Effects of Global Privacy Control (GPC) on Web Tracking Across Different Regional Jurisdictions

Young June Yoon
Washington University in St. Louis
yoon.y@wustl.edu

Jiwoo Seo
Washington University in St. Louis
jiwooseo@wustl.edu

Abstract

In the digital age, user data has become a core part of the profit in online business models, leading to advanced tracking methods and rising concerns over user privacy. This paper examines the effectiveness of Global Privacy Control (GPC) across different jurisdictions, particularly under the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR). Our study analyzes the impact of GPC on web tracking activities, focusing on three regions: St. Louis (Missouri), Los Angeles (California), and Frankfurt (Germany). We analyzed the top 1000 websites from the Tranco 1M list, assessing changes in HTTP requests and cookies with GPC enabled versus disabled. Our findings reveal a reduction in tracking activities in St. Louis and Los Angeles, where enabling GPC led to a notable decrease in HTTP requests and cookies, reflecting compliance with user privacy preferences. In contrast, the data from Frankfurt shows minimal impact from enabling GPC, suggesting the robustness of GDPR's existing privacy controls. These results highlight the varied effectiveness of GPC across different regions and provide insights into how the emphasis and focus of privacy laws can incur different outcomes in tracking behaviors.

Keywords Global Privacy Control (GPC), Califonial Consumer Privacy Act (CCPA), Global Data Protection Regulation (GDPR), HTTP Requests, Cookies, Do Not Track (DNT)

1 Introduction

In the rapidly expanding realm of online advertising and markets, users' personal information has increasingly become a central component of profit generation. Numerous tracking methods have been developed to monitor users and monetize their data. These tracking processes often collect highly personal information, as the more personal it is, the more tailored the advertisements can be. However, this intense and active tracking can be seen as a violation of privacy, especially since users are often unaware of their data being collected.

In response to the need for giving consumers greater control over their personal information, several regional privacy laws have been established. Two notable examples are the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR) of the European Union.

The CCPA, effective since January 2020, empowers California residents with the right to know what personal data is being collected about them, to request the deletion of their data, and to opt-out of the sale of their personal information by businesses. It applies to any for-profit entity that collects consumers' personal data and satisfies certain thresholds [6].

The GDPR, implemented in May 2018, is a comprehensive data protection law in the European Union. It gives individuals more control and rights over their personal data. It applies to all organizations that process the data of EU residents, regardless of the organization's location. The GDPR mandates clear consent for data processing, provides rights for data access, correction, and erasure, and requires companies to implement protective measures for data security [11].

The right to opt-out is especially crucial as it determines whether individuals' data is entered into the online advertising ecosystem. If data is not collected in the first place, there would be no necessity to request access to or deletion of this data [20]. To allow consumers to exercise their opt-out rights, CCPA requires businesses to provide a clear and conspicuous link on their website's homepage, titled "Do Not Sell My Personal Information." However, this method can be very exhausting and tedious because the user has to visit DNSMPI link and fill up opt-out form for every website they visit. The GDPR explicitly mentions that any withdrawal of consent must be as easy as giving it in GDPR Art. 7(3). In the light of simplifying the process of managing online privacy settings and let consumers exercise their rights with initiative, Global Privacy Control was developed.

Instead of having to manually opt-out of data selling on every website, users can set their preferences once in their browser, and these preferences are communicated automatically to each website they visit.

Global Privacy Control functions as a binary switch for web tracking. It can be implemented either through the Sec-GPC

request header or via the GPC JavaScript DOM property [13]. This allows websites to quickly ascertain the opt-out status of a visitor.

In this paper, by investigating top 1000 websites from Tranco 1M with GPC signals on/off, we aim to answer the following questions:

1. Is Global Privacy Control relevant and respected by popular websites across the regions with privacy laws?
2. Will websites accessed from regions with stringent privacy laws (e.g., California with CCPA) are more likely to respect the GPC and exhibit reduced tracking behaviors compared to the region without such laws?

2 Background and Related Work

2.1 DNT

'Do Not Track (DNT)' request header, proposed in 2009, was designed to allow internet users to opt-out of tracking by websites. It included the collection of data regarding user activity across multiple distinct contexts. Similar to GPC, DNT request header sends a signal from a user's browser to all sites they visit stating that user's preference not to be tracked.

