ABSTRACT

Data protection regulations, such as GDPR and CCPA, require websites and embedded third-parties, especially advertisers, to seek user consent before they can collect and process user data. Only when the users opt in, should these entities collect, process, and share user data. Websites typically incorporate Consent Management Platforms (CMPs), such as OneTrust and CookieBot, to solicit and convey user consent to the embedded advertisers, with the expectation that the consent will be respected. However, neither the websites nor the regulators currently have any mechanism to audit advertisers’ compliance with the user consent, i.e., to determine if advertisers indeed do not collect, process, and share user data when the user opts out.

In this paper, we propose an auditing framework that leverages advertisers’ bidding behavior to empirically assess the violations of data protection regulations. Using our framework, we conduct a measurement study to evaluate four of the most widely deployed CMPs, i.e., Didomi, Quantcast, OneTrust, and CookieBot, as well as advertiser-offered opt-out controls, i.e., National Advertising Initiative’s opt-out, under GDPR and CCPA. Our results indicate that in many cases user data is unfortunately still being collected, processed, and shared even when users opt-out. We also find that some CMPs are better than the others at conveying user consent and that several ad platforms ignore user consent. Our results also indicate that advertiser-offered opt-out are equally ineffective at protecting user privacy.

1 INTRODUCTION

There has been a recent increase in the promulgation of data protection regulations, such as General Data Protection Regulation (GDPR) [47], California Consumer Privacy Act (CCPA) [48], and General Personal Data Protection Act (LGPD) [49], across the globe. At a high level, data protection regulations aim to protect user privacy by mandating online services to take user consent before collection, processing, and sharing of user data. Because of their mass deployment, automatic enforcement, and legal binding, data protection regulations possess the potential to protect user privacy; provided that users do not consent to data collection and processing. In fact, infringement fines have already amounted to billions. For example, in case of GDPR – arguably the most mature data protection regulation – the fines have accumulated to a total of €1.6 billion [21].

However, despite legal binding, prior research has found that online services often trick users into giving positive consent [75], do not include controls to opt-out of data collection and processing [88], or deploy user interfaces that are unintuitive to navigate in terms of providing consent [51, 66]. In cases where users are indeed able to exercise their rights, user data is poorly handled. For example, online services often ignore or respond late to data access requests [87] and even leak sensitive user data to unauthorized users because of weak authentication mechanisms [55, 63]. In some cases, the existence of these issues could be attributed to the complexity of the regulations, unpreparedness, or oversights of online services. In other cases, it could be attributed to reconsideration of online services towards data protection regulations.

Regulators have mostly focused on auditing compliance of large well-known corporations, such as Amazon [5] and Google [8], perhaps because of the lack of systematic mechanisms to automatically detect infringements at scale [22]. Prior research [51, 66, 75, 88] has focused on auditing the implementation deficiencies in consent management platforms/tools but it has largely ignored the instances where compliance is correctly conveyed but online services fail to comply. Though, negligence in implementation raises doubts on the seriousness of online services in protecting users’ privacy, it does not by itself imply non-compliance.

In this paper, we set out to fill this gap in the state-of-the-art research and deployed practice by regulatory bodies in assessing whether online services are actually compliant with the data regulations or not. To this end, we propose a framework to automatically audit regulatory compliance. We focus on cases where user consent is correctly conveyed but online services may not necessarily comply. We evaluate our auditing framework on the web, whereby websites typically record user consent using consent management platforms (CMPs), e.g., OneTrust [29], and convey it to advertisers under GDPR and CCPA. Our key idea is to leak user interest data in controlled A/B experiments, opt-out/in of processing and selling through CMPs, and leverage advertisers’ bidding behavior as a side channel in the advertising ecosystem to infer the processing and selling of user information. Since the bidding behavior of advertisers is shaped up by their pre-existing knowledge of the user, we expect to receive higher bids when advertisers process or sell leaked user interest data, i.e., are non-compliant with the law, despite the user choosing to opt-out.

We summarize our key contributions as follows:

(1) We propose a framework to automatically audit regulatory compliance of online services. We implement our framework by extending OpenWPM [64]. The framework allows us...
to imitate real user, automatically opt-out/opt-in of data processing and selling, and capture advertisers bidding by advertisers.

