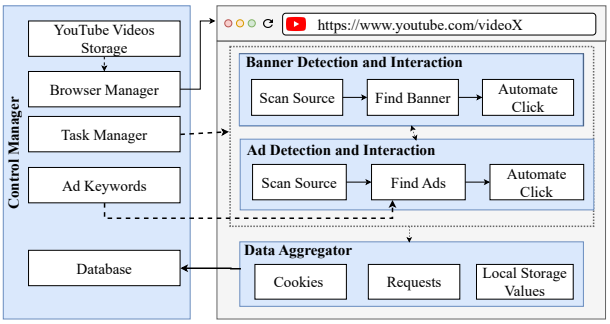


Figure 2: Overview of the *YT-AdTrack* framework.

viewers interact with ads, measure conversions, and adjust spending in real time, all within the same platform [7].

Recent work by Mai et al. [30] examined how YouTube's privacy settings affect ad delivery, showing that disabling ad personalization can paradoxically increase both ad volume and exposure to predatory ads. While their findings highlight the consequences of user privacy choices, our work addresses a complementary dimension of YouTube's web-based advertising ecosystem. Despite the central role of click-based identifiers (e.g.,`gclid`) in ad attribution, their behavior and privacy implications have not been systematically studied within the YouTube environment. Our empirical analysis fills this gap by characterizing how `gclid` is introduced after ad clicks, persists via cookies set by advertisers, and is transmitted to third-party domains regardless of consent settings, browsers, or geographies.

4 METHODOLOGY

In this section, we present the methodology used to study `gclid`-based tracking in YouTube's advertising ecosystem, including the design of our crawling system, the data collection process, and the detection of potential navigational tracking.

4.1 Crawling System

To investigate the privacy risks of YouTube ad interactions, we developed *YT-AdTrack*, a measurement framework that implements a fully automated pipeline for ad interaction and data collection. The framework consists of two main components: the *Control Manager*, which coordinates browser sessions and data storage, and the *Task Manager*, which executes in-browser interactions and data collection. Figure 2 provides an overview of these components and their interaction in the *YT-AdTrack* framework:

- *Control Manager*: The control manager orchestrates the measurement process. It maintains the storage of YouTube video links to be visited, initializes and configures browser instances via Selenium-Wire version 5.1.0[3], and provides keyword lists to guide ad detection. For traffic interception, Selenium-Wire extends traditional Selenium[4] by employing Mitmproxy version 11.0.2[5] as an underlying proxy to capture HTTPS traffic. Before each run, we install a custom root certificate into both the operating system's and browser's trust stores to prevent certificate errors. This setup enables us to comprehensively collect cookies, storage values, and all HTTP(S) requests and responses. The control manager also coordinates task execution (e.g., banner interaction, ad clicking) and stores all captured cookies, storage values, and HTTP(S) request/response records in a structured database for further analysis.
- *Task Manager*: The task manager operates inside the browser context and is responsible for (i) detecting and interacting with cookie banners, (ii) identifying and clicking on YouTube ads, and (iii) collecting cookies, storage values, and network requests throughout the session. It consists of three submodules:
  - *Banner interaction*: Prior work shows that interacting with cookie banners affects tracking behavior [13, 46]. Thus, to interact with cookie banners, *YT-AdTrack* integrates and extends *BannerClick* [46], a tool designed to automatically detect and interact with cookie banners. *BannerClick* achieves high accuracy (about 99%) in automating banner interactions and has recently been updated to support a broader range of banner types [45]. Note that we further evaluated the performance of *BannerClick* through manual verification of both acceptance and rejection interactions, achieving accuracies of 96.3% and 96.2%, respectively (see Appendix A). On every video and destination page load, the system invokes *BannerClick* to detect and interact with the banner by simulating either an "Accept" or "Reject" action, depending on the experimental configuration. While *BannerClick* was originally restricted to Firefox, we extended its implementation to support Chromium-based browsers (Chrome, Edge, Brave), enabling consistent cross-browser interaction.
  - *Ad detection and interaction:* During video playback, *YT-AdTrack* monitors the YouTube interface for advertisements. To identify ad components, the system applies a set of CSS selectors (`#player-ads`, `.video-ads`, `a[hrefˆ="https://www.googleadservices.com/pagead/aclk?"]`, `div.ytp-visit-advertiser-link` `span.ytp-visit-advertiser-link__text`)[6]. We filter detected elements for visibility and interactivity. If multiple candidates are present, we randomly select one to reduce systematic bias. Once an element is selected, we simulate a user click and monitor the browser for the opening of a new tab corresponding to the destination page. If no ad is detected, or if the click does not result in a new navigation (e.g., due to the ad disappearing during interaction), we log the event as unsuccessful and continue the session.
  - *Data aggregator*: A data aggregator captures cookies, web requests, and local storage values during the process.

4.2 Data Collection

We utilized the YouTube Data API [22] to collect 430 unique trending videos over three consecutive days across seven countries in February 2025: Germany, Sweden, India, the USA, Australia, Brazil,

[3]https://pypi.org/project/selenium-wire/
[4]https://pypi.org/project/selenium/
[5]https://www.mitmproxy.org/

[6]We tested the ad detection component on a random sample of 50 videos and manually observed no missed advertisements, suggesting that our detection approach is reliable in practice.

and South Africa. Note that, to focus on content more likely to deliver ads, we only retained videos with a minimum duration of five minutes. This cutoff was chosen empirically, as very short videos (e.g., clips under a few minutes) are often less likely to carry pre-roll advertising. In contrast, longer videos consistently trigger such ads more often.

We then use *YT-AdTrack* to conduct four measurement campaigns to analyze the privacy risks of YouTube ad interactions. To account for the inherent variability of ad delivery on YouTube, we repeat every iteration five times.

- *Baseline* run: In this measurement campaign, we run Chrome in headless mode from a server located in Germany and accept YouTube's cookie banner as well as cookie banners on advertiser landing pages (see Figure 3). In each iteration, *YT-AdTrack* sequentially visits all 430 collected videos in a stateless browser and, for each video, loads and plays a trending video while continuously monitoring the player for ads. When *YT-AdTrack* detects an ad, it identifies all visible, interactive ad elements (e.g., call-to-action overlays, companion banners), randomly selects one, and performs a simulated click. If no ad appears during playback, or if the ad disappears before the click reaches a landing page, *YT-AdTrack* logs the attempt as unsuccessful and proceeds to the next video. When the click succeeds, *YT-AdTrack* visits the advertiser's landing page, detects and accepts the cookie banner if present, and then reloads the page once to capture additional resources and delayed requests. At each of these steps, *YT-AdTrack* collects cookies, JavaScript-accessible cookies, local and session storage values, navigational requests, and all HTTP(S) requests and responses. Screenshots are also captured at each stage for further verification.
- *Rejection* run: To evaluate whether the banner interaction impacts ad click-based tracking, we configure *YT-AdTrack* to reject cookie banners on both YouTube and advertiser landing pages. We repeat the *baseline* procedure under this configuration and collect the resulting data.
- *Multi-browser* run: To evaluate potential variations in `gclid`-based tracking behavior across different browsers, we configure *YT-AdTrack* to run the baseline campaign in Firefox and Edge, alongside Chrome. We intentionally exclude Brave from this comparison, as it already strips identifiers such as the `gclid` parameter from URLs [57], which we manually verified. These browsers were selected for their distinct approaches to handling tracking parameters and privacy controls that may influence `gclid` propagation. Chrome serves as the reference point, as it natively supports `gclid` attribution within Google's advertising and analytics ecosystem. Edge, which shares the Chromium core, integrates Microsoft's privacy features such as SmartScreen and tracking prevention [33]. Firefox employs Enhanced Tracking Protection, which blocks known trackers and restricts third-party cookies [35]. This configuration enables a controlled comparison of browser-specific privacy mechanisms and their effects on the persistence and transmission of `gclid` in ad interactions. To reflect typical user configurations, we use each browser's default tracking protection settings and collect data to assess whether browser choice influences `gclid`-based tracking behavior.
- *Multi-vantage points* run: To investigate how geographical location impacts ad delivery and tracking triggered by ad clicks, we configure *YT-AdTrack* to run the baseline campaign in six geographic locations via Proton VPN[7], using a signed-in Google account: Germany, Australia, India, Brazil, USA (California), and USA (New York). These geographic locations were selected to capture a diverse segment of YouTube's global advertising ecosystem, spanning both developed and emerging markets with varying levels of advertiser activity and YouTube penetration [54]. Germany represents a GDPR-regulated region [1]; California reflects a major U.S. ad market under CCPA regulation [2]; New York provides a non-CCPA U.S. baseline; and Australia, India, and Brazil represent geographically distributed markets with distinct ad inventories and localization practices. The goal is not to compare ad volumes across regions but to examine whether `gclid` tagging persists consistently across diverse advertising and regulatory environments. We note that a signed-in account is required because YouTube flags traffic originating from VPN endpoints as automated activity. Without an account, every crawl triggers mandatory CAPTCHA challenges before video playback, making data collection infeasible. To ensure consistency, we created country-specific accounts while being connected to the corresponding country's VPN endpoint and used them for corresponding country-specific crawls.

