Privacy in Digital Age: Term Project

Measuring the Impact of Global Privacy Control on Website Tracking Behavior

Submitted by: Group 3

Ajay Suresh, Brendan Reed, Mburu Kagiri and Mohini Madhur

February 8, 2026

Table of Contents

Abstract

Online behavioral tracking remains a central mechanism underpinning digital advertising ecosystems, despite increasing regulatory scrutiny and user resistance. Global Privacy Control (GPC), introduced in 2020, is a legally enforceable browser-level signal designed to communicate user preferences regarding the sale and sharing of personal data, with legal recognition under certain U.S privacy laws, such as the California Consumer Privacy Act (CCPA).

This study examines whether enabling GPC results in measurable changes to third-party tracking activity compared to (1) default browsing and (2), manual cookie opt-out mechanisms. Using a limited controlled experimental framework, we analyze network traffic, cookie storage, and third-party requests across a diverse set of commercial websites under three conditions: default browsing, manual cookie rejection, and GPC-enabled browsing. Data is collected via HTTP Archive (HAR) files using Edge and BraveBrowsers configured for default, manual reject, and GPC-enabled conditions. Each of these environments are set to fully purge all history and cache data upon exit, so each browsing session is done from a clean starting point.

Evaluation metrics include the volume of third-party requests, unique third-party domains, known tracker requests, and cookie storage.The findings aim to assess GPC's technical effectiveness as a privacy-preserving mechanism and inform ongoing policy and compliance discussions surrounding browser-based consent signals. Limitations, including geographic variability, time-of-day effects, and the inability to fully capture fingerprinting, are discussed.

Introduction

The modern web is sustained by extensive mechanisms of user tracking that enable targeted advertising, personalization through behavioral analytics, and content delivery. These mechanisms form a complex ecosystem of technologies, including HTTP cookies, third-party scripts, tracking pixels, and browser fingerprinting. While these practices generate substantial economic value, they raise persistent concerns regarding user autonomy, consent, and privacy.

Early attempts to mitigate these concerns include the introduction of the "Do Not Track" (DNT) header in 2009, which sought to provide users with a standardized method of signaling their preference to opt out of tracking (Mayer & Mitchell, 2012). However, DNT lacked legal enforceability and was widely ignored by advertisers and data brokers. In response, more recent efforts have focused on integrating privacy preferences into regulatory frameworks, culminating in the development of Global Privacy Control (GPC).

GPC represents a shift from voluntary compliance toward legally recognized consent signals, particularly within U.S. state-level privacy regimes. Yet despite its growing regulatory recognition, the practical effectiveness of GPC remains underexplored. This paper investigates whether GPC meaningfully reduces observable tracking compared to traditional manual opt-out mechanisms.

Background

The expansion of behavioral advertising in the early 2000s led to widespread cross-site tracking across websites via HTTP cookies, embedded scripts, tracking pixels, and browser fingerprinting (Englehardt & Narayanan, 2016). As concerns over cross-site profiling and data aggregation grew, the "Do Not Track" (DNT) header was introduced in 2009 as a browser-based mechanism allowing users to signal their preference not to be tracked. Inspired by the National Do Not Call registry in the U.S.A., and advocated by privacy and cybersecurity professionals at the time, the feature was established as a standardized method of signaling user preferences to opt out of tracking for marketing purposes (Kamara and Kosta, 2016). However, unlike the comprehensive federal database that needed ongoing revision, the DNT was amended to be a header, allowing this centralized design to subvert the "substantial technical and privacy challenges inherent to compiling, updating, and sharing a comprehensive registry of tracking services or web users."

The header, lacking concrete federal frameworks and enforcement, immediately faced challenges. Definitional disagreements of terms like 'tracking,' 'storage,' and 'fair processing', along with disagreements on features such as default settings, intentions behind tracking, or compliance mechanisms, all led to a dizzying presentation of DNTs by various providers. As a consequence, most DNT headers only opted users out of the tracking technology, rather than advertising itself. Ad networks had the capacity to "fingerprint" browsers as a technique to defeat ad blockers by identifying unique characteristics in a user's browser configuration. All these combined to render the DNT header largely ineffectual.