(2) As a case study, we use our proposed framework to audit regulatory compliance of online services under GDPR and CCPA with four consent management platforms, i.e., Didomi [13], Quantcast [39], OneTrust [29], and CookieBot [9]. Our results indicate that in many cases the advertisers do not necessarily comply with the user consent to opt-out of data processing and selling. Some CMPs perform better than the others, though. For example, when consent is conveyed through Didomi, advertisers bidding behavior significantly changes under CCPA.

(3) We also pursue a comparative analysis between state-enforced regulations and advertiser-offered controls, i.e., National Advertising Initiative’s (NAI) central opt-out [28], in reduction of collection and selling of user data. Our results indicate that the advertiser-offered NAI’s opt-out controls might be equally ineffective at protecting user privacy.

Paper Organization: The rest of the paper is outlined as follows. Section 2 presents an overview of online privacy threats and protection mechanisms. Section 3 describes the design of our framework to audit regulatory compliance of online services. Section 4 presents the results of our auditing. Section 5 presents discussion and limitations of our proposed auditing framework. Section 6 offers the main conclusions from our work.

2 BACKGROUND & RELATED WORK

2.1 Online Tracking
Online trackers capture users browsing histories and activities across the web to facilitate online behavioral advertising, among other use cases [58]. Online tracking is typically conducted through cookies that are set by third party resources loaded on websites, with the key idea being third parties having cross-site access to their cookies. Since most third parties are present on a limited number of websites, they often partner with each other to increase their coverage. Prior research has shown that trackers engage in data sharing partnerships and exchange cookies with as much as 118 other third parties [64], which allows them to increase their coverage by as much as 7 times [82].

Online tracking, and especially tracking driven advertising, poses a serious threat to users’ privacy both at the individual and the societal level. At the individual level, trackers collect sensitive personal information, for example, about health and sexual orientation, which is then used to hyper-target the individuals, for instance, through personalized ads [54, 79]. At the societal level, tracking driven advertising has been leveraged to conduct mass surveillance [26], increase political polarization [50], spread misinformation [17], and discriminate [18]. Overall, people are frustrated by the privacy harms facilitated by online tracking.

2.2 Protection Mechanisms

2.2.1 Self-Regulations. To tackle user privacy concerns and pressure from the regulatory bodies, such as the Federal Trade Commission (FTC), the online advertising industry has responded with self-regulations [19, 33]. However, prominent self-regulatory actions, such as the ones facilitated by browsers, for example, Platform for Privacy Preferences (P3P) [35] and Do Not Track (DNT) [42], and the ones offered by the advertisers, for example, Digital Advertising Alliance’s (DAA) AdChoices [2] and National Advertising Initiative’s (NAI) central opt-out [28], are either not respected by majority of the vendors or they are too convoluted to be used or understood by the lay users.

Browser-Facilitated Automated Controls. Browsers provide several mechanisms that advertisers can leverage to enforce self-regulatory measures in an automated manner. P3P and DNT request headers are two such mechanisms. P3P, now discontinued, was an automated mechanism for online services (e.g., website and third-party vendors) to communicate their privacy policies to web browsers. It was implemented by major web browsers, such as Internet Explorer and Firefox [40, 72], and supported by thousands of websites [60]. However, P3P was often misrepresented by online services [73, 84] likely because it was not enforced under any state regulation. Similarly, DNT was proposed to convey user’s privacy preferences to the online services in an automated manner. However, it also enjoyed limited adoption and it had practically no impact in limiting tracking. Libert et al. [74] reported that only 7% of the websites mentioned DNT in their privacy policies, and in majority of those cases specified that the DNT signal is not respected. Miguel et al. [56], conducted an A/B study and identified that the DNT signal essentially had no impact on ad targeting, experienced by users.

Advertiser-Offered Manual Controls. In response to the concerns from FTC, advertising networks formed National Advertising Initiative (NAI), which provides a central interface for users to opt-out from targeted advertising, i.e., if users opt-out through NAI’s central opt-out interface, they will (supposedly) no longer be tracked for online advertising [27]. McDonald and Cranor [76] conducted a user study and found that only 11% of respondents understood NAI’s opt-out mechanism, which indicates that its adoption is perhaps low. Similarly, taking a step forward in self-regulations, several of the advertising consortiums, created Digital Advertising Alliance (DAA) with an aim to provide easy to access user transparency and control, with “AdChoices” icon, to opt-out of targeted advertisements [2]. Unfortunately, similar to NAI’s opt-out, only 9.9% of ads shown on top websites had AdChoices icon [67].