However, without any legal enforcement, the DNT header was not respected by many websites. It was studied that only two out of hundreds of advertising networks had agreed to respect DNT headers at the time of the study [1].

DNT headers remained largely ineffective for a long time, and in 2019, Apple brought an end to the DNT header. Apple removed the DNT toggle button from Safari, stating that DNT ironically makes users more susceptible to fingerprinting tracking, as trackers could use the DNT header as a variable for fingerprinting [17]. The failure of DNT underscores the importance of legal enforcement for beneficial features to be respected and effectively used, highlighting how implementation can make a significant difference.

GPC is regarded as the spiritual successor to DNT, and they are similar in that both serve as a binary switch to signal user preferences to browsers. To avoid the pitfalls experienced by DNT, legal enforcement was emphasized during the development of GPC.

2.2 Legal Bindings

As discussed in Section 2.1, it is crucial to establish legal bindings between GPC and privacy laws to ensure that websites comply with users' preferences.

2.2.1 California Consumer Privacy Act (CCPA)

Per CCPA, California consumers can direct businesses to not sell or share their personal information to third parties. 'Selling' is defined as obtaining any monetary gain, for example, by disclosing a consumer's personal information to an ad network on a website via third party cookies [9]. The 'Sharing' part was added to the CCPA when the California Privacy Rights Act (CPRA) amended it. 'Sharing' is defined as the disclosure of consumers' personal information to another entity for the purpose of advertising, based on the user's interactions on the website or inferred preferences [10]. This could be understood as any exchange between the first and third parties that doesn't involve direct monetary transactions, but where both parties benefit from the disclosure of users' information. An example of this is re-targeted ads, where an ad network re-targets a business's products while the business provides the user's personal information.

As CCPA gives consumers right to opt-out, we can infer that GPC request header is a valid request to opt-out of the sale and share of their data. The Office of the California Attorney General has stated, 'CCPA requires businesses to treat a user-enabled global privacy control as a legally valid consumer request to opt out of the sale of their data. [3]' Furthermore, in 2022, the California Attorney General announced a $1.2 million settlement with Sephora for failing to process user requests to opt out of the sale and sharing of data via user-enabled GPC. This highlights the Office of the California Attorney General's commitment to ensuring businesses respect users' preferences when signaled and enforcing accountability for those still not complying with California's consumer privacy laws. The OAG explicitly states - "There are no more excuses. Follow the law, do right by consumers, and process opt-out requests made via user-enabled global privacy controls. [7]"

These cases show the strong legal bindings between California's consumer privacy laws (CCPA and CPRA) and GPC.

2.2.2 General Data Protection Regulation (GDPR)

GDPR is a comprehensive data protection law that came into effect in the European Union that aims to enhance individuals' control and rights over their personal data. Under GDPR, personal data is defined broadly and includes any information relating to an identified or identifiable natural person ('data subject'). This can be anything from a name, an ID number, location data, to factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that person (GDPR Art. 4) [12].

The GDPR grants numerous rights to data subjects, including the right to access their personal data (Art. 15), the right to have incorrect data corrected (Art. 16), the right to have their data erased under certain conditions (the 'right to be forgotten') (Art. 17), the right to restrict or object to processing of their data (Art. 18, 20), and the right to data portability (Art. 21). The regulation places stricter conditions on the consent mechanism, requiring it to be given through an affirmative act (such as ticking a box), freely, specific, informed, and un-

ambiguous (Art. 7). Consent should also be withdrawn at any time (Art. 7 Recital 43) [12].

GDPR and CCPA differ in how they require businesses to handle user data before any user preferences (such as consent, withdrawal, opt-in, or opt-out) are expressed. Notably, the GDPR does not incorporate 'opt-outs.' Instead, it explicitly mandates an 'opt-in' approach through user consent, and any request to stop sharing data with a third party is essentially equivalent to withdrawing that consent [16]. In essence, GDPR operates on a default opt-out basis, meaning that businesses must seek consent from users in the EU before they can sell or share their personal information, regardless of whether the user has enabled GPC or not. Therefore, the presence of GPC may not affect the opt-outness, for the websites should not be selling or sharing user data before acquiring the consent.

On the other hand, non-compliance with GPC can be considered a serious violation of GDPR, as it signifies a disregard for user preferences and consent, which are central tenets of GDPR. As we aim to research the effects of GPC on web tracking across different regional jurisdictions, these distinctions between the two regional privacy laws present an intriguing variable for our study.