The GPC arose in 2020 to replace DNT headers with a legally-enforceable set of web technologies that could communicate to websites user preferences regarding the sale and sharing of personal data.[1] The enforcement mechanisms are set in jurisdictions governed by laws such as the California Consumer Privacy Act (CCPA). Rather than the manual opt-in opt-out system that users were subjected to under DNT, GPC allowed for users to universalize these preferences for all websites visited, streamlining user preference communication. Functioning as a browser extension, GPC currently gains regulatory recognition in California, Colorado, Virginia, and a select number of states, where businesses must respect GPC signals to avoid compliance violations. However in states such as Pennsylvania, users must download the GPC extension as a means of actively communicating their preferences. Websites are therefore not legally compelled under state law to honor GPC signals. However, for operational simplicity, risk minimization, and consent platform design, we imagine that, for particularly large commercial companies, compliance is likely to be adopted.

This optional mechanism allows for testable conditions on the effectiveness of this set of web technologies, as traffic packets, advertising cookies, and other tracking measures can be modulated and analyzed pre and post GPC extension implementation.

Literature Review

Online tracking infrastructures are pervasive and sophisticated. Cranor et al. (2013) evaluate these tracking technologies within internet monitoring, web tracking, location tracking, and audio and visual surveillance. These include an extensive "combination of HTTP cookies and an ecosystem" that allows "advertising companies [to] serve advertisements on many popular websites [that enable] this sort of tracking." Similarly, Englehardt and Narayan (2016) demonstrate that third-party tracking occurs on the majority of popular websites and often persists even after users attempt to limit data collection. They note the combination of cookies, browser fingerprinting, and cross-site identifiers that networks use to construct detailed user profiles. Equally important, they illustrate the challenge of designing recognition mechanisms capable of identifying and mitigating the diverse set of tracking web activity.

At the same time, some web browsers such as DuckDuckGo already implement GPC natively, while others, like Microsoft Edge, do not, allowing for greater flexibility and control in an experimental setting (Zimmeck et al.). Since sites can still detect and interpret GPC signals in a variety of ways – for example by limiting "all third party user tracking regardless of location" or by limiting "data sharing in only some jurisdictions" – multiple large-scale websites across

[1] Global Privacy Control: How to Implement Global Privacy Control (GPC) for Publishers

various market spaces (media, retail, government, etc) can be visited to test for compliance complexity.

One continuous challenge is the usage of beacons or web-bugs as invisible elements for web-tracking; this study has yet to discover whether GPC is able to screen this information (Cranor et. al., 2013). This is important because many companies include beacons on popular websites as a form of online behavioral advertising, which could effectively circumvent GPC. Similarly, this study is yet to identify whether GPC protects against the potential use of Local Shared Objects (LSOs) by advertisers, another mechanism that "can store approximately twenty five times as much information as a standard HTTP cookie."[2]

While these limitations highlight the uncertainty surrounding whether GPC can fully prevent advanced tracking mechanisms, more recent research has started to examine how GPC has been rolled out as a response to evolving tracking technologies.

Methodology

Website Selection Across Categories & Legal Regimes

To evaluate the impact of Global Privacy Control (GPC) on tracking behavior, we selected a representative sample of websites across multiple domains, including news media, e-commerce, social networking platforms, entertainment services, and health-related sites. The sample was chosen to ensure diversity in website type, popularity, and tracking complexity. While our selection includes sites with audiences in multiple jurisdictions, we note that geographic IP variation could influence tracking behavior; controlling for this factor was not feasible in the scope of this study and is acknowledged as a limitation. Sites subject to privacy regulations, such as the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR), were included to examine how GPC interacts with legally recognized consent frameworks.

[2] Ibid
Global Privacy Control (GPC) Specification. World Wide Web Consortium (W3C).
Sourcepoint. Global Privacy Control: How to Implement Global Privacy Control (GPC) for Publishers.
Zimmeck, S., Wang, O., Alicki, K., Wang, J., & Eng, S. Usability and Enforceability of Global Privacy Control. Proceedings on Privacy Enhancing Technologies, 2023.

Browser Test Environments & GPC Modes

Experiments were conducted using two browsers:[3] *Microsoft Edge* and *Brave Browser*. Edge was configured with default settings and no privacy settings enabled, while Brave was used because of its native GPC-enabled functionality. Three primary browsing conditions were tested:

1. Default Browsing (no GPC): Using default-settings in a non-GPC-native browser environment and accepting cookies if prompted by the website.
2. Manual Cookie Reject (if prompted): Reject cookies using the website's consent interface.
3. GPC-Enabled Browsing: Enabling GPC request headers natively via Brave browser to communicate privacy preferences automatically.