2.2.2 User-Managed Privacy Protections. Currently, the most effective way for users to self-protect their privacy is to rely on off-the-shelf privacy-enhancing tools, such as AdBlock Plus [1], Privacy Badger [37], and Disconnect [16]. However, privacy-enhancing tools are not available by default in browsers and need to be installed separately; which limits their adoptability to mostly tech-savvy users. Further, trackers engage in an arms-race with privacy-enhancing tools and try to come up with evasive tactics, for example, bounce tracking [89] and CNAME cloaking [61], to evade privacy protections.

The other likely more feasible alternative is to rely on default privacy protections offered by the mainstream browsers, which are available to a larger population. However, these protections are too weak to completely protect user privacy. For example, some mainstream browsers block third-party cookies, which makes them susceptible to new and sophisticated ways of tracking, such as browser
fingerprinting [64, 69]. Further, some browsers, such as Google Chrome, are too cautious even in blocking third-party cookies because of website breakage concerns [43].

2.2.3 State-Enforced Regulations: Focus of Our Work. Both self-regulations and user-managed privacy protections do not have any legal binding and are thus blatantly bypassed by the advertisers and trackers. Only recently, legislators have promulgated regulations, such as General Data Protection Regulation (GDPR) [47] in EU and California Consumer Privacy Act (CCPA) [48] in California, that have potential to rein-in online advertising and tracking ecosystem. These regulations have clearly-stated frameworks that define protocols to collect, share, and use personal user information. Most importantly, their infringements can be prosecuted; which can lead to heavy fines [20, 48]. For example, both Amazon and Google were recently fined for €746 [5, 12] and €50 millions [8] under GDPR, respectively. Essentially, these regulations possess the ability to keep advertising and tracking ecosystem in check.

Both GDPR and CCPA guarantee a right for individuals to opt-out of processing and selling of their data. Under GDPR, online services need to take user consent (Articles 4 (11)) before they can process user data (Article 6 (1) (a)). GDPR has a broad definition of data processing, that includes collecting, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of user data (Article 4 (2)). Under CCPA, online services need to provide user control to opt-out of sale of personal user data (Section 1798 (a) (1)). CCPA has a broad definition of personal data selling, that includes selling, renting, releasing, disclosing, disseminating, making available, and transferring data to another business or a third party for monetary or other valuable consideration (Section 178.140 (t) (1)). Both GDPR’s and CCPA’s data processing and selling definition covers routine data exchanges, such as processing user data to serve personalized ads (e.g., through Real-Time Bidding (RTB) protocol [41]), and sharing data with advertising partners under data sharing partnerships (e.g., with cookie syncing [65]). In fact, The Office of the California’s Attorney General explicitly lists several such examples as violations of CCPA [7, 80]. It is noteworthy that GDPR requires to obtain consent beforehand (Article 6 (1)(a)): Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes. Whereas, CCPA requires to provide tools to opt-out later (Section 1798.120 (a)): A consumer shall have the right, at any time, to direct a business that sells or shares personal information about the consumer to third parties not to sell or share the consumer’s personal information. This right may be referred to as the right to opt-out of sale or sharing. CCPA does not require a beforehand consent because it only restricts the selling/sharing of personal data and not its collection.

Both GDPR and CCPA require websites to provide privacy notices with information and controls to opt-in/out of personal information collection and/or processing. To obtain user consent, websites typically embed off-the-shelf consent management platforms (CMPs), e.g., OneTrust [29] and Cookiebot [9]. CMPs scan websites and identify all cookies set by the HTTP headers and scripts, from both the first and third party resources. In case of GDPR, CMPs should ensure that only strictly necessary cookies are shared and consent is obtained before non-essential cookies, such as for advertising and analytics, are shared. In case of CCPA, CMPs should ensure that they provide controls to users to opt-out to sell their personal information.

![Consent management dialog for GDPR](image1.png)

(a) Consent management dialog for GDPR.

![Consent management dialog for CCPA](image2.png)

(b) Consent management dialog for CCPA.

Figure 1: OneTrust’s consent management dialog for GDPR and CCPA.

![Consent management dialog for CCPA](image3.png)

Figure 1a shows an example consent dialog displayed under GDPR, and Figure 1b shows an example consent dialog displayed under CCPA.