We conducted our experiments on seven virtual machines running Debian GNU/Linux 12 (bookworm). Each instance was provisioned under VMware full virtualization, equipped with four CPU cores and 8 GB of RAM.

4.3 Detecting `gclid` Exposure

We first construct the redirection chain by extracting the *URL path* observed after each ad click, from the originator to the final destination page, including all intermediate redirectors. Each hop is validated using HTTP response metadata: a hop is recorded when the response contains a `Location` header together with a redirect status code (`301`, `302`, `307`, or `308`) [32]. The `Location` value specifies the following URL in the path. This validated chain forms the basis for `gclid` redirection, enabling us to analyze where identifiers are introduced, propagated, or transformed across intermediaries (e.g., in query parameters, `Referer` headers, or cookie-setting).

We then analyze the validated redirection chain and subsequent requests from the advertiser landing page to detect potential exposure of the extracted `gclid` values. We consider three vectors through which `gclid` may be propagated beyond the advertiser's control: (i) the inclusion of the whole landing URL in `Referer` headers attached to outgoing requests, (ii) direct requests to third-party URLs in which the `gclid` parameter appears explicitly in the query string, and (iii) cookies set by embedded third-party domains where the stored values contain `gclid`. By inspecting these signals, we can determine whether the `gclid` value introduced at the ad click is propagated to the advertisers and beyond, thereby revealing the specific client-side pathways through which third-party entities may gain access to the identifier.

Note that we also attempt to detect other user identifiers (UIDs) in our dataset (see Appendix B). However, we find that `gclid` is the

[7] https://protonvpn.com/

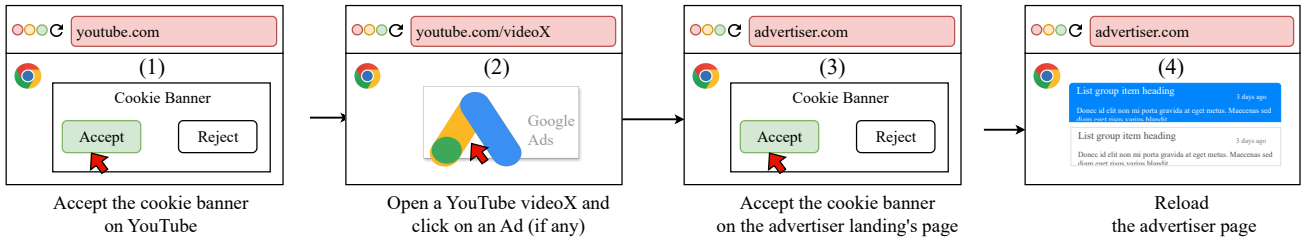


Figure 3: Overview of the measurement workflow for a single video under the *baseline* configuration.

only identifier systematically used for tracking when users click on ads on YouTube. We assume that this is because YouTube, as part of Google's advertising infrastructure, is tightly integrated with Google Ads and therefore relies exclusively on `gclid` as its standard mechanism for click and conversion attribution.

5 RESULTS

In this section, we present the outcomes of our measurements of `gclid`-based tracking in YouTube's advertising system. We begin by examining the exposure of `gclid` in the advertising ecosystem. Next, we analyze the effect of cookie banner rejection on this behavior. We then investigate whether browser choice influences the extent of `gclid`-based tracking by comparing results across Chrome, Edge, and Firefox. Finally, we study geographic variation by conducting measurements from six geographic locations, highlighting how location may shape ad-related tracking practices. We note that we do not perform statistical significance analysis among different configurations and therefore refrain from making causal claims. Instead, we clarify that the observed differences between configurations are not statistically significant but rather illustrate the persistent presence of the `gclid`-based tracking across all configurations—irrespective of cookie banner interaction, browser choice, or geographic location.

5.1 Exposure Of `gclid` In The Advertising Ecosystem

Metric	Baseline
Total Video Visits	430 × 5
Ad Interactions w/ Successful Advertiser Landing Page Visit	568
Unique Advertisers	76
Unique URL Paths w/ `gclid`	589
Ad Interactions w/ ≥1 URL Path w/ `gclid`	568
Unique Advertisers that Stored `gclid` as a Cookie	64

Table 1: Summary statistics of video visits, ad interactions, and propagation of `gclid` collected in the *baseline* configuration involving Chrome browser with the cookie banner accepted in Germany.

5.1.1 Overview. We summarize the statistics of the *baseline* configuration collected in Germany using the Chrome browser with the accepted cookie banners in Table 1. Across 2,150 video visits, we successfully interacted with 568 ads, resulting in 76 unique advertisers. In total, these interactions generated 589 URL paths that contained the `gclid` parameter. When aggregated at the interaction level, we observe that all 568 ad interactions included at least one URL path carrying `gclid`, showing that the parameter was systematically embedded in advertiser redirections, and that every ad click was consistently tagged with a unique `gclid` value.

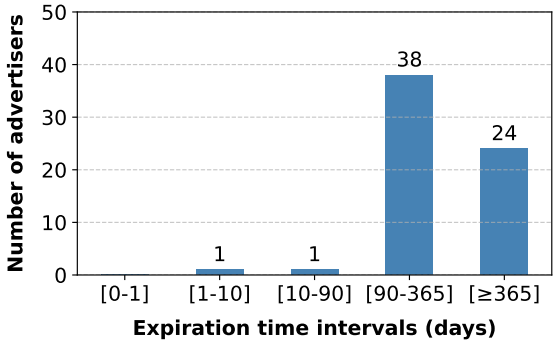


Figure 4: Distribution of maximum expiration times of first-party cookies storing the `gclid` value across 64 advertisers. Most cookies were configured with lifetimes of 90–365 or ≥365 days, extending a short-lived tracking token into a long-term identifier.

Notably, 64 destinations stored the `gclid` value as a first-party cookie. Although storing `gclid` in this way is part of Google's recommended setup for conversion tracking [24], persisting it in a cookie transforms it from a short-lived token into a long-lived identifier that is automatically sent on every revisit, enabling the destination to recognize returning visitors even when they access the site directly rather than through an ad click. Our analysis of expiration intervals shows that the maximum expiration times of `gclid` cookies were configured to 90–365 days (38 advertisers) or ≥365 days (24 advertisers) for the majority of advertisers, thereby extending the persistence of `gclid` far beyond its intended short-term use (see Figure 4).

5.1.2 How `gclid` is Transmitted to Advertisers. Table 2 shows the distribution of the 83 unique domain paths containing `gclid` observed between ad clicks and advertisers. 59.04% of paths involve a direct redirection from *www.googleadservices.com* to the advertiser, highlighting its central role in ad navigation. 28.92% of paths include both *www.googleadservices.com* and *ad.doubleclick.net*, and 8.43% originate from *ad.doubleclick.net* before reaching the advertiser

Path	Number	Percentage
www.googleadservices.com → Advertiser	49	59.04%
www.googleadservices.com → ad.doubleclick.net → Advertiser	24	28.92%
ad.doubleclick.net → Advertiser	7	8.43%
www.googleadservices.com → ad13.adfarm1.adition.com → Advertiser	1	1.20%
www.googleadservices.com → ad.doubleclick.net → servedby.flashtalking.com → Advertiser	1	1.20%
ad13.adfarm1.adition.com → Advertiser	1	1.20%

Table 2: Distribution of domain paths containing `gclid`. Percentages are based on the 83 unique domain paths. Each domain is shown in a consistent color.

Leakage channel	Advertiser (#/%)	Receiver (#/%)
Cookies	55 / 72.4%	4 / 3.0%
Referer header	15 / 19.7%	81 / 60.9%
URL parameter	76 / 100.0%)	75 / 56.4%
Total	76 / 100.0%	133 / 100%

Table 3: Breakdown of `gclid` leakage to third-party domains. Percentages are given out of a total of 76 unique advertiser's domains and 133 unique receivers (third-party domains).

landing page. In addition, when clicking on ads delivered through Google's network of domains (e.g., Google Ads or DoubleClick), the click leads to domain paths that involve *ad13.adfarm1.adition.com*, operated by ADITION [56], a European provider of programmatic advertising solutions, and *servedby.flashtalking.com*, operated by Flashtalking [16], an ad-serving and analytics platform.

Our findings demonstrate that `gclid` is not only propagated through Google's infrastructure but also transmitted by third-party ad networks, thereby extending the exposure of this identifier beyond Google's ecosystem. We also confirm that this behavior is consistent across different experimental setups, including the *rejection*, *multi-browser*, and *multi-vantage points* configuration runs (see Table 7, Table 8, and Table 9 in the Appendix).