Each site was visited under all conditions, and trials were conducted to account for variability in network traffic, dynamic advertising campaigns, and potential temporal effects.

Trial Execution and Control Measures

To ensure consistency and control for confounding variables, all trials were executed with the following standardizations:

- Fresh browser profiles were used for each trial, with cache, cookies, and local storage cleared prior to browsing.
- The same browser version and user-agent string were maintained across all trials.
- Navigation paths were standardized for each website to ensure identical interactions.
- Page dwell time was set at _x_ seconds per page to allow all scripts and trackers to load.

The order of experimental conditions was randomized for each site to mitigate any bias arising from order effects or time-of-day variations. Each condition was repeated __x__ times per site per browser, providing sufficient data for statistical analysis of differences across conditions.

Data Collection

Network and cookie-level data were captured in a completely default and brand new Windows 10 virtual environment with no settings changed or configured during setup. A local "offline" account was used. Microsoft Edge comes installed as default, and is used to download and install Brave Browser[4]. Following this, both browsers were set to 'Delete browsing data: On Exit'[5] as to keep sessions consistent between site visits.

[3] Mazel, J., Garnier, R., & Fukuda, K. (2019). A comparison of Web Privacy Protection Techniques. *Computer Communications*, *144*, 162–174. https://doi.org/10.1016/j.comcom.2019.04.005

[4] *Privacy updates*. Brave. (2026, January 5). https://brave.com/privacy-updates/

[5] Brink, S. (n.d.). *Turn on or off clear browsing data on close in microsoft edge chromium | tutorials*. How to Turn On or Off Clear Browsing Data on Close in Microsoft Edge Chromium. https://www.tenforums.com/tutorials/153307-turn-off-clear-browsing-data-close-microsoft-edge-chromium.html

Using DevTools in Brave and Edge ‘Preserve Log’ and ‘Disable Cache’ were enabled as to capture purely the network traffic and HTTP requests as they were occurring in realtime. Researchers manually exported the session’s HTTP Archive (HAR) files for each website and browsing session. HAR files contain detailed information on HTTP requests and responses, including request URLs, response codes, cookies set, and third-party requests. They provide a standardized format for analyzing traffic and client/server interactions.[6] Finally, these HAR files were exported from the virtual test environment and brought to a production server for analysis. Analysis of traffic and cookies was completed using the Google Admin Toolbox HAR Analyzer.[7] This is an industry standard tool used for analyzing the network performance of websites and apps by either consumers or website administrators.

Tracking Definition

For the purposes of this study, tracking is defined as any mechanism designed to collect behavioral, advertising, or analytic data across websites. This includes HTTP requests to third-party domains, tracking pixels, cookies, and similar mechanisms. While HAR files capture requests and cookies effectively, advanced tracking techniques, such as browser fingerprinting and Local Shared Objects (LSOs), are not fully observable through HAR alone and are noted as a limitation.

Metrics

The study evaluates both network-level and cookie-level metrics, including:

Metric	Definition
Total Requests (TR)	Total HTTP requests per page load
Third-Party Requests (TPR)	Requests where the request domain differs from the top-level domain
Unique Third-Party Domains (UTPD)	Number of distinct third-party domains contacted
Known Tracker Requests (KTR)	Requests matching known tracker lists (EasyPrivacy, Disconnect, known ad-tech domains)

[6] Piccini, J. (n.d.). *My journey to performance analysis 2/2 (har files) | by Julien Piccini | TDS archive | medium*. My journey to Performance Analysis 2/2 (HAR files). https://medium.com/data-science/my-journey-to-performance-analysis-2-2-har-files-8a94a52bfac9

[7] *Google admin toolbox har analyzer*. HAR Analyzer. (n.d.). https://toolbox.googleapps.com/apps/har_analyzer/

Total Cookies (TC)	Number of cookies stored during a session
Third Party Cookies (TPC)	Cookies with domains differing from the top-level site
Persistent Cookies (PC)	Cookies with expiration times exceeding the session length

These metrics provide a quantitative basis for comparing tracking behavior across browsing conditions and assessing the effectiveness of GPC in reducing data collection.[8].