2.3 Header bidding

Header bidding [24] is a strategy in which websites, known as publishers, allocate various advertising slots for advertisers. The advertiser with the most competitive bid wins the opportunity to showcase their ads within the relevant ad slots. In the context of client-side header bidding, users can conveniently view all the bids directly from their web browser. A prominent illustration of this approach is demonstrated by prebid.js [36]. We’ve identified the Alexa top 100k websites, encompassing those with advertisements (e.g., cnn.com) and those without (e.g., google.com), to verify their utilization of prebid.js. Our findings revealed that 5421 websites are employing prebid.js with the standard API label pbjs (Personalized custom API labels are also utilized within prebid.js, and these are excluded from our tally of detections.). This signifies that over 5% of websites continue to employ prebid.js.

In contrast, server-side header bidding involves conducting the bidding auction on the ad server instead of the user’s browser. Consequently, the bids from participating advertisers remain concealed from the web user’s perspective. Noteworthy instances of server-side header bidding include Google Open Bidding, Amazon TAM, and Prebid Server. Comparing to server-side header bidding, the client side header bidding has the following advantages:

1. Through header bidding, publishers retain the ability to select buyers via header bidding wrappers. Additionally, publishers have the authority to set the minimum price for each ad unit. Consequently, the entire auction process becomes visible and clear for both publishers and advertisers. However, such transparency is not as pronounced with server-side header bidding. While publishers still determine the floor price, they lack visibility into the buyers participating in the auction, resulting in a more concealed auction process.
The primary rationale for favoring client-side header bidding over server-side header bidding lies in auction management. Header bidding wrappers empower publishers to oversee and manage the auction. Publishers can add buyers, establish timeout configurations, and ensure simultaneous bid requests to all buyers using these wrappers. In contrast, server-side header bidding involves the server reaching out to buyers and initiating bid requests, hence the management is primarily executed by the server.

(3) Client-side header bidding enables advertisers to directly access ad units from publishers’ web pages using wrappers, thereby gaining access to user cookie data. This data can be further employed for targeted advertising. Conversely, server-side header bidding encounters limitations in cookie matching.

Since the server-side header bidding does not expose auction at the client side, we do not consider it in our measurements.

2.4 Statistical Analysis
To evaluate if there are significant differences in advertisers bidding behavior when users opt-out under GDPR and CCPA, we conduct Mann-Whitney U test of statistical significance [57]. Mann-Whitney U test is a nonparametric test to compare the differences between two distributions. Since we perform multiple comparisons, i.e., compare bid values for all 16 personas, we also conduct Bonferroni correction on the statistical test. Our null hypothesis is that the bid distributions for opt-in and opt-out are similar to each other. We reject the null hypothesis, when the p-value (after correction, i.e., original value multiplied by 16) is less than 0.05 (reflecting a 95% confidence interval), i.e., the distributions are statistically different. We also measure the magnitude of the difference between bid values by calculating the effect size [57]. Effect size less than 0.3, between 0.3 and 0.5, and greater than 0.5 is considered small, medium, and large, respectively. Effect sizes are reported only in cases where statistically significant differences are observed. In instances where no bids are accumulated under either opt-out or opt-in conditions, the calculation of p-value and effect size becomes unfeasible, as these measures necessitate two datasets for meaningful comparison.

2.5 Related Work
Prior research has identified that online services design unintuitive and hard to navigate data access interfaces [51, 66], trick users into giving positive consent [75], and do not include controls to opt-out of data selling [88]. Alizadeh et al. [51] conducted a user study to understand data rights under GDPR and identified that the participants find data access interfaces unintuitive and hard to navigate. Specifically, users prefer structured and easy-to-navigate data usage reports in contrast to data dumps, that are hard to explore. Habib et al. [51] conducted a measurement study of 150 websites and identified that the privacy controls were hard to locate on the majority of websites. Furthermore, in several instances, links to privacy control did not lead to stated choices. Matte et al. [75] investigated CMPs and identified that the consent is often incorrectly conveyed. Specifically, websites often register consent before the user has made any choice, register positive consent regardless of user’s choice, or nudge users to give pre-selected positive consent. Urban et al. [86] discovered that 93% of the examined websites included third-party elements originating from regions that potentially do not conform to the prevailing legal framework. More recently, Nortwick and Wilson [88], conducted a measurement study of top 500K English websites and identified that only 2% of the websites provided controls to users to opt-out of data selling, i.e., “Do Not Sell My Personal Information” (DNSMPI), under CCPA.