5.1.3 Escalation of `gclid` *into cross-party leakage.* We next examine whether `gclid` values, once passed in the URL to advertiser destinations, can be further transmitted beyond the advertiser. To this end, we inspect requests triggered from the advertiser's landing page, focusing on three possible transmission channels:

- The full landing URL included in `Referer` headers
- Third-party requests whose URLs carry the `gclid` parameter
- Cookies set by embedded third-party domains containing the `gclid` value.

We observed that among 76 advertisers, `gclid` values were transmitted to 133 distinct third-party domains via the `Referer` header, direct URL parameter requests, or cookies. The most common pattern was exposure to three third-party domains per site, which we observed among 11 advertisers. The highest number of third-party domains receiving `gclid` from an advertiser was 41[8]. We further observe that for 55 out of 76 advertisers with auto-tagging enabled, *www.googleadservices.com* sets a cookie that stores the `gclid` value, thereby allowing Google to persist the identifier itself.

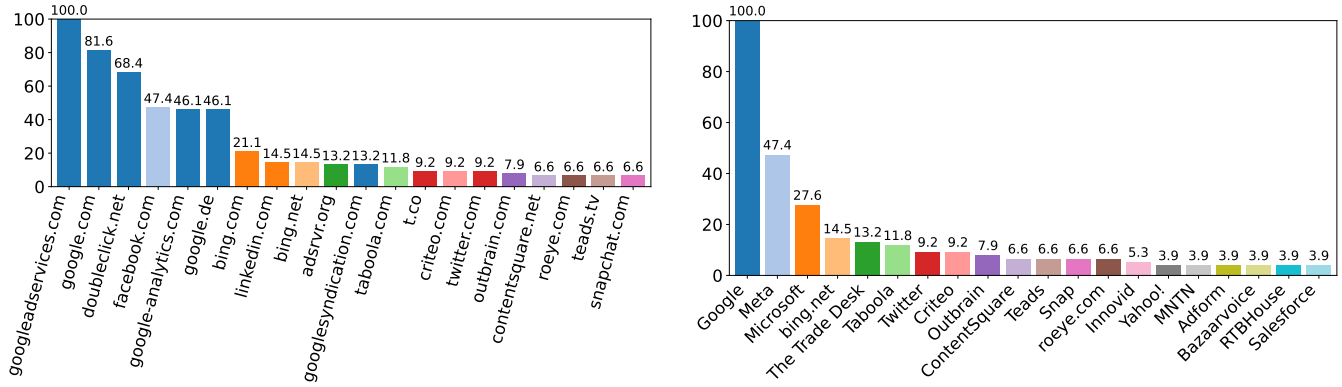
As summarized in Table 3, we first observe accidental leakage cases, in which 15 advertisers propagate `gclid` values to 81 receivers via `Referer`-based leakage[9]. Furthermore, we identify intentional leakage, where 76 advertisers leak `gclid` directly to 75 receivers through URL parameters, and 55 advertisers share them with 4 distinct third-party domains via cookies. Overall, `gclid` can propagate beyond the advertiser's domain through multiple leakage channels, likely maximizing `gclid` collection and synchronization, which are highly valuable within the tracking ecosystem.

Figure 5 presents the top 20 third-party domains receiving `gclid` values and their aggregation by company ownership, where entities are matched using the Disconnect tracking protection list [15]. We find that Google-controlled services receive `gclid` from all 76 advertiser destinations, highlighting Google's central role in collecting and consolidating data from ad interactions across all the advertisers we examined. Since these values are unique for each ad click and are consistently propagated, Google can link user interactions across multiple advertiser sites, strengthening its ability to create detailed cross-site user profiles. At the same time, other major companies such as Meta, Microsoft, and The Trade Desk also receive `gclid`, expanding the scope of exposure beyond Google's infrastructure. This indicates that a single ad click on YouTube might not only be propagated into Google's attribution and tracking systems but also transmitted to other large ad tech firms. These companies could add the identifier to their own tracking systems, thereby widening the network of parties that could access user interactions across different contexts.

Key takeaway: All ad visits from YouTube are associated with a unique `gclid` value. Furthermore, `gclid` is both embedded in advertiser redirection chains and persisted as a first-party cookie, transforming it from a short-lived query parameter into a long-lived identifier. Finally, a single ad click on YouTube propagates `gclid` into Google's tracking systems and may also transmit it to other large ad tech firms, such as Meta, Microsoft, and The Trade Desk, via embedded third-party resources on advertiser landing pages.

[8] www.centerparcs.de

[9] As discussed in Ref. [43, 53], `Referer`-based leakage occurs when a webpage's URL is included in the HTTP `Referer` header and transmitted to third-party domains. In our context, this mechanism unintentionally exposes identifiers, gclid values, when they appear in advertiser URLs and are subsequently exposed through the standard behavior of the browser's `Referer` mechanism.



(a) Top 20 Third-party domains

(b) Top 20 Third-party companies

Figure 5: gclid escalating to cross-party leakage on advertiser's landing page, where gclid is included in the advertiser, are further transmitted to embedded third-party domains, expanding the tracking surface beyond the initial ad click. Domains belonging to the same company are shown in a consistent color. Percentages are based on the 76 unique destination domains.

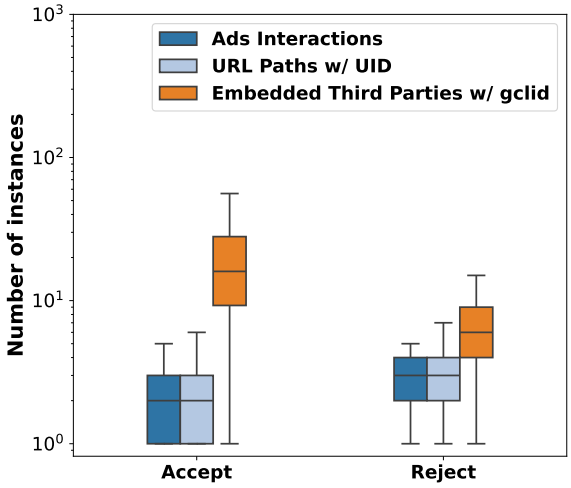


Figure 6: Distribution of ad interactions and gclid-based tracking paths per video under *baseline* run (accept banner) and *rejection* run (reject banner). Each box represents the per-video totals, aggregated across five runs.

5.2 Impact of Banner Rejection On gclid-based Tracking

Here, we present how rejecting cookie banners influences the propagation of gclid after ad interactions, depicted in Figure 6. As already mentioned in § 4.2, we configure *YT-AdTrack* to reject cookie banners on both the YouTube and the advertiser landing pages. In the *baseline* (accept) configuration, each video produced, on average, 2.08 ad interactions and 2.18 URL paths with gclid, indicating a near one-to-one relationship between clicks and gclid propagation. Under the *rejection* configuration, there are 2.76 ad interactions and 3.06 URL paths with gclid, meaning that rejecting banners results in more URL paths carrying gclid per video. Although the number of ad interactions may differ between runs, gclid consistently accompanies ad interactions in both configurations.

For embedded third parties receiving gclid, we observed an average of 19.97 per video in the *accept* configuration and 8.99 per video in the *rejection* configuration, since rejecting cookie banners on some advertiser landing pages prevents certain advertising and analytics scripts from executing, thereby lowering the opportunities for gclid to be transmitted. In addition, under the *rejection* configuration, we observed that 41 out of 74 unique advertisers set the gclid value as a first-party cookie on their own domains (see Table 4 in Appendix). We also find that when 14 advertisers enable auto-tagging, www.googleadservices.com sets a cookie containing the gclid value, allowing Google to persist the identifier directly.

Key takeaway: Rejecting cookie banners does not prevent the use of gclid in YouTube ad interactions. Every ad click continues to be tagged with a gclid value. While rejecting banners reduces the extent of leakage to embedded third parties by blocking some advertising and analytics scripts, gclid is still persisted as a cookie by many advertisers and by www.googleadservices.com through auto-tagging.

5.3 Impact of Browser On gclid-based Tracking

We then examine how different browsers influence the propagation of gclid following ad interactions, as shown in Figure 7.

In the Edge browser, each video generated on average 2.45 ad interactions and 2.58 URL paths carrying gclid, indicating a close correspondence between ad clicks and identifier propagation. The number of embedded third parties receiving gclid decreased to 17.36 per video. We further observed that advertisers persisted gclid as a first-party cookie in 120 out of 157 cases (see Table 5 in Appendix), and that www.google.com sets a cookie containing the identifier in 104 out of 157 cases.