2.3 GPC

'Global Privacy Control' (GPC) is a technical standard that enables users to automatically communicate their privacy preferences, such as opting out of the sale of their personal information, to websites they visit. It's designed to work with existing legal frameworks like the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR) in the European Union.

User Preference Setting Users can set their privacy preferences in their web browser configuration settings or through other applications. This setting indicates that they want to limit how their personal data is used or sold by the websites they visit.

Automatic Communication When a user with GPC enabled visits a website, the browser automatically communicates the user's privacy preference to the website through an HTTP header (Sec-GPC).

Website Compliance Websites that recognize and respect GPC should then act according to the user's preferences. This might involve not selling the user's data, not tracking them for advertising purposes, or providing additional privacy protections.

Legal Frameworks GPC is designed to work within existing legal frameworks. In jurisdictions like California, where the law requires businesses to respect user opt-outs for the sale of personal information, GPC can serve as a legally binding indication of the user's preferences.

DNT header was considered vulnerable by Apple because it could be exploited for fingerprinting. To address this issue, some browsers, including Brave, are now adopting the GPC header as their default configuration setting. This approach ensures that Brave users are protected from fingerprinting risks while exercising their opt-out rights [5]. The effectiveness of GPC would increase significantly if more browsers adopted it as their default configuration setting.

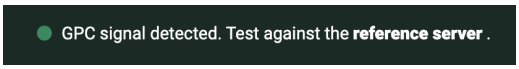


Figure 1: GPC signal detection on globalprivacycontrol.org website

To verify if the header request is correctly sent, users can visit https://globalprivacycontrol.org/ and check the top banner for the GPC signal, as shown in Figure 1.

GPC was developed through a collaborative effort involving a diverse group of stakeholders, including web browser developers, technology companies, researchers, and privacy advocates [14]. This initiative wasn't founded by a single individual or organization; rather, it was a collective response to the growing demand for enhanced online privacy controls and the necessity for a standardized method to implement and respect user privacy choices, in line with evolving laws and regulations.

The development and adoption of GPC represent a significant stride in the broader movement towards strengthening online privacy and empowering users with greater control over their personal data. However, the effectiveness of GPC may depend on its widespread acceptance by both users and websites, as well as the enforcement of relevant legal frameworks in various jurisdictions.

3 Methodology

In this research, we aim to assess the impact of Global Privacy Control (GPC) in diverse legal environments. In order to observe the effectiveness of GPC on various websites, we need to collect a wide range of data, including information on tracking cookies, as well as HTTP request / response details. In this section, we outline the techniques we use to collect this essential data.

3.1 Website Selection

We start by selecting the websites to crawl for our study. For a website selection, we need to gather a website list that can represent websites that normal users frequently visit. In order to get a list that fulfills this requirement, we decided to use the Tranco list [19] - a research-focused ranking of top websites designed to be resistant to manipulation. From this list, we extracted the top 1,000 websites to represent websites from

various categories. The Tranco list is updated daily, so we used the latest version available on November 12th, 2023. This approach ensured consistency in our website selection as we collected web data throughout the course of our research.

Along with the list of popular websites, our study requires a list of tracking domains. This is to isolate and focus solely on domains related to tracking, enabling a more accurate assessment of GPC's effectiveness. For this purpose, we utilized The Block List Project [4] from GitHub. The project offers domain lists that are frequently updated by community members, maintaining their relevance against emerging online threats. Among their various lists, we specifically opted tracking domain list, which includes 15,070 domains dedicated to tracking and gathering visitor information.

3.2 Vantage Points

Next, we selected various strategic locations as vantage points to perform our web crawls, aiming to highlight the varying effectiveness of GPC in regions with different privacy laws. Los Angeles, California was chosen to observe GPC's impact under the California Consumer Privacy Act (CCPA). Frankfurt, Germany was selected as our second vantage point to evaluate GPC under the General Data Protection Regulation (GDPR). For the baseline location, we chose St. Louis, Missouri, which doesn't have any specific local privacy laws and is not affected by CCPA or GDPR.

Due to the geographical constraints, we opted to use a hardware-level VPN service to simulate our presence in these locations. To accomplish this, we utilized ExpressVPN, allowing us to set our hardware's apparent location to our chosen vantage points.