The study by Toth et al. [85] found that CMPs themselves may exhibit dark patterns and could track users’ data to some extent by investigating 10 consent services from 5 CMPs deployed on different blank websites. They also identified that default configurations of consent pop-ups often violate regulations and that their configuration options may lead to non-compliance. Recently, Nguyen et al. [78] studied the implementation of consent notices specifically on Android apps and identified that about 20% of these apps violate at least one GDPR consent. In the study conducted by Demir et al. [62], a thorough examination of 114 prior research papers on web measurement was undertaken. The findings revealed a significant trend, with the majority (72.6%) of these papers lacking a comprehensive inventory of the pages they had analyzed. This has substantial implications for experiment reproducibility, as it highlights a prevalent issue where the majority of experiments cannot be replicated in terms of the specific sites and pages that were studied.

Though negligence in obtaining consent and not providing easy-to-navigate opt-out controls raises doubts on online services’ seriousness in protecting users’ data and respecting their consent, it does not automatically imply non-compliance. Prior work, to the best of our knowledge, has not directly measured non-compliance through consent notices on traditional web browsers, especially for the cases where consent is properly conveyed to the online services. To bridge that gap, in our work, we set out to audit the usage and selling of personal user data, where the user has directed online services to cease the processing and selling of their data, and their consent is properly recorded by the CMPs.

2.6 Inferring Non-Compliance
Online services, including publishers, advertisers, and trackers, do not offer much transparency in the usage and sharing of collected data, which makes it challenging to directly assess non-compliance. Though prior work has not directly measured advertisers and trackers non-compliance, they have relied on side channel information to infer the usage and sharing of user data [53, 59, 71, 81, 83].

A series of studies [59, 81, 83] leaked user interest data, in controlled experiments, and leveraged advertisers bidding behavior as a side channel to infer the usage and sharing of user data. Especially in the study [81] the author mentioned that the prices for profiles “Only category” are about 40% higher than those for “New user”. Their main insight is that the advertisers bidding behavior is shaped by their pre-existing knowledge of the user, which typically results in higher bid values, as compared to bid values for users for which advertisers do not have knowledge. Specifically, higher bids made by the advertiser to which the data was leaked indicates the usage of the leaked data for ad targeting. Whereas, higher bids from the advertiser to which data was not leaked indicates the sharing of data from advertisers to which the data was leaked.
Data sharing is an essential component of online advertising ecosystem and it is baked into ad delivery protocols, such as RTB [41] and HB [24] protocols. Prior work [64, 82] has identified that advertisers and trackers use ad delivery protocols, to directly share user data with each other at the client side, e.g., by cookie syncing [46]. Thus, client side data sharing can be directly inferred by analyzing network requests (e.g., redirects), between advertising and tracking services.

We argue that analyzing advertisers bidding behavior and network traffic should suffice in establishing whether advertisers comply with the user consent, when they opt-out of processing and selling of their data under GDPR and CCPA. Thus, in this study, we leverage advertisers bidding behavior and network traffic to audit regulatory compliance of advertisers under GDPR and CCPA.

3 METHODOLOGY
In this section, we describe our framework to audit advertising and tracking services under GDPR and CCPA. At a high level, we simulate synthetic user personas (profiles) with specific interests, intentionally leak those interests to advertisers and trackers, opt-out of processing and selling of user data, and analyze advertisers bidding behavior and network traffic to infer the usage and selling of leaked data. Figure 2 gives an overview of our approach.

3.1 Pre-Conditions: Crawling Under GDPR & CCPA

3.1.1 Web Crawling. We rely on OpenWPM [64] to set up our auditing framework. OpenWPM is a widely used Firefox-based, open-source web measurement tool that has been used in numerous research studies [34]. OpenWPM by default provides functionality to automatically visit websites and capture network requests, among other things. To adapt to our needs, we further extend OpenWPM to automatically opt-out of processing and selling of user data, and to capture advertisers bids on ad slots. In the opt-out process, we perform either the JavaScript opt-out event activation or engage the opt-out button provided by the CMP. We describe comprehensive information in Section 3.3.1. The JavaScript opt-out function is accomplished using a browser extension, while the opt-out button is clicked through the utilization of Selenium. It’s worth noting that OpenWPM employs Selenium for browser handling, allowing functions compatible with Selenium to also function within OpenWPM. Throughout the phase of recording advertisers’ bidding behaviors, the getBidResponse method, supported by prebid.js, is employed.