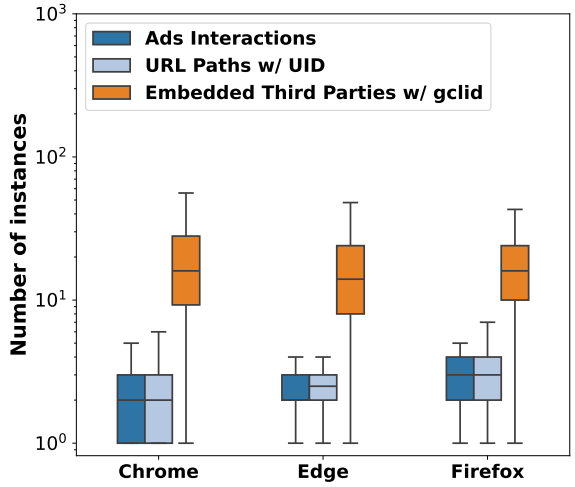


Figure 7: Distribution of ad interactions and gclid-based tracking paths per video under the *Accept* banner interaction mode across three browsers. Each box summarizes per-video event totals, aggregated over five repeated runs.

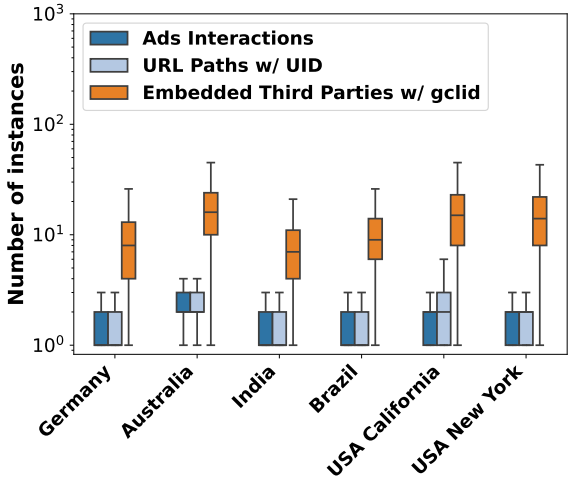


Figure 8: Distribution of ad interactions and gclid-based tracking paths per video under the *Accept* banner interaction mode across six geographic locations. Each box represents event totals per video, aggregated over five repeated runs.

In the Firefox browser, we observed 3.11 ad interactions and 3.24 URL paths with gclid per video. The number of embedded third-party recipients remained comparable to Edge at 17.87 per video. Advertisers persisted gclid as a first-party cookie in 143 out of 180 cases, while www.google.com set a cookie containing the identifier in 127 out of 180 cases.

We note that this behavior differs from Chrome in the baseline configuration, where the cookie containing gclid is set by www.googleadservices.com. In contrast, both Firefox and Edge store the gclid cookie under the www.google.com domain, suggesting that Google adapts the storage domain based on the browser environment. Although the number of ad interactions and URL paths differs slightly between browsers, gclid consistently accompanies ad interactions, is frequently persisted as a cookie, and is transmitted to third-party domains in all three browsers, including Chrome in the *baseline* configuration.

Key takeaway: gclid-based tracking is prevalent across different browsers. Every ad click continues to be tagged with a gclid value. While the number of ad interactions and URL paths differs slightly between Edge, Firefox, and Chrome, gclid is frequently persisted as a cookie by advertisers through auto-tagging and is transmitted to third-party domains on advertiser landing pages.

5.4 Variation of gclid-based Tracking Across Geographic Locations

In this section, we report how geographic differences influence the propagation of gclid after ad interactions from different geographic locations using a signed-in account, as shown in Figure 8.

We first confirm that when using a signed-in account, every ad click continues to be tagged with a gclid value. Although the number of ad interactions and URL paths differs slightly from a signed-out account (see Figure 6, under the *baseline* run), the gclid tagging persists regardless of account state, highlighting the consistent and pervasive nature of gclid propagation.

In Germany and Australia, on average, we observed 1.48 and 2.34 ad interactions per video, respectively, and 1.64 and 2.53 URL paths with gclid, respectively, depicting that each click was typically accompanied by gclid propagation. A near one-to-one ratio of ad interactions and URL paths with gclid was also observed for India (1.34:1.53), Brazil (1.46:1.57), California, USA (1.85:2.03), and New York, USA (1.70:1.89). First-party cookies set by advertisers using gclid remained high in all locations, ranging from 72.5% in Germany to 88.46% in the United States (New York) (see Table 6 in Appendix). In addition, in all geographic locations, we observe a third-party cookie set by www.googleadservices.com, which stores the gclid value directly, consistent with Google's auto-tagging mechanism that automatically persists the identifier for attribution. The embedded third parties receiving gclid, on average per video, were the highest in the USA (New York - 18.66, California - 17.04), and Australia (18.19).

Key takeaway: Under the signed-in account configuration, gclid tagging consistently accompanies ad interactions. Although geographic variation influences the scale of propagation, gclid consistently accompanies ad interactions, is frequently persisted as a cookie, and is transmitted to third-party domains across all geographic locations.

6 DISCUSSION

In this section, we discuss the expected and observed handling of gclid, its relation to GDPR consent boundaries, potential mitigations at the browser and network levels, the ethical considerations, and the limitations of our study.

6.1 Expected vs. Observed Handling of gclid

Based on Google's attribution design described in § 2.1, the expected handling of gclid is confined to advertiser and Google-operated domains. Google encourages advertisers to store the gclid value as a first-party cookie and share it with Google Ads or Google Analytics for conversion measurement. Under this workflow, the gclid should not persist beyond the defined attribution window, nor be transmitted to unrelated third parties.

Our measurements, however, reveal broader propagation of gclid values to third-party domains beyond Google's own services. We observe that gclid identifiers are included in requests to unrelated analytics, marketing, and remarketing platforms automatically triggered during page load. This form of cross-party leakage extends the scope of gclid beyond its intended attribution purpose, allowing independent third parties to associate ad-click data with their own identifiers. Such behavior deviates from Google's stated design and raises privacy concerns by enabling cross-site profiling and re-identification across advertising networks. These findings underscore the need for stricter tag-scoping policies and stronger browser-level controls to prevent identifier propagation beyond legitimate attribution contexts.

Furthermore, according to Google's documentation, the storage of gclid is not expected when users deny consent for advertising-related data collection. Google's Consent Mode [21] and Tag Manager Consent APIs [23] define distinct consent types and states, with ad_storage specifically governing the handling of advertising cookies and related identifiers. Under a denied consent state, no advertising cookies — including those derived from click-based identifiers such as gclid — should be stored, transmitted, or used for ad attribution. Advertisers integrating Google tags are therefore required to respect these consent signals and ensure compliance with both Google's framework and data protection laws such as the GDPR, which mandates informed and enforceable consent across all tracking mechanisms. However, our measurements reveal a clear misalignment between these documented expectations and real-world practices. We observed that the gclid parameter often persisted as a first-party cookie even when users rejected cookie consent. This indicates that either advertisers' configurations fail to set up Google's consent APIs or that they deliberately bypass consent enforcement to preserve attribution functionality. Such deviations undermine the effectiveness of cookie banners and erode user control, raising compliance concerns under the GDPR's principles of *lawfulness, fairness, and transparency*.

These findings also highlight the importance of advertiser education and configuration practices. Advertisers should ensure that tracking scripts respect users' cookie rejections and refrain from sharing gclid values with external third parties. Strengthening guidance and documentation from Google—particularly regarding consent handling, tag configuration, and proper use of gclid parameters—could help prevent unexpected behaviors.

6.2 Ad Click Identifiers and the Boundaries of GDPR Consent

The technical design of the gclid parameter also raises broader privacy considerations. Each Google ad click generates a unique gclid that is appended to the advertiser's landing page URL. Advertiser websites typically capture and store this value as a first-party cookie to facilitate conversion tracking—ensuring that when a user completes an action (e.g., a purchase or signup), the conversion can be attributed to the original ad click. Although gclid represents a single interaction, multiple such identifiers can potentially be linked across sessions and contexts when combined with other signals (e.g., first-party cookies, device fingerprints, or logged-in account information). Consequently, what appears to be a transient click-level identifier could, in practice, contribute to broader user profiling across sites and services. Our results show that gclid-based tracking persists even when users reject cookie banners, indicating a possible gap between user consent choices and the behavior of advertising tags in practice. This misalignment may undermine user expectations regarding consent and data minimization, and highlights the need for clearer accountability in advertiser tag configurations as well as stronger enforcement of consent propagation across the ad ecosystem. These observations raise an important compliance question: if gclid continues to be appended in URLs, and be stored as a first-party cookie, even after users reject cookie banners, does this behavior align with the principles of consent under the GDPR? The gclid can serve as a linkable token capable of enabling cross-site tracking even in the absence of cookie storage, which could raise concerns under both the GDPR and the ePrivacy Directive (ePD). Both frameworks require user consent for any mechanism that stores or accesses information on user devices—extending beyond cookies to include URL parameters, tracking pixels, and unique identifiers such as gclid [4]. Moreover, such identifiers are rarely disclosed in cookie banners, which may raise transparency and purpose limitation concerns under Article 5(1)(a) of the GDPR. While industry actors may justify gclid use under *legitimate interest* (Art. 6(1)(f)), regulatory bodies such as the European Data Protection Board (EDPB) and national data protection authorities (e.g., CNIL) have clarified that identifiers transmitted via mechanisms other than cookies—such as URL parameters or fingerprinting—are subject to the same consent standards [25]. In this light, the persistence of gclid following cookie rejection could be viewed as a form of consent ambiguity, underscoring the need for further legal and technical scrutiny rather than constituting a definitive GDPR breach.