Statistical Analysis

In an environment with multiple DoNotTrack requests (GPC, DNT, EU-consent), which takes precedence?[9][10]

Findings

This section summarizes the observed differences in network activity between *Brave* (GPC-enabled) and *Microsoft Edge* (no GPC) across six commercial websites: CNN, Best Buy, Target, The Guardian, WebMD, and Zillow.

As Table 1.1 indicates, across all, Brave transmitted the Sec-GPC: 1 header in 1,532 requests, while Edge transmitted none. In addition, there were substantial decreases in traffic reduction as measured by cookie activity. On average, third-party requests decreased by 84%, known tracker/ad requests decreased by 98.2%, and referer leakage events decreased by 83.6%. The most pronounced effect appears in the Tracker/Ad Requests category, suggesting that GPC-enabled browsing dramatically reduces observable advertising-related network activity. In addition, no "Do Not Track (DNT) headers" were observed in either browser.

Table 1.1 : Aggregate Results Across all Sites

Metric	Brave (GPC)	Edge (No GPC)	Reduction
Total HTTP Requests	1,737	7,745	↓ 77.6%

[8] Sim, K., Heo, H., & Cho, H. (2024, October 5). *Combating Web Tracking: Analyzing Web Tracking Technologies for user privacy*. MDPI. https://www.mdpi.com/1999-5903/16/10/363

[9] *Global Privacy Control (GPC)*. W3C. (n.d.). https://www.w3.org/TR/gpc/

[10] Hils, M., Woods, D. W., & Böhme, R. (2023). Conflicting Privacy Preference Signals in the wild. *Data Protection and Privacy, Volume 15*. https://doi.org/10.5040/9781509965939.ch-004

Third-Party Requests	1,083	6,749	↓ 84.0%
Tracker/Ad Requests	48	2,653	↓ 98.2%
Referer Leakage Events	1,079	6,593	↓ 83.6%

Site-Level Findings

The results suggest a mixed outcome of strong suppression of ad-tech infrastructure under GPC conditions, and a selective suppression of ad-tech domains rather than a blanket reduction in page functionality. For instance for CNN, twenty-one advertising and data broker domains appeared only in Edge, including 3lift, Criteo, OpenX, and Taboola. In contrast, for Best Buy, while the overall reduction in total traffic was moderate, advertising-related requests were almost entirely eliminated. Only one tracker request was observed under Brave versus 153 under Edge. Target's results were the most dramatic case, with Brave generating only three total HTTP requests, compared to 646 under Edge. This suggests either extremely strong tracker blocking behavior, or significant site functionality suppression under GPC conditions. This outlier warrants further investigation in the Analysis section.

The Guardian exhibited one of the highest concentrations of advertising infrastructure in the Edge condition (1,634 third-party requests), which was largely suppressed under GPC. WebMD reported one of the largest absolute reductions in tracker activity. For Zillow, although overall traffic reduction was moderate relative to other sites, tracker suppression remained consistently high.

Patterns Across All Sites

We observed consistent tracker suppression, variability in total request reduction, and an absence of observable cookies. For tracker suppression, across all six websites, tracker/ad requests were reduced by 97–99% in every case, numerous advertising domains appeared exclusively in the Edge condition, and referrer leakage closely tracked third-party request reductions.This consistency suggests systematic suppression of advertising and tracking infrastructure when GPC is enabled.

For variability in total request reduction, there was great variability, ranging from moderate (22%) on Best Buy, high (90%+) on Guardian, WebMD, and extreme (99.5%) on Target. This indicates that while tracker blocking is consistently strong, overall network behavior varies depending on site architecture.

Lastly, regarding absences in observable cookies, no request cookies or Set-Cookie responses were observed in either browser condition. This suggests that either cookies were not set during the captured session window, or tracking occurred primarily through request-based identifiers rather than cookie persistence. Because HAR captures do not detect fingerprinting or Local Shared Objects (LSOs), tracking may persist through non-cookie mechanisms.