3.3 OpenWPM Setup

To gather necessary information from websites, choosing a web crawler that fits our needs is important. Upon reviewing various available open-source web crawlers, we decided to use OpenWPM for its stability, scalability, and ease of use, along with strong community support. OpenWPM efficiently captures detailed data like cookies from HTTP requests and JavaScript, as well as HTTP request-response details.

Custom Browser Profile Since OpenWPM is highly customizable, the platform provides the ability to choose a browser and load a custom browser profile for the crawl. OpenWPM's high customizability allowed us to select and configure Firefox as our browser for web crawling, utilizing its support for Global Privacy Control (GPC) starting from Firefox version 95 [15]. We created two distinct Firefox profiles for our study: one with GPC enabled and the other with GPC disabled, ensuring both were set up with fresh installations for consistent measurement. In the profile where GPC was disabled, the HTTP request headers sent by the profile do not include any signs of GPC. These profiles were then integrated into OpenWPM for data collection during our website crawls.

Stateful vs. Stateless Crawl OpenWPM offers two modes of web crawling: stateful and stateless. In stateful crawling, the same browser profile is maintained throughout multiple page visits within the same browser session. On the other hand, stateless crawls use a fresh browser profile in each new page visit, treating every request as a standalone interaction, independent of any prior browsing activity. We chose to go with stateless crawling in our study, as this approach ensures more uniform results by treating each website visit independently, without influence from the sequence of sites visited.

3.4 Crawling Web Data

We performed twelve crawl sessions to collect information from websites on our list. At each of our selected vantage points, we executed two crawls for the top 1,000 websites from the Tranco list: one with GPC enabled and one without GPC header. This resulted in six crawls in total. To ensure the accuracy and reliability of our data, we repeated these crawls, bringing the total number of crawls for our study to twelve.

During our crawling process, we encountered issues with 262 to 268 websites, approximately 26% of the list, due to various errors such as DNS errors or connection failure errors. Such issues were expected as Tranco list contains many popular domains that do not host websites. For instance, URLs associated with content distribution networks (CDN), like `http://rlcdn.com`, often do not host websites.

The crawls were conducted using a 2021 Apple MacBook Pro, which is powered by an Apple M1 Pro processor and equipped with 16GB of RAM. The operating system on this device is MacOS Sonoma, version 14.1.

4 Evaluation

In this section, we evaluate our crawled data to assess how GPC impacts the tracking behavior of popular websites, with a particular emphasis on regional variations.

4.1 HTTP Requests

Number of All HTTP Requests Number of HTTP requests is an important indicator of how websites are tracking users. A number of HTTP requests gives a preliminary idea about the potential tracking on a website since more requests could mean more chances for user tracking and data collection. Figure 2 presents the number of HTTP requests in three different regions, comparing with GPC header enabled and without GPC.

In St. Louis, when GPC is enabled, the number of HTTP requests drops by 15,740, which is a 12.6% decrease compared to the baseline, where GPC is disabled. In Los

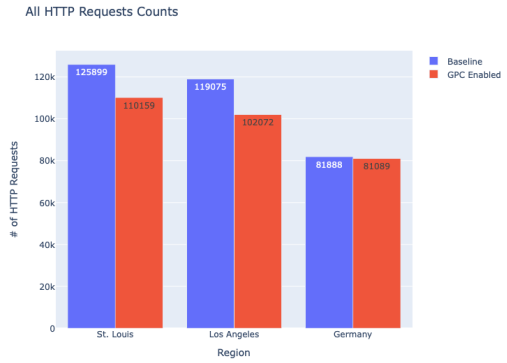


Figure 2: Number of All HTTP Requests

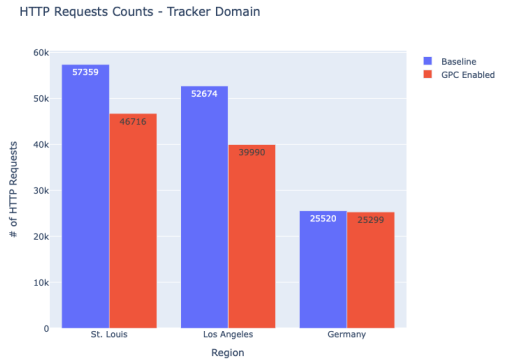


Figure 3: Number of HTTP Requests to Tracker Domain

Angeles, the activation of GPC led to a decrease of 17,003 HTTP requests, translating to a 14.3% drop compared to the baseline. However, in Frankfurt, Germany, the impact of GPC on HTTP requests was minimal, with only a 799 request reduction, accounting for a mere 1% decrease.