6.3 Mitigations at the Browser Level and Beyond

Beyond Chrome and Edge, some browsers deploy stronger defenses against tracking. Brave strips common tracking parameters such as gclid, fbclid[10], and msclkid[11] from URLs before navigation, directly preventing the kind of link-decoration tracking we observed in our study [57]. Such URL parameters are used to tag users across sites, enabling persistent cross-site tracking even in the absence of cookies [3]. This highlights the importance of parameter-stripping as a mitigation strategy. Firefox's Enhanced Tracking Protection (ETP) primarily restricts third-party cookies and known tracker domains but does not strip URL parameters like gclid or fbclid,

[10] Facebook Click Identifier is a unique tracking parameter automatically added by Facebook to outgoing links shared on its platform.
[11] Microsoft Click Identifier is a unique identifier automatically added to the end of a URL when you enable auto-tagging in Microsoft Advertising.

consistent with our observation of high tracking incidence on Firefox. Safari's Intelligent Tracking Prevention (ITP) blocks third-party cookies, limits first-party storage, and downgrades referrer information, reducing—but not fully eliminating—navigational tracking risks. In contrast, Tor Browser standardizes configurations, blocks advanced fingerprinting vectors, and leverages network anonymity, offering the strongest defense even against complex tracking forms [31]. Overall, only browsers that combine parameter-stripping (as in Brave) with privacy-by-design architectures (as in Tor) effectively mitigate the link-decoration vectors highlighted by both our results and [3], while mainstream browsers continue to leave users exposed.

Lightweight browser extensions can automatically sanitize tracking parameters without compromising website functionality—for instance, the PURL system [37] demonstrated this capability by stripping decorated links across the web at scale. Network-level defenses are also feasible. For example, a DNS resolution system LDPRESOLVE [8] shows how resolvers can filter or anonymize queries before they reveal an identifier pattern, proving to be a viable defense that can be integrated at the resolver or client side to mitigate DNS-based user tracking without completely breaking DNS-based services. These approaches extend protection beyond browser boundaries, offering users defense even when site-level or browser-level controls fall short. However, their deployment requires careful engineering to avoid disrupting legitimate ad-attribution flows and ensuring compliance with site analytics needs.

6.4 Ethical Considerations

This study automates interactions with YouTube ads to investigate tracking behaviors that occur only after user engagement has occurred. These behaviors are invisible to passive observation. Our goal is to understand how ad platforms track users beyond ad impressions. All interactions are limited to what is necessary for measurement and are conducted with care to avoid unnecessary impact on advertisers or platforms.

We also note that *YT-AdTrack* measurements do not capture the actual user behavior, e.g., what they intend to buy. Thus, our tool cannot be persuaded to make a purchase after clicking an ad. Therefore, it can be argued that our clicks create potential financial losses for advertisers. However, precisely quantifying the potential advertising costs resulting from our experiments is challenging. Randall et al. [44] argued that several factors may influence the cost involved. For instance, advertisements can be charged in different ways, such as cost-per-thousand views (CPM), cost-per-click (CPC), or cost-per-action (CPA). Moreover, different ads cost different amounts depending on the publisher and placement. Importantly, our methodology aligns with previous studies that also used controlled ad-click automation to analyze online advertising and navigational tracking [10, 44].

In addition, the digital ad industry is a trillion-dollar industry [55], driven largely by profiling and targeting individual users. Thus, academic research, including direct engagement with ad systems to measure practices like `gclid` smuggling (which attempts to bypass privacy protections), is crucial. Such research offers valuable insights for consumers, regulators, and developers of privacy-enhancing technologies. We believe these benefits far outweigh any minor financial cost to advertisers that our experiments have caused. We will make our analysis scripts, raw dataset, and our findings publicly available. The *YT-AdTrack* framework will be shared upon reasonable research request, rather than through full public release, to prevent potential misuse (e.g., facilitating fraudulent ad-click activities) while still supporting reproducibility and further research in the community.

6.5 Limitations and Future Work

Our study, while providing the first systematic analysis of `gclid`-based tracking, has some limitations. First, our measurements are restricted to YouTube's web interface, even though a significant portion of usage occurs on mobile devices and within the YouTube app, where different identifiers and app-based telemetry may alter tracking pathways. The app environment may differ substantially from the web interface, motivating future work to extend our analysis to mobile and app ecosystems for a more comprehensive understanding of `gclid`-based tracking within the broader YouTube Ads infrastructure. Secondly, given the rapid evolution of Google Ads and YouTube's tracking infrastructure, our results may not necessarily hold over time. We therefore intend to conduct longitudinal studies to systematically monitor changes in tracking practices and the persistence of `gclid` over time. Third, our crawling relied on automated environments with specific browsers, VPN geographic locations, and scripted ad interactions, which cannot fully reproduce the heterogeneity of real user behavior, such as variable view times, scrolling patterns, and device diversity. Finally, while we included vantage points across six geographic locations, this coverage does not represent the full spectrum of global regulatory regimes. Expanding future measurements to a broader set of regions would provide a more representative understanding of how legal and policy contexts shape `gclid`-based tracking.

7 CONCLUSION

In this paper, we presented the first systematic study of navigational tracking in YouTube's advertising ecosystem, with a focus on the role of the Google Click Identifier `gclid`. Using our novel automated framework, *YT-AdTrack*, we demonstrated that every ad click consistently appends a unique `gclid` to advertiser destinations, where it is often persisted as a first-party cookie and further propagated to third-party services. We showed that this identifier enables long-lived cross-site recognition, persists even when users reject cookie banners, and propagates across browsers and geographic regions. Our findings highlight how an attribution mechanism originally intended for campaign measurement operates as a robust tracking channel, raising concerns about user consent, regulatory compliance, and privacy exposure. By uncovering these risks, we aim to advocate for stronger privacy-enhancing technologies and regulatory frameworks that can effectively address identifier-based navigational tracking on large-scale advertising platforms.

Availability: To foster reproducibility and further research, we have made our datasets and analysis scripts publicly available at [12]. The *YT-AdTrack* framework will also be available from the authors on request for research purposes.

ACKNOWLEDGMENTS

This research was supported by the Max Planck Society. We appreciate the anonymous PoPETs Editor and Reviewers for their valuable feedback, which significantly improved the paper. The authors used generative AI-based tools Grammarly and ChatGPT-5 to revise the text, correct any typos, grammatical errors, and awkward phrasing. No content was generated related to technical results, data, code, or analysis.

References

[1] 2016. General Data Protection Regulation (GDPR). Official Journal of the European Union, L119, 1–88. https://gdpr-info.eu/ Accessed: 2025-08-27.

[2] 2018. California Consumer Privacy Act (CCPA). California Legislative Information, California Civil Code §1798.100 et seq.. https://cppa.ca.gov/regulations/pdf/ccpa_statute.pdf Accessed: 2025-08-27.

[3] Paschalis Bekos, Panagiotis Papadopoulos, Evangelos P Markatos, and Nicolas Kourtellis. 2023. The Hitchhiker's guide to facebook web tracking with invisible pixels and click IDs. In *Proceedings of the ACM Web Conference (WWW)*. ACM, 2132–2143.

[4] European Data Protection Board. 2024. Guidelines 2/2023 on Technical Scope of Article 5(3) of the ePrivacy Directive. https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202302_technical_scope_art_53_eprivacydirective_v2_en_0.pdf Accessed: 2025-08-29.

[5] Brave Software. 2023. Brave blocks… Cookie consent notices. https://brave.com/did-you-know/brave-blocks-cookie-consents/ Accessed: 2025-05-24.

[6] Tomasz Bujlow, Valentín Carela-Español, Josep Solé-Pareta, and Pere Barlet-Ros. 2017. A Survey on Web Tracking: Mechanisms, Implications, and Defenses. *Proc. IEEE* 105, 8 (2017), 1476–1510.

[7] Google Ads Help Center. 2025. Link Your YouTube Channel to Google Ads for Conversion Tracking. https://support.google.com/youtube/answer/3063482?hl=en Accessed: 2025-08-29.

[8] Deliang Chang, Joann Qiongna Chen, Zhou Li, and Xing Li. 2022. Hide and seek: Revisiting dns-based user tracking. In *Proceedings of the IEEE 7th European Symposium on Security and Privacy (EuroS&P)*. IEEE, 188–205.