3.1.2 Simulating Measurements under GDPR & CCPA. We conduct our measurements from EU and California to audit third-party compliance under both GDPR and CCPA. We choose Frankfurt (Germany) and Northern California as representative jurisdictions under GDPR and CCPA, respectively. We rely on Amazon EC2 to simulate web crawls through the respective locations. We setup a new EC2 node, i.e., with a unique IP address, for each OpenWPM instance.

3.2 Simulating User Interest Personas
Recognizing the distinct bidding patterns exhibited by advertisers based on varying user interests, we undertake the simulation of 16 unique user interest personas. These personas are shaped by the categories of the top 16 Alexa-listed websites [4]. Notably, our selection approach compensates for Alexa’s shift in offerings after September 2020 [3]. The method of persona simulation involves initializing a fresh browser profile within an OpenWPM instance. This occurs on a pristine EC2 node, each furnished with an exclusive IP address. The process entails iterative visits to the top 50 websites within each category, with the browser profile being updated following each visit. Importantly, it is pertinent to highlight that our interactions were limited to the main pages of these websites. Our rationale for crafting these simulated personas rests upon their potential to persuade advertisers and trackers regarding the interests of each persona. The goal is to incentivize advertisers to submit higher bids when tailoring personalized ads for each persona. Inclusive of the aforementioned 16 personas, our study also introduces a control persona, represented by an empty browser profile. This control persona functions as a benchmark, facilitating the measurement of disparities in bidding behavior across personas. Noteworthy measures undertaken in our methodology encompass the activation of OpenWPM’s bot mitigation features and the introduction of random delays ranging between 10 to 30 seconds subsequent to loading each website. These steps serve to enhance the authenticity of user behavior emulation.

We deployed a total of 34 instances: 17 in Germany (16 personas + 1 Control) using 17 different IPs, and 17 in California (16 personas + 1 Control) using 17 different IPs.

We automated the loading of selected web pages and simulated various user interactions, including mouse movements and scrolls, with random time gaps between actions. The mouse cursor is moved...
We shortlist websites that support opt-out through CMPs and also implement header bidding through prebid.js. We identify such websites, by crawling Alexa top-100K websites, using OpenWPM, and probing for the presence of CMPs and prebid.js (as described in Section 3.3.1 and 3.4.2).

Table 1 lists the presence of CMPs and prebid.js on Alexa top-100K websites. We note that a large number of websites deploy CMPs but not all of them deploy prebid.js. However, scanning top-100K websites allows us to filter a meaningful number (i.e., 352) of websites that deploy CMPs and prebid.js under both GDPR and CCPA.

3.3 Filtering Opt-Out and Header Bidding Supported Websites

Table 2: Number of 3rd party requests and cookies set during manual test on 4 CMPs: Cookiebot, Didomi, Onetrust and Cookiebot. Column "3rd R" represents the number of 3rd party HTTP requests, and column "3rd C" represents the number of 3rd party cookies.

| CMP Tested Website | Cookiebot | Didomi | Onetrust | Quantcast |
|--------------------|-----------|--------|----------|-----------|
|                     | 3rd R     | 3rd C  | 3rd R    | 3rd R     |
| Before Choice       | 103       | 223    | 0        | 251       |
| Opt-in              | 210       | 648    | 10       | 21        |
| Refresh after Opt-in| 537       | 64      | 3        | 159       |
| Opt-out             | 161       | 18     | 0        | 8         |
| Refresh after Opt-out| 112      | 208    | 0        | 171       |

Table 3: CMP and prebid.js deployment on Alexa top-100K websites under GDPR and CCPA. +PB represents the count of websites for each CMP that also deploy prebid.js. Common websites column represents the count of websites that deploy both CMPs and prebid.js and are common across GDPR and CCPA.

| CMP        | GDPR count | +PB count | CCPA count | +PB count | Common websites |
|------------|------------|-----------|------------|-----------|----------------|
| Didomi     | 119        | 20        | 90         | 104       | 192            |
| Quantcast  | 2,543      | 234       | 2,875      | 94        | 77             |
| OneTrust   | 3,046      | 96        | 3,222      | 185       | 71             |
| Cookiebot  | 756        | 22        | 599        | 15        | 12             |
| Total      | 6,893      | 594       | 7,405      | 501       | 352            |
scripts that load prior to user consent. However, there is no available information pertaining to Quantcast. We conducted manual testing on all four CMPs using German IPs, calculating the quantity of HTTP requests generated by 3rd parties and the number of 3rd party cookies. Employing a Macbook device equipped with a Chrome browser, all data was monitored through Chrome DevTools. The exact counts of 3rd party HTTP requests and cookies are presented in Table 2, depicting the figures before consent is given, after consent is granted, or after consent is denied. From the standpoint of request and cookie numbers, it appears that Cookiebot, Didomi, and Quantcast prevent 3rd parties from setting trackers in cookies before user consent. Additionally, the number of requests is lower in the Opt-out scenario compared to Opt-in. Conversely, such a trend is not evident in the case of OneTrust. Notably, cookies from domains "googleleads.g.doubleclick.net" and "agead2.googlesyndication.com" consistently appear both before and after user consent or rejection.