Preliminary Interpretation

The data demonstrates that enabling GPC (via Brave) corresponds with:

- Substantial reductions in third-party communication
- Near-total elimination of known tracker domains
- Major decreases in referrer leakage

However, because Brave also includes built-in tracker blocking protections beyond the GPC header itself, the observed reductions cannot be attributed solely to the GPC signal without further isolation testing. Nonetheless, the results indicate that, in practice, GPC-enabled browsing environments are associated with dramatically reduced observable advertising and third-party tracking activity compared to a non-GPC baseline browser.

Analysis

Usability and Enforceability of Global Privacy Control[11]: Global Privacy Control is technically simple for users to enable. However, its effectiveness may be highly dependent on website implementation and regulatory context.

Across the websites tested, browsing in a GPC-enabled environment was associated with a substantial reduction in third-party requests, tracker domains, and referrer leakage compared to default browsing conditions. In several cases, tracker and advertising-related requests dropped by more than 90%, indicating that privacy-enhanced browser environments can significantly limit observable tracking activity. These results align with prior research showing the widespread use of third-party tracking infrastructure and the difficulty users face in controlling it through manual consent mechanisms.

However, the results also show that tracking behavior is not uniform across websites. Some sites continued to generate third-party requests even when GPC was enabled, suggesting inconsistent interpretation of privacy signals or reliance on alternative tracking techniques. Differences in consent banner design, jurisdictional requirements, and site architecture likely contributed to this variation. Sites operating across multiple regulatory regions may apply different tracking practices depending on perceived legal obligations.

Browsers such as Brave include built-in tracker blocking and privacy protections that operate alongside the GPC signal. As a result, the findings demonstrate the combined effect of privacy-oriented browser configurations rather than isolating the independent impact of GPC itself. Additionally, because the study relied on HAR and network-level measurements, tracking methods such as fingerprinting or server-side profiling may not have been captured. The analysis suggests that automated privacy signals can reduce tracking in practice, but their effectiveness depends on browser implementation, website compliance, and regulatory context.

Limitations

This research is being conducted with a limited team and an accelerated timeline, which constrained observations that could be performed. Additionally, the study focuses primarily on HTTP-based tracking and may not fully capture advanced techniques such as browser fingerprinting. Future research could expand this work by increasing sample size, incorporating longer observation periods, analyzing server-side consent enforcement, and evaluating emerging privacy signals across additional platforms and jurisdictions.

[11] Zimmeck, S., Wang, O., Alicki, K., Wang, J., & Eng, S. (2023). Usability and enforceability of Global Privacy Control. *Proceedings on Privacy Enhancing Technologies*, *2023*(2), 265–281. https://doi.org/10.56553/popets-2023-0052

Conclusion

This study set out to examine whether enabling Global Privacy Control leads to measurable reductions in website tracking compared to default browsing and manual cookie opt-out mechanisms. Across six commercial websites, we observed consistent and substantial decreases in third-party requests, advertising-related traffic, and referrer leakage when browsing in a GPC-enabled environment. Tracker and advertising requests were reduced by more than 95% in most cases, suggesting that browser environments sending a GPC signal are associated with significantly lower observable tracking activity.

Brave browser includes built-in tracker blocking features beyond the GPC signal itself, meaning that the observed reductions cannot be attributed solely to GPC. The results therefore demonstrate how privacy-enhanced browsing environments can reduce tracking in practice, but do not conclusively isolate the independent effect of GPC.

The study highlights several important highlights. The universal privacy signals like GPC have the potential to reduce tracking without requiring repeated user interaction with consent banners. At the same time, implementation remains inconsistent across websites and jurisdictions, indicating that legal recognition alone does not guarantee uniform compliance. Browser design choices play a major role in shaping user privacy outcomes, often more than website consent interfaces.

Overall, our findings suggest that while Global Privacy Control represents a meaningful step toward automated privacy preference signaling, its real-world effectiveness depends on a combination of browser implementation, website compliance, and regulatory enforcement. Continued measurement and policy attention are necessary to ensure that legally recognized privacy signals translate into practical protections for users.