[9] Juan Chen and Chuanxiong Guo. 2006. Online detection and prevention of phishing attacks. In *Proceedings of the International Conference on Communications and Networking in China (Chinacom)*. IEEE, 1–7.

[10] Salim Chouaki, Oana Goga, Hamed Haddadi, and Peter Snyder. 2023. Understanding the privacy risks of popular search engine advertising systems. In *Proceedings of the ACM Internet Measurement Conference (IMC)*. ACM, 370–382.

[11] Ha Dao, Johan Mazel, and Kensuke Fukuda. 2021. CNAME cloaking-based tracking on the web: Characterization, detection, and protection. *Transactions on Network and Service Management* 18, 3 (2021), 3873–3888.

[12] Ha Dao, Abhishek Shinde, Sana Athar, and Devashish Gosain. 2025. Raw dataset and analysis scripts for Google Click Identifier in YouTube Ads measurement. https://doi.org/10.17617/3.H5T0W4

[13] Nurullah Demir, Tobias Urban, Norbert Pohlmann, and Christian Wressnegger. 2024. A Large-Scale Study of Cookie Banner Interaction Tools and Their Impact on Users' Privacy. *Proceedings on Privacy Enhancing Technologies (PETS)* 2024, 1 (2024), 5–20.

[14] Yana Dimova, Gunes Acar, Lukasz Olejnik, Wouter Joosen, and Tom Van Goethem. 2021. The CNAME of the Game: Large-scale Analysis of DNS-based Tracking Evasion. *Proceedings on Privacy Enhancing Technologies (PETS)* 2021, 3 (2021), 394–412.

[15] Disconnect. 2019. Tracking Enties. https://raw.githubusercontent.com/disconnectme/disconnect-tracking-protection/refs/heads/master/entities.json Accessed: 2024-12-30.

[16] Flashtalking. 2025. Independent Global Ad Server and Analytics Platform. https://www.flashtalking.com/ Accessed: 2025-08-28.

[17] Asmaa El fraihi, Nardjes Amieur, Walter Rudametkin, and Oana Goga. 2024. Client-side and Server-side Tracking on Meta: Effectiveness and Accuracy. *Proceedings on Privacy Enhancing Technologies (PETS)* 2024, 3 (2024), 431–445.

[18] Gertjan Franken, Tom Van Goethem, and Wouter Joosen. 2018. Who Left Open the Cookie Jar? A Comprehensive Evaluation of {Third-Party} Cookie Policies. In *Proceedings of the 27th USENIX Security Symposium (USENIX Security)*. USENIX Association, 151–168.

[19] Google. 2020. Google Click Identifier (GCLID): Definition. https://support.google.com/google-ads/answer/9744275?hl=en Accessed: 2025-08-27.

[20] Google. 2020. Google to phase out third-party cookies in Chrome. https://privacysandbox.google.com/cookies Accessed: 2025-08-27.

[21] Google Ads Help. 2024. How Google Ads Consent Mode Works. https://support.google.com/google-ads/answer/13802165?hl=en Accessed: 2025-11-05.

[22] Google Developers. 2024. YouTube Data API v3. https://developers.google.com/youtube/v3/docs/ Accessed: 2025-08-11.

[23] Google Developers. 2025. Google Tag Manager: Consent APIs. https://developers.google.com/tag-platform/tag-manager/templates/consent-apis Accessed: 2025-11-05.

[24] Google Ads Help. 2025. How Google Ads tracks website conversions. https://support.google.com/google-ads/answer/7521212?sjid=567358432708360360-EU Accessed: 2025-08-28.

[25] MWE Privacy Insights. 2024. EU Regulators Confirm that Cookie Consent Rules Apply to Much Broader Range of Tracking Technologies. https://www.mwe.com/insights/eu-regulators-confirm-that-cookie-consent-rules-apply-to-much-broader-range-of-tracking-technologies/ Accessed: 2025-08-29.

[26] Intelpoint Insights. 2024. YouTube's Revenue from Adverts Surged by More Than 400% from 2017 to 2024. https://intelpoint.co/insights/youtubes-revenue-from-adverts-surged-by-more-than-400-from-2017-to-2024/ Accessed: 2025-05-23.

[27] Umar Iqbal, Steven Englehardt, and Zubair Shafiq. 2021. Fingerprinting the fingerprinters: Learning to detect browser fingerprinting behaviors. In *Proceedings of the IEEE Symposium on Security and Privacy (SP)*. IEEE, 1143–1161.

[28] Navpreet Kaur, Sami Azam, Krishnan Kannoorpatti, Kheng Cher Yeo, and Bharanidharan Shanmugam. 2017. Browser fingerprinting as user tracking technology. In *Proceedings of the 11th International Conference on Intelligent Systems and Control (ISCO)*. IEEE, 103–111.

[29] Martin Koop, Erik Tews, and Stefan Katzenbeisser. 2020. In-depth evaluation of redirect tracking and link usage. *Proceedings on Privacy Enhancing Technologies* 2020, 4 (2020), 394–413.

[30] Cat Mai, Bruno Coelho, Julia Kieserman, Lexie Matsumoto, Kyle Spinelli, Eric Yang, Athanasios Andreou, Rachel Greenstadt, Tobias Lauinger, and Damon McCoy. 2025. More and Scammier Ads: The Perils of YouTube's Ad Privacy Settings. *Proceedings on Privacy Enhancing Technologies (PETS)* 2025, 4 (2025), 1014–1038.

[31] The Tor Project: Tor Browser User Manual. 2025. Anti-fingerprinting. https://tb-manual.torproject.org/anti-fingerprinting/ Accessed: 2025-08-29.

[32] MDN Web Docs. 2025. Redirections in HTTP. https://developer.mozilla.org/en-US/docs/Web/HTTP/Redirections Accessed: 2025-05-23.

[33] Microsoft Corporation. 2023. Microsoft Edge Privacy Whitepaper. https://learn.microsoft.com/en-us/microsoft-edge/privacy-whitepaper Accessed: 2025-08-28.

[34] Chris Mills. 2023. Saying goodbye to third-party cookies in Firefox in 2024. https://developer.mozilla.org/en-US/blog/goodbye-third-party-cookies/ Accessed: 2025-05-24.

[35] Mozilla Foundation. 2024. Enhanced Tracking Protection in Firefox. https://support.mozilla.org/en-US/kb/enhanced-tracking-protection-firefox-desktop Accessed: 2025-08-28.

[36] Shaoor Munir, Patrick Lee, Umar Iqbal, Zubair Shafiq, and Sandra Siby. 2024. {PURL}: Safe and Effective Sanitization of Link Decoration. In *Proceedings of the 33rd USENIX Conference on Security Symposium (USENIX Security)*. USENIX Association, 4103–4120.

[37] Shaoor Munir, Patrick Lee, Umar Iqbal, Zubair Shafiq, and Sandra Siby. 2024. PURL: Safe and Effective Sanitization of Link Decoration. https://github.com/shaoormunir/purl Accessed: 2025-11-05.

[38] Nick Nikiforakis, Alexandros Kapravelos, Wouter Joosen, Christopher Kruegel, Frank Piessens, and Giovanni Vigna. 2013. Cookieless monster: Exploring the ecosystem of web-based device fingerprinting. In *Proceedings of the IEEE Symposium on Security and Privacy(SP)*. IEEE, 541–555.

[39] Nimbata. 2022. All You Need to Know About GCLID Tracking for Google Ads. https://www.nimbata.com/tips/gclid-tracking-for-google-ads Accessed: 2025-08-28.

[40] Adam Oest, Penghui Zhang, Brad Wardman, Eric Nunes, Jakub Burgis, Ali Zand, Kurt Thomas, Adam Doupé, and Gail-Joon Ahn. 2020. Sunrise to sunset: Analyzing the end-to-end life cycle and effectiveness of phishing attacks at scale. In *Proceedings of the 29th USENIX Security Symposium (USENIX Security)*. USENIX Association, 361–377.

[41] Emmanouil Papadogiannakis, Panagiotis Papadopoulos, Nicolas Kourtellis, and Evangelos P Markatos. 2021. User tracking in the post-cookie era: How websites bypass gdpr consent to track users. In *Proceedings of the ACM Web Conference 2021*. ACM, 2130–2141.

[42] Panagiotis Papadopoulos, Nicolas Kourtellis, and Evangelos Markatos. 2019. Cookie synchronization: Everything you always wanted to know but were afraid to ask. In *Proceedings of the ACM Web Conference (WWW)*. ACM, 1432–1442.

[43] Tien-Huy Pham, Quoc-Huy Vo, Ha Dao, and Kensuke Fukuda. 2025. I never willingly consented to this! Investigate PII leakage via SSO logins. *IEEE Transactions on Privacy* 2 (2025), 67–78.