Each of the four CMPs also establishes consent cookies following user decisions to either grant or deny consent. In the case of Cookiebot, a new cookie named "CookieConsent" is created once the user makes a choice regarding consent. Didomi employs two cookies, namely "didomi_token" and "euconsent-v2," to store consent-related information. OneTrust uses the "OptanonConsent" cookie to retain the user’s consent preference. In the context of Quantcast, three cookies are generated upon user consent: "euconsent-v2," "_pbjs_userid_consent_data," and "addtl_id_." If users opt to decline consent, only the "euconsent-v2" cookie is present. It’s important to note that all these cookies are designated as 1st party cookies and are not affiliated with the CMPs themselves.

3.4 Measuring Targeting on User Interest Personas

3.4.1 Measuring Targeting on Personas. Next, we measure targeting received by our personas to infer compliance (or lack thereof) under GDPR and CCPA. As mentioned earlier, we register negative user consent, i.e., opt-out of processing and selling of user data, through Didomi, Quantcast, OneTrust, and CookieBot and capture bids through prebid.js.

After filtering the websites, we iteratively visit each website nine times from each of our 16 (+ control) personas under both GDPR and CCPA. We visit the websites first time to opt-out of processing or selling of data and the next eight times to collect bids. Occasionally, the internet connection might experience instability, causing the browser to miss out on receiving bids. The quantity of bids received by the browser during distinct visits can also vary. It is unfeasible to ensure that the framework or a typical browser captures bids from all potential advertisers within a single visit. Therefore, we configured our framework to access the website on 8 occasions. The choice of the number 8 isn’t dictated by any particular rationale; rather, we opted for a relatively sizable number due to necessity. Specifically, additional factors, e.g., day/week and website popularity, may influence the bids [59, 81, 83]. In addition, we also use identical hardware/software, collect bids at the same time, from the same location, and on the same websites, across all personas. Overall, we expect that crawling websites several times and keeping conditions consistent will minimize the variability in bids.

3.4.2 Capturing Bidding by Advertisers. We treat advertisers bidding behavior as an indication of advertisers and trackers non-compliance with the user consent (as discussed in § 2.6). To this end, we audit advertisers and trackers on websites that support header bidding, more specifically prebid.js—a widely used implementation of header bidding protocol [25], primarily because header bidding occurs at the client side and allows us to intercept the bidding process [24]. Additional header bidding solutions such as Amazon Transparent Ad Marketplace and Google Ad Manager (GAM) featuring EBDA (Exchange Bidding Dynamic Allocation) operate through server-side mechanisms, preventing us from accessing bid data on the client side. Previously, Google offered a client-side header bidding service. Nevertheless, the current unavailability of the API googleTag.pubads().getBidsReceived() has impacted this functionality. To capture the bids, we first identify header bidding supported websites. We identify such websites by injecting a script on the webpage that probes the prebid.js version; if we receive a response, we consider the website as prebid.js supported website. Note that we do not consider personalized custom API labels (i.e., other than pbjs) in our measurements. After identification, we capture the bids by calling the getBidResponses method which returns the bids CPMs. In case, we do not get any bids, we request the bids ourselves by calling the requestBids method.

3.4.3 Capturing Cookie Syncing by Advertisers. Client side data sharing is a standard practice in the online advertising ecosystem. Advertisers most commonly share data through cookie syncing [65]. Specifically, advertisers read their cookies (or other identifiers) from the browser and embed them as redirects in the browser, which work with the redirected domain cookies. To capture the cookie syncing events, we monitor whether opt-outs, under GDPR and CCPA, prevent cookie syncing. To understand the impact of regulations, we also establish a baseline by opting in to the processing and selling of data. Our rationale for opting in is to get the upper bound