Appendix

Table A1: CNN Results

Metric	Brave (GPC)	Edge (No GPC)	% Difference (Brave vs Edge)
Total HTTP Requests	274	1240	↓ 77.9%
Sec-GPC Header Present	184	0	—
GPC Value(s)	1	—	—
DNT Header Present	0	0	N/A
Third-Party Requests	104	995	↓ 89.5%
Unique Third-Party Domains	43	154	↓ 72.1%
Tracker/Ad Requests	30	488	↓ 93.9%
Unique Tracker Domains	11	32	↓ 65.6%
Total Request Cookies Sent	0	0	N/A
Unique Cookie Names	0	0	N/A
Set-Cookie (response) Total	0	0	N/A
Set-Cookie: Secure flag	0	0	N/A
Set-Cookie: HttpOnly flag	0	0	N/A
Referer Leakage (3rd party)	104	975	↓ 89.3%

Table A2: Best Buy Results

Metric	Brave (GPC)	Edge (No GPC)	% Difference (Brave vs Edge)
Total HTTP Requests	1078	1382	-22.00%
Sec-GPC Header Present	1025	0	–
GPC Value(s)	1	–	–
DNT Header Present	0	0	N/A
Third-Party Requests	668	957	-30.20%
Unique Third-Party Domains	7	43	-83.70%
Tracker/Ad Requests	1	153	-99.30%
Unique Tracker Domains	1	13	-92.30%
Total Request Cookies Sent	0	0	N/A
Unique Cookie Names	0	0	N/A
Set-Cookie (response) Total	0	0	N/A
Set-Cookie: Secure flag	0	0	N/A
Set-Cookie: HttpOnly flag	0	0	N/A
Referer Leakage (3rd party)	668	954	-30.00%

Table A3: Target Results

Metric	Brave (GPC)	Edge (No GPC)	% Difference (Brave vs Edge)
Total HTTP Requests	3	646	-99.50%
Sec-GPC Header Present	2	0	–
GPC Value(s)	1	–	–
DNT Header Present	0	0	N/A
Third-Party Requests	0	421	-100.00%
Unique Third-Party Domains	0	18	-100.00%
Tracker/Ad Requests	3	278	-98.90%
Unique Tracker Domains	1	6	-83.30%
Total Request Cookies Sent	0	0	N/A
Unique Cookie Names	0	0	N/A
Set-Cookie (response) Total	0	0	N/A
Set-Cookie: Secure flag	0	0	N/A
Set-Cookie: HttpOnly flag	0	0	N/A
Referer Leakage (3rd party)	0	420	-100.00%

Table A4: The Guardian Results

Metric	Brave (GPC)	Edge (No GPC)	% Difference (Brave vs Edge)
Total HTTP Requests	131	1671	-92.20%
Sec-GPC Header Present	126	0	–
GPC Value(s)	1	–	–
DNT Header Present	0	0	N/A
Third-Party Requests	94	1634	-94.20%
Unique Third-Party Domains	4	173	-97.70%
Tracker/Ad Requests	4	691	-99.40%
Unique Tracker Domains	2	35	-94.30%
Total Request Cookies Sent	0	0	N/A
Unique Cookie Names	0	0	N/A
Set-Cookie (response) Total	0	0	N/A
Set-Cookie: Secure flag	0	0	N/A
Set-Cookie: HttpOnly flag	0	0	N/A
Referer Leakage (3rd party)	90	1601	-94.40%

Table A5: WebMD Results

Metric	Brave (GPC)	Edge (No GPC)	% Difference (Brave vs Edge)
Total HTTP Requests	118	2294	-94.90%
Sec-GPC Header Present	83	0	—
GPC Value(s)	1	—	—
DNT Header Present	0	0	N/A
Third-Party Requests	104	2254	-95.40%
Unique Third-Party Domains	23	211	-89.10%
Tracker/Ad Requests	6	896	-99.30%
Unique Tracker Domains	6	46	-87.00%
Total Request Cookies Sent	0	0	N/A
Unique Cookie Names	0	0	N/A
Set-Cookie (response) Total	0	0	N/A
Set-Cookie: Secure flag	0	0	N/A
Set-Cookie: HttpOnly flag	0	0	N/A
Referer Leakage (3rd party)	104	2161	-95.20%

Table A6: Zillow Results

Metric	Brave (GPC)	Edge (No GPC)	% Difference (Brave vs Edge)
Total HTTP Requests	133	512	-74.00%
Sec-GPC Header Present	112	0	—
GPC Value(s)	1	—	—
DNT Header Present	0	0	N/A
Third-Party Requests	113	488	-76.80%
Unique Third-Party Domains	17	46	-63.00%
Tracker/Ad Requests	4	147	-97.30%
Unique Tracker Domains	4	18	-77.80%
Total Request Cookies Sent	0	0	N/A
Unique Cookie Names	0	0	N/A
Set-Cookie (response) Total	0	0	N/A
Set-Cookie: Secure flag	0	0	N/A
Set-Cookie: HttpOnly flag	0	0	N/A
Referer Leakage (3rd party)	113	482	-76.60%