[44] Audrey Randall, Peter Snyder, Alisha Ukani, Alex C Snoeren, Geoffrey M Voelker, Stefan Savage, and Aaron Schulman. 2022. Measuring UID smuggling in the wild. In *Proceedings of the 22nd ACM Internet Measurement Conference (IMC)*. ACM, 230–243.

[45] Ali Rasaii, Ha Dao, Anja Feldmann, Mohammadmahdi Javid, Oliver Gasser, and Devashish Gosain. 2025. Intractable Cookie Crumbs: Unveiling the Nexus of Stateful Banner Interaction and Tracking Cookies. *Proceedings on Privacy Enhancing Technologies (PETS)* 2025, 4 (2025), 429–445.
[46] Ali Rasaii, Shivani Singh, Devashish Gosain, and Oliver Gasser. 2023. Exploring the cookieverse: A multi-perspective analysis of web cookies. In *Proceedings of the Passive and Active Network Measurement Conference (PAM)*. Springer Nature, 623–651.
[47] Google Business Resources. 2023. A Beginner's Guide to YouTube Video Ads: Drive Action with Video Advertising. https://business.google.com/us/resources/articles/beginners-guide-youtube-ads/ Accessed: 2025-08-29.
[48] Craig A Shue, Andrew J Kalafut, and Minaxi Gupta. 2008. Exploitable Redirects on the Web: Identification, Prevalence, and Defense.. In *2nd USENIX Workshop on Offensive Technologies (WOOT)*. USENIX Association.
[49] Peter Snyder, Soroush Karami, Arthur Edelstein, Benjamin Livshits, and Hamed Haddadi. 2023. {Pool-Party}: Exploiting browser resource pools for web tracking. In *Proceedings of the 32nd USENIX Security Symposium (USENIX Security 23)*. USENIX Association, 7091–7105.
[50] Peter Snyder and Brave Software. 2021. Understanding redirection-based tracking. https://brave.com/blog/redirection-based-tracking/ Accessed: 2025-05-23.
[51] Brave Software. 2024. Brave Browser. https://brave.com Accessed: 2025-05-23.
[52] Klaus Solberg Söilen. 2024. Using Google Ads in digital marketing. , 417–426 pages.
[53] Oleksii Starov, Phillipa Gill, and Nick Nikiforakis. 2016. Are you sure you want to contact us? Quantifying the leakage of pii via website contact forms. *Proceedings on Privacy Enhancing Technologies (PETS)* 2016, 1 (2016), 20–33.
[54] Statista. 2024. Leading YouTube markets worldwide based on monthly users. https://www.statista.com/statistics/280685/number-of-monthly-unique-youtube-users-worldwide/ Accessed: 2025-08-28.
[55] Statista. 2025. Advertising - Worldwide. https://www.statista.com/outlook/amo/advertising/worldwide Accessed: 2025-08-30.
[56] ADITION technologies AG. 2020. Programmatic Advertising Solutions. https://virtualminds.com/adition/ Accessed: 2025-08-28.
[57] The Brave Privacy Team. 2020. Grab bag: query stripping, referrer policy, and reporting API. https://brave.com/privacy-updates/5-grab-bag/ Accessed: 2025-05-23.
[58] TrafficGuard. 2023. GCLID 101: What is GCLID and Its Importance in Google Ads. https://www.trafficguard.ai/blog/gclid-101-what-is-gclid-and-why-is-it-important-to-implement-this-in-your-google-ads-account Accessed: 2025-08-28.
[59] D Yu Weider, Shruti Nargundkar, and Nagapriya Tiruthani. 2008. A phishing vulnerability analysis of web based systems. In *Proceedings of the IEEE Symposium on Computers and Communications*. IEEE, 326–331.
[60] John Wilander. 2020. Full Third-Party Cookie Blocking and More in Safari's ITP. https://webkit.org/blog/10218/full-third-party-cookie-blocking-and-more/ Accessed: 2025-05-24.
[61] YouTube Help. 2024. View counts on YouTube. https://support.google.com/youtube/answer/2375464?hl=en Accessed: 2025-05-23.

A BannerClick Performance

To further assess the performance of *BannerClick* for banner interaction, we manually verified the first run of the *Baseline* experiment to calculate *BannerClick*'s acceptance accuracy, and the first run of the *Rejection* experiment to calculate its rejection accuracy. *BannerClick* successfully accepted banners for 26 out of 27 advertisers (that had banners), resulting in an accuracy of 96.3%. Similarly, it successfully rejected banners for 25 out of 26 advertisers (that had banners), achieving an accuracy of 96.2%. These results further demonstrate the robustness and reliability of *Bannerclick*'s performance.

B User Identifier Detection

To identify potential user identifiers being smuggled, we adopt a methodology inspired by Randall et al. [44] and Chouaki et al. [10]. This approach considers all query parameters, local storage values, and cookie values as *tokens*. Filtering heuristics are then applied to distinguish tokens that may represent user identifiers from benign values such as session identifiers, dates, timestamps, URLs, or plain-text words. Building on this methodology, we slightly modify the heuristics to focus on detecting identifiers that are used explicitly for tracking in the context of YouTube ad clicks.

(1) Tokens must be unique to an ad interaction. Identifiers that are constant across all ad interactions are discarded, since they cannot serve as unique tracking identifiers.
(2) Following programmatic heuristics from prior work [10, 44], we discard tokens that correspond to timestamps, URLs, plain-text words, or that have a length shorter than eight characters.
(3) We remove campaign-related parameters (e.g., `utm_campaign`, `utm_source`, `utm_medium`) that are commonly used for marketing analytics but do not act as user identifiers.

As a result, we identify one token, `gclid`, that consistently passes our filtering heuristics. Among all observed parameters, `gclid` is the only value that exhibits the characteristics of a user identifier in the context of YouTube ad clicks, and is systematically propagated for tracking purposes.

Metric	Rejection
Total Video Visits	430 × 5
Ad Interactions w/ Successful Advertiser Landing Page Visit	947
Unique Advertisers	74
Unique URL Paths w/ `gclid`	1,019
Ad Interactions w/ ≥1 URL Path w/ `gclid`	947
Unique Advertiser That Stored `gclid` As A Cookie	41

Table 4: Summary statistics of video visits, ad interactions, and propagation of `gclid` collected in the *rejection* configuration: Chrome browser with the cookie banner rejected in Germany.

C Summary Statistics of Video Visits, Ad Interactions, and Propagation of `gclid` Collected in Other Configurations

In the *rejection* configuration (Chrome, Germany), all ad interactions propagated the `gclid` via URL paths. However, a substantial fraction of advertisers (41/74) also stored the `gclid` in cookies, indicating that navigational propagation remained the dominant mechanism while persistent storage was still common (see Table 4). In the *multi-browser* configuration (Edge and Firefox, Germany), both browsers exhibited a precise one-to-one correspondence between ad interactions and `gclid` propagation through URL paths. Many advertisers additionally stored the `gclid` in cookies (see Table 5). Across all vantage points, ad interactions consistently propagated the `gclid` via URL paths, and cookie-based storage of the `gclid` remained relatively frequent across all regions (see Table 6).

D Distribution of Domain Paths containing `gclid` in Other Configurations

In the *rejection* setup (Chrome, Germany), `gclid` flows were highly concentrated: over 98% of observed paths involved *googleadservices.com* or *doubleclick.net*. This concentration underlines Google's central role in cross-site tracking infrastructure (see Table 7). In

Metric	Edge	Firefox
Total Video Visits	430×5	430×5
Ad Interactions w/ Successful Advertiser Landing Page Visit	1,025	1,101
Unique Advertisers	157	180
Unique URL Paths w/ `gclid`	873	1,138
Ad Interactions w/ $\geq$1 URL Path w/ `gclid`	1,025	1,101
Unique Advertisers That Stored `gclid` As A Cookie	120	143

Table 5: Summary statistics of video visits, ad interactions, and propagation of `gclid` collected in the *multi-browser* configuration: Edge and Firefox browsers with the cookie banner accepted in Germany.

Edge and Firefox, `gclid` was mainly propagated via Google domains (*googleadservices.com*, *doubleclick.net*). Edge showed some extra diversity (e.g., Flashtalking, ADITION), while Firefox was more concentrated on Google, meaning both browsers still funneled most tracking through Google with slight differences (see Table 8). In all vantage points, `gclid` paths were dominated by Google domains (*googleadservices.com*) (see Table 9).

Metric	Germany	Australia	India	Brazil	USA - California	USA - New York
Total Video Visits	430 × 5	430 × 5	430 × 5	430 × 5	430 × 5	430 × 5
Ad Interactions w/ Successful Advertiser Landing Page Visit	238	1,010	235	314	552	1,168
Unique Advertisers	120	479	117	168	295	286
Unique URL Paths w/ `gclid`	257	867	249	330	589	583
Ad Interactions w/ ≥1 URL Path w/ `gclid`	238	1,010	235	314	552	1,168
Unique Advertisers That Stored `gclid` As A Cookie	87	413	96	135	256	253

Table 6: Summary statistics of video visits, ad interactions, and propagation of `gclid` collected in the *multi-vantage points* configuration: Chrome browser with the cookie banner accepted across six vantage points: Germany, Australia, India, Brazil, USA - California, and USA - New York.