Number of HTTP Requests Made to Tracker Domain While the total count of HTTP requests suggests the tracking behavior of websites, examining the number of HTTP requests specifically made to the tracker domain reveals more detailed insight into their tracking behaviors. To achieve this, we utilized a tracker domain list from The Block List Project to isolate only those HTTP requests directed towards known tracking domains, filtering out requests to non-tracking sites. Figure 3 displays the volume of HTTP requests directed to tracking domains across three different regions, comparing with and without GPC enabled.

Figure 3 shows a significant reduction in HTTP requests to tracking domains with GPC enabled. In St. Louis, there's a decline of 10,643 requests, amounting to an 18.6% reduction compared to the baseline without GPC. Los Angeles sees a more substantial drop of 12,684 requests to tracking domains, which is a 24.1% decrease from the baseline. Conversely, in Frankfurt, Germany, the reduction is marginal with only 221 fewer requests to tracker domains, less than a 1% decrease. These figures indicate that activating GPC effectively reduces HTTP requests to tracking domains in St. Louis and Los Angeles. Moreover, when examining the proportion of this reduction in relation to the total decrease in HTTP requests, we can observe interesting patterns. In St. Louis, about 68% of the overall reduction in HTTP requests can be attributed to tracking domains. A similar trend is observed in Los Angeles, where approximately 74% of the total HTTP request reduction is linked to tracker domains. This demonstrates that in St. Louis and Los Angeles, activating GPC noticeably reduces the number of HTTP requests to tracking domains.

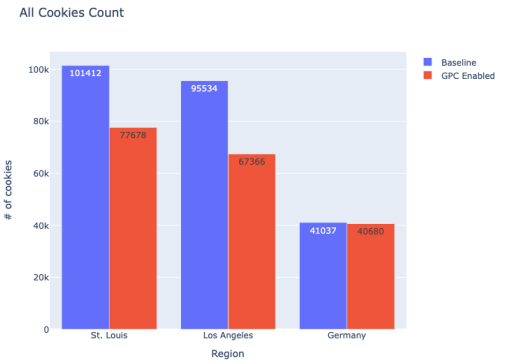


Figure 4: Number of Cookies (JavaScript + HTTP response)

4.2 Number of Cookies

Number of All Cookies The number of cookies set by JavaScript and through HTTP responses is another important metric for assessing user tracking on websites. Cookies, often used as tracking tools, store various user information such as preferences, login details, and browsing history. JavaScript-set cookies, which are dynamically generated during browsing sessions, reveal the tracking mechanisms activated by user interaction, while cookies set via HTTP responses from the server indicate server-side tracking practices. Figure 4 illustrates the number of cookies set by both JavaScript and HTTP responses in three regions, comparing scenarios with and without GPC enabled.

In St. Louis, when GPC is enabled, the number of cookies drops by 23,734, which is a 23.4% decrease compared to the baseline, where GPC is disabled. In Los Angeles, the activation of GPC led to a decrease of 28,168 cookies, translating to a 29.5% drop compared to the baseline. However, in Frankfurt, Germany, the impact of GPC on HTTP requests was minimal, with only a 357 request reduction, accounting for a mere 0.8% decrease.

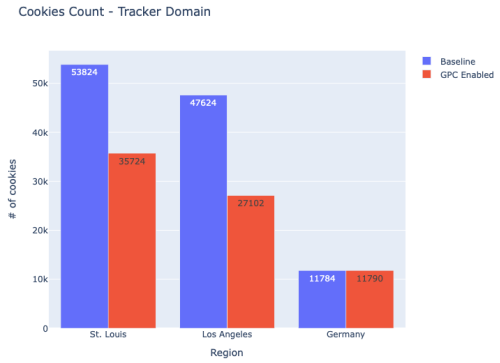


Figure 5: Number of Cookies set by Tracker Domains (JavaScript + HTTP response)

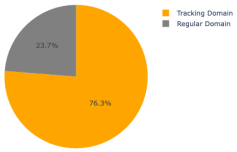
Number of Cookies Set by Tracker Domains While the total count of cookies set by JavaScript and HTTP responses indicates the tracking behavior of websites, a closer examination of cookies specifically set by known tracking domains offers a more detailed insight into their tracking practices. Figure 5 illustrates the number of cookies set by tracking domains across three regions, comparing scenarios with and without GPC enabled.