Table A7: All Websites Combined Results

Metric	Brave (GPC)	Edge (no GPC)
Total HTTP Requests	1737	7745
Requests w/ Sec-GPC header	1532	0
Third-Party Requests	1083	6749
Tracker/Ad Requests	48	2653
Total Request Cookies	0	0
Set-Cookie Responses	0	0
Referer Leakage Events	1079	6593

GPC Impact (Brave reduction vs Edge):

- Third-Party Requests → ↓ 84.0% reduction
- Tracker Requests → ↓ 98.2% reduction
- Total Cookies Sent → N/A (Edge = 0)
- Set-Cookie Responses → N/A (Edge = 0)
- Referer Leakage → ↓ 83.6% reduction

References

Academic & Research. Autopsy. (2019, August 15). https://www.autopsy.com/use-case/academic-research/

Builtwith trends. (n.d.-a). https://trends.builtwith.com/websitelist/US-Privacy-User-Signal-Mechanism

Builtwith trends. (n.d.-b). https://trends.builtwith.com/websitelist/Global-Privacy-Control

Congiu, R., Sabatino, L., & Sapi, G. (2022). The impact of privacy regulation on web traffic: Evidence from the GDPR. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4025033

Cranor, L. F., Sleeper, M., & Ur, B. (2013), Tracking and Surveillance. Mimeo.

Englehardt, S., & Nayaranan, A. (2016, October 24). Online Tracking: A 1-million-site Measurement and Analysis. *Association for Computing Machinery*. https://doi.org/10.1145/2976749.2978313

Englehardt, S., & Narayanan, A. (2016). Online Tracking. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. https://doi.org/10.1145/2976749.2978313

Global Privacy Control (GPC). W3C. (n.d.). https://www.w3.org/TR/gpc/

Global Privacy Control (GPC). (2025, January 28). State of California - Department of Justice - Office of the Attorney General. https://oag.ca.gov/privacy/ccpa/gpc

Global Privacy Control. (2020, October 7). Globalprivacycontrol.org. https://globalprivacycontrol.org/press-release/20201007

Hils, M., Woods, D. W., & Böhme, R. (2023). Conflicting Privacy Preference Signals in the wild. *Data Protection and Privacy, Volume 15*. https://doi.org/10.5040/9781509965939.ch-004

Kamara, I. & Kosta, E. (2016 November). Do Not Track Initiatives: Regaining the Lost User Control. *International Data Privacy Law,* vol. 6, Issue 4, pp 276–290, https://doi.org/10.1093/idpl/ipw019

Mayer, J. R., & Mitchell, J. C. (2012). Third-Party Web Tracking: Policy and Technology. *2012 IEEE Symposium on Security and Privacy*. https://doi.org/10.1109/sp.2012.47

Mazel, J., Garnier, R., & Fukuda, K. (2019). A comparison of Web Privacy Protection Techniques. *Computer Communications*, *144*, 162–174.

https://doi.org/10.1016/j.comcom.2019.04.005

My journey to performance analysis 2/2 (har files) | by Julien Piccini | TDS archive | medium. (n.d.). https://medium.com/data-science/my-journey-to-performance-analysis-2-2-har-files-8a94a52bfac9

Sim, K., Heo, H., & Cho, H. (2024, October 5). *Combating Web Tracking: Analyzing Web Tracking Technologies for user privacy*. MDPI. https://www.mdpi.com/1999-5903/16/10/363

Zimmeck, S., Wang, O., Alicki, K., Wang, J., & Eng, S. (2023). Usability and enforceability of Global Privacy Control. *Proceedings on Privacy Enhancing Technologies*, *2023*(2), 265–281. https://doi.org/10.56553/popets-2023-0052

Zimmeck, S., Snyder, P., Brookman, J., & Zucker-Scharff, A. (Eds.). (2025, December 17). *Global Privacy Control*. W3.org. https://www.w3.org/TR/gpc/