Path	Number	Percentage
www.googleadservices.com → Advertiser	49	58.33%
www.googleadservices.com → **ad.doubleclick.net** → Advertiser	20	23.81%
ad.doubleclick.net → Advertiser	12	14.29%
www.googleadservices.com → tracker.clixtell.com → Advertiser	1	1.19%
www.googleadservices.com → m.exactag.com → Advertiser	1	1.19%
pixel.everesttech.net → Advertiser	1	1.19%

Table 7: Distribution of domain paths containing `gclid` in the *rejection* configuration: Chrome browser with the cookie banner rejected in Germany. Percentages are based on the 84 unique domain paths. Each domain is shown in a consistent color.

Browser	Path	Number	Percentage
Edge	**www.googleadservices.com** → Advertiser	107	64.46%
	www.googleadservices.com → **ad.doubleclick.net** → Advertiser	39	23.49%
	ad.doubleclick.net → Advertiser	11	6.63%
	www.googleadservices.com → **ad.doubleclick.net** → servedby.flashtalking.com → Advertiser	2	1.20%
	www.googleadservices.com → ad13.adfarm1.adition.com → Advertiser	2	1.20%
	www.googleadservices.com → youtu.be → Advertiser	1	0.60%
	www.googleadservices.com → **ad.doubleclick.net** → youtu.be → Advertiser	1	0.60%
	ad13.adfarm1.adition.com → Advertiser	1	0.60%
	www.googleadservices.com → swccgl.abr.ge → Advertiser	1	0.60%
	swccgl.abr.ge → Advertiser	1	0.60%
Firefox	**www.googleadservices.com** → Advertiser	142	75.94%
	www.googleadservices.com → **ad.doubleclick.net** → Advertiser	26	13.90%
	ad.doubleclick.net → Advertiser	10	5.35%
	www.youtube.com → **www.googleadservices.com** → Advertiser	4	2.14%
	swccgl.abr.ge → Advertiser	1	0.53%
	www.googleadservices.com → swccgl.abr.ge → Advertiser	1	0.53%
	www.youtube.com → Advertiser	1	0.53%
	1l-go.my.games → Advertiser	1	0.53%
	www.googleadservices.com → ad13.adfarm1.adition.com → Advertiser	1	0.53%

Table 8: Distribution of domain paths containing `gclid` in the *multi-browser* configuration: Edge and Firefox browsers with the cookie banner accepted in Germany. Percentages are based on the number of unique domain paths per browser: Edge (166) and Firefox (187). Each domain is shown in a consistent color.

Country	Path	Number	Percentage
Germany	www.googleadservices.com → Advertiser	63	48.46%
	www.googleadservices.com → ad.doubleclick.net → Advertiser	47	36.15%
	ad.doubleclick.net → Advertiser	17	13.08%
	www.googleadservices.com → ad2.adfarm1.adition.com → Advertiser	1	0.77%
	ad13.adfarm1.adition.com → Advertiser	1	0.77%
	ad2.adfarm1.adition.com → Advertiser	1	0.77%
Australia	www.googleadservices.com → Advertiser	449	97.40%
	www.googleadservices.com → clickserve.dartsearch.net → Advertiser	4	0.87%
	monitor.clickcease.com → Advertiser	2	0.43%
	www.googleadservices.com → gsght.com → Advertiser	1	0.22%
	clickserve.dartsearch.net → Advertiser	1	0.22%
	www.googleadservices.com → monitor.clickcease.com → Advertiser	1	0.22%
	gsght.com → Advertiser	1	0.22%
	www.googleadservices.com → jkkf7.app.link → Advertiser	1	0.22%
	myid.telstra.com → Advertiser	1	0.22%
India	www.googleadservices.com → Advertiser	89	68.99%
	www.googleadservices.com → ad.doubleclick.net → Advertiser	25	19.38%
	ad.doubleclick.net → Advertiser	13	10.08%
	www.googleadservices.com → io.clickguard.com → Advertiser	1	0.78%
	www.googleadservices.com → ad.doubleclick.net → track.mfilter.net → Advertiser	1	0.78%
Brazil	www.googleadservices.com → Advertiser	124	71.68%
	www.googleadservices.com → ad.doubleclick.net → Advertiser	35	20.23%
	ad.doubleclick.net → Advertiser	7	4.05%
	www.googleadservices.com → clickserve.dartsearch.net → ad.doubleclick.net → Advertiser	2	1.16%
	www.googleadservices.com → sympla.queue-it.net → Advertiser	1	0.58%
	monitor.clickcease.com → Advertiser	1	0.58%
	clickserve.dartsearch.net → ad.doubleclick.net → Advertiser	1	0.58%
	servedby.flashtalking.com → Advertiser	1	0.58%
	www.googleadservices.com → ad.doubleclick.net → servedby.flashtalking.com → Advertiser	1	0.58%
USA - California	www.googleadservices.com → Advertiser	184	60.13%
	www.googleadservices.com → ad.doubleclick.net → Advertiser	79	25.82%
	ad.doubleclick.net → Advertiser	23	7.52%
	www.googleadservices.com → monitor.lunio.ai → Advertiser	2	0.65%
	ad.doubleclick.net → d.agkn.com → Advertiser	2	0.65%
	d.agkn.com → Advertiser	2	0.65%
	www.googleadservices.com → ad.doubleclick.net → servedby.flashtalking.com → Advertiser	1	0.33%
	www.googleadservices.com → 3689.xg4ken.com → Advertiser	1	0.33%
	clickserve.dartsearch.net → ad.doubleclick.net → Advertiser	1	0.33%
	5350.xg4ken.com → Advertiser	1	0.33%
	6147.xg4ken.com → Advertiser	1	0.33%
	www.googleadservices.com → clickserve.dartsearch.net → ad.doubleclick.net → Advertiser	1	0.33%
	2801.xg4ken.com → Advertiser	1	0.33%
	pixel.everesttech.net → Advertiser	1	0.33%
	3689.xg4ken.com → Advertiser	1	0.33%
	www.googleadservices.com → ad.doubleclick.net → monitor.lunio.ai → Advertiser	1	0.33%
	www.googleadservices.com → 6147.xg4ken.com → Advertiser	1	0.33%
	www.googleadservices.com → pixel.everesttech.net → Advertiser	1	0.33%
	www.googleadservices.com → 2801.xg4ken.com → Advertiser	1	0.33%
	www.googleadservices.com → 5350.xg4ken.com → Advertiser	1	0.33%
USA - New York	www.googleadservices.com → Advertiser	199	65.68%
	www.googleadservices.com → ad.doubleclick.net → Advertiser	58	19.14%
	ad.doubleclick.net → Advertiser	20	6.60%
	monitor.clickcease.com → Advertiser	5	1.65%
	www.googleadservices.com → ad.doubleclick.net → monitor.lunio.ai → Advertiser	2	0.66%
	www.googleadservices.com → pixel.everesttech.net → Advertiser	2	0.66%
	www.googleadservices.com → monitor.lunio.ai → Advertiser	2	0.66%
	www.googleadservices.com → 2801.xg4ken.com → Advertiser	1	0.33%
	pixel.everesttech.net → Advertiser	1	0.33%
	www.googleadservices.com → 5350.xg4ken.com → Advertiser	1	0.33%
	www.googleadservices.com → ad.doubleclick.net → servedby.flashtalking.com → Advertiser	1	0.33%
	www.googleadservices.com → clickserve.dartsearch.net → ad.doubleclick.net → Advertiser	1	0.33%
	clickserve.dartsearch.net → ad.doubleclick.net → Advertiser	1	0.33%
	www.googleadservices.com → pulse.clickguard.com → Advertiser	1	0.33%
	servedby.flashtalking.com → Advertiser	1	0.33%
	2801.xg4ken.com → Advertiser	1	0.33%
	www.googleadservices.com → tracker.clixtell.com → Advertiser	1	0.33%
	5350.xg4ken.com → Advertiser	1	0.33%
	www.googleadservices.com → monitor.clickcease.com → Advertiser	1	0.33%
	pulse.clickguard.com → Advertiser	1	0.33%
	ad.doubleclick.net → monitor.lunio.ai → Advertiser	1	0.33%
	ad.doubleclick.net → servedby.flashtalking.com → Advertiser	1	0.33%

Table 9: Distribution of domain paths containing `gclid` across six geographic locations. Percentages are based on the number of unique domain paths per country: Germany (130), Australia (461), India (129), Brazil (173), USA–California (306), and USA–New York (303). Each domain is shown in a consistent color.