Figure 5 shows a significant reduction in cookies set by tracking domains with GPC enabled. In St. Louis, there's a decline of 18,100 cookies, amounting to a 33.6% reduction compared to the baseline without GPC. Los Angeles experienced an even more pronounced decrease, with 20,522 fewer cookies set by tracking domains, amounting to a 43.1% reduction from the baseline. In Frankfurt, Germany, we observed a slight increase in the cookie counts. These findings suggest that activating GPC effectively diminishes the number of cookies set by tracking domains. As illustrated in Figure 6, we could observe interesting patterns as we looked into the proportion of this reduction in relation to the total decrease in total cookie counts. As illustrated in Figure 6 - in St. Louis, about 76.3% of the total reduction in cookies was set by tracking domains. Similarly, in Los Angeles, around 72.9% of the overall decrease in cookies was attributed to tracker domains.

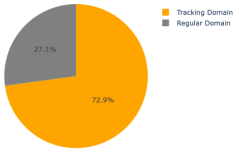
Although the impact of GPC in Frankfurt was none, the number of cookies set by tracker domains was only about one-fifth to one-quarter of that in other regions before enabling the GPC header. This indicates a minimal level of cookie setting by tracking domains under the GDPR, regardless of users' opt-out preferences.

4.3 Top 10 Cookies Domain Reduction

Next, we aimed to assess the impact of GPC on the quantity of JavaScript cookies set by prominent tracking domains in St. Louis and Los Angeles. To do so, we conducted an analysis comparing the number of JavaScript cookies set by the top



(a) St. Louis



(b) Los Angeles

Figure 6: Breakdown of Cookie Reduction Percentage – Comparison between Non-Tracking Domain Cookies and Tracking Domain Cookies as a Proportion of Total Decrease in Cookie Counts

Tracker Domain Name	Cookies Count - No GPC	Cookies Count - GPC Enabled	Drop Percentage
pubmatic	4370	3329	24%
rubiconproject	4164	960	77%
yahoo	2442	1733	29%
adsrvr	2200	1547	30%
demdex	1729	1015	41%
doubleclick	1253	1103	12%
casalemedia	1167	0	100%
adnxs	1117	757	32%
tapad	1078	772	28%
amazon-adsystem	899	523	42%

(a) St. Louis

Tracker Domain Name	Cookies Count - No GPC	Cookies Count - GPC Enabled	Drop Percentage
pubmatic	3956	2131	46%
rubiconproject	3055	611	80%
yahoo	2179	1324	39%
adsrvr	2002	720	64%
demdex	1664	851	49%
doubleclick	1231	845	31%
casalemedia	1051	0	100%
adnxs	1011	482	52%
tapad	923	473	49%
amazon-adsystem	800	473	41%

(b) Los Angeles

Figure 7: The Difference in the number of Javascript Cookies set by Popular Tracking Domains when comparing GPC enabled and GPC disabled in St. Louis and Los Angeles

10 tracking domains with GPC enabled versus disabled in both St. Louis and Los Angeles. These domains were selected based on their high volume of JavaScript cookies when GPC is disabled. This analysis provides insights into how popular tracking domains respond to GPC, specifically in terms of the number of JavaScript cookies, in both St. Louis and Los Angeles.

Figure 7(a) shows the decrease in the amount of JavaScript cookies set by the top 10 tracking domains in St. Louis when GPC is activated. The reductions range from 12% to a complete 100%. It's noteworthy that a major tracking domain like RubiconProject shows a 77% decline in cookie settings. Also, the tracker domain CasaleMedia stops setting JavaScript cookies entirely with GPC enabled, leading to a 100% drop. This data indicates that GPC effectively reduces the number of JavaScript cookies set by well-known domains in St. Louis.

Figure 7(b) depicts the reduction in JavaScript cookies set by the top 10 tracking domains in Los Angeles with GPC enabled. In Los Angeles, every domain among the top 10 trackers shows a decrease in JavaScript cookie setting when GPC is enabled. Interestingly, the percentage drop in most of these tracking domains is about double compared to the reductions observed in St. Louis. This suggests that top tracking domains exhibit more restraint in cookie setting in Los Angeles when GPC is enabled. It also highlights the effectiveness of GPC in substantially reducing the number of tracking-related cookies set by popular trackers in the Los Angeles area.

5 Ethics

Although our research did not directly involve human subjects, it did require the collection of data from websites, which might have included personal information. However, given that our selection comprised the top 1000 websites from the Tranco 1M list, we believe our study focused on sites that are widely accessible to the public and less likely to contain personal information.

The data collected during the crawl was stored in SQLite format, as provided by OpenWPM. To prevent any data breaches, we have decided to delete all the crawled data after completing this report, keeping only the statistical values.

6 Conclusion and Discussion

GPC enabled v. no GPC header There are notable differences in the number of HTTP requests and cookies, especially with tracker domains, when comparing the scenarios where GPC is enabled versus disabled in both St. Louis and Los Angeles. It's important to note that in our experiment, for the baseline profiles where GPC was disabled, the HTTP request headers sent by these profiles did not include any indication of GPC.

St. Louis v. Los Angeles St. Louis and Los Angeles did not show a significant difference in the drop in the number of HTTP requests and cookies. We initially expected a greater decrease in Los Angeles with the GPC header, considering its stringent laws, unlike St. Louis, which doesn't have any. However, it's noteworthy that the number of HTTP requests and cookies in Los Angeles was already about 6% - 10% lower even before enabling GPC. This suggests that the existence of stringent laws may impact tracking practices, regardless of user preferences. As the state of California is committed to enforcing businesses to comply with privacy laws, including but not limited to the CCPA [8], we anticipate seeing greater compliance from websites, especially as California actively penalizes businesses that do not adhere to these regulations.

On the other hand, assessing the applicability of the CCPA is challenging. It's uncertain how many of the top 1000 websites fall under the CCPA's jurisdiction. Given that our experiments were conducted on these top 1000 websites, we believe that many are likely subject to the CCPA. In the future, it would be more meaningful to conduct such a study specifically on businesses that are applicable under the CCPA, after thorough website classification.

It's also interesting to note that St. Louis showed a similar percentage reduction in the number of HTTP requests and cookies. This suggests that many businesses are becoming more cautious in collecting users' personal information when GPC signals are detected. With various regions across the globe beginning to adopt stringent privacy laws [2], it's possible that websites are choosing to respect the GPC signal without implementing geofencing, in an effort to avoid violating any new regulations. Furthermore, some privacy laws, while not explicitly defining their territorial scope, are applicable to entities handling the data of regional residents [2]. Given these developments, it's reasonable for businesses to adopt a more conservative approach to data collection.

When comparing the top 10 domains that set the most cookies in both Los Angeles and St. Louis, a significantly greater reduction in cookie count was observed in Los Angeles. We believe that these top 10 domains are big players, given their extensive cookie settings across the top 1000 websites. The fact that they set considerably fewer cookies for users in Los Angeles compared to those in St. Louis suggests that these big players may be employing geofencing strategies to maximize their profits.

GDPR Even though the number of HTTP requests in Germany was already two-thirds and the number of cookies one-third compared to other regions before enabling GPC, the impact of enabling GPC in Germany was minimal. As discussed in Section 2.2.2, the GDPR places a strong emphasis on 'consent.' Businesses are required to obtain users' consent before selling their data. This implies that user preferences are effectively set to 'opt-out' as they access websites under GDPR. This explains why Germany showed a low number of HTTP requests and cookies with and without GPC.

One could argue that setting the GPC header to 0 in the European Union might imply an 'active opt-in' by the user. This is because, under normal circumstances, users would not have set the GPC header at all [16]. This perspective presents an interesting area for observation, and it would be insightful to explore which aspects of GPC, GDPR, CCPA, and other privacy laws contain loopholes or controversial elements.

Effects of GPC on different regional jurisdiction The effectiveness of GPC varies across regions with different privacy laws, likely influenced by the specific phrasing and

focus of each law. While both the CCPA and GDPR aim to give users more control over their personal information, their approaches to enforcing this control differ. The CCPA provides consumers with the right to opt-out, whereas the GDPR places a stronger emphasis on obtaining user consent.

This divergence in focus is reflected in the differing results observed in California and Frankfurt, each governed by its respective regional privacy laws. Therefore, it is important for policymakers to understand that their choice of language and emphasis can significantly affect the implementation and efficacy of regulations. It is known that approximately 17 regional jurisdictions have referenced the GDPR while developing their own data privacy laws [18]. In formulating these policies and adopting elements from existing frameworks, it becomes essential to integrate the effective aspects and address the areas where improvements are needed.

References

[1] R. Balebako, P. G. Leon, R. Shay, B. Ur, Y. Wang, L. F. Cranor, *Measuring the Effectiveness of Privacy Tools for Limiting Behavioral Advertising*, In Proceedings of the Web 2.0 Workshop on Security and Privacy, IEEE, San Francisco, CA, USA, 2012, pp. 1–10.

[2] A. Baig, *Data Protection & Privacy Laws Around the World*, Published on November 8, 2021, Updated May 5, 2023, Available: https://securiti.ai/data-privacy-laws/, Accessed on 2023-12-05.

[3] Xavier Becerra, Twitter, *[#CCPA]*, [Jan. 28, 2021], [https://twitter.com/AGBecerra/status/1354850758236102656].

[4] The Block List Project, *Primary Block Lists*, [Online]. Available: https://github.com/blocklistproject/Lists. [Accessed: Dec. 11, 2023].

[5] Brave Web Standards Team, *Global Privacy Control, a new Privacy Standard Proposal*, Last Updated October 7, 2020, Available: https://brave.com/web-standards-at-brave/4-global-privacy-control/.

[6] California Department of Justice. California Consumer Privacy Act (CCPA). *Office of the Attorney General, State of California Department of Justice*. Available at: https://oag.ca.gov/privacy/ccpa. Accessed: 2023-12-05.

[7] California Department of Justice, *Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act*, August 24, 2022, Available: https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-0, Accessed on 2023-12-05.

[8] California Department of Justice, *Privacy Enforcement Actions*, Available: https://oag.ca.gov/privacy/privacy-enforcement-actions, Accessed on 2023-12-05.

[9] California State Legislature, *TITLE 1.81.5. California Consumer Privacy Act of 2018*, Available: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5.

[10] CookieYes, *What is 'share' in CPRA?*, Available: https://www.cookieyes.com/knowledge-base/ccpa/what-is-share-in-cpra/, Accessed: 2023-12-05.

[11] GDPR-info. Chapter 1 - General provisions - GDPR. *GDPR-info.eu*. Available at: https://gdpr-info.eu/chapter-1/. Accessed: 2023-12-05.

[12] GDPR Info, *General Data Protection Regulation (GDPR)*, Available: https://gdpr-info.eu/, Accessed: 2023-12-05.

[13] Privacy Community Group. Global Privacy Control (GPC) Specification. *Privacy Community Group at W3C*. Available at: https://privacycg.github.io/gpc-spec/. Accessed: 2023-12-11.

[14] Global Privacy Control Consortium, *Global Privacy Control*, Available: https://globalprivacycontrol.org/, Accessed on 2023-12-05.

[15] Mozilla, *Implementing Global Privacy Control*, [Online]. Available: https://blog.mozilla.org/netpolicy/2021/10/28/implementing-global-privacy-control/. Accessed: 2023-12-05.

[16] H. J. Pandit, *GPC + GDPR: will it work?*, Published on January 28, 2021, Available: https://harshp.com/research/blog/gpc-gdpr-can-it-work, Accessed: 2023-12-05.

[17] M. Simon, *Apple Safari Removing 'Do Not Track'*, Macworld, Published on February 7, 2019, Available: https://www.macworld.com/article/232426/apple-safari-removing-do-not-track.html.

[18] D. Simmons, *17 Countries with GDPR-like Data Privacy Laws*, Published on January 13, 2022, Available: https://insights.comforte.com/countries-with-gdpr-like-data-privacy-laws.

[19] *Tranco: A Research-Oriented Top Sites Ranking Hardened Against Manipulation*, [Online]. Available: https://tranco-list.eu. [Accessed: Nov. 12, 2023].

[20] Sebastian Zimmeck, Oliver Wang, et al. Usability and Enforceability of Global Privacy Control. In *Proceedings on Privacy Enhancing Technologies (PoPETs)*, volume 2, pages 265–281, 2023. DOI: https://doi.org/10.56553/popets-2023-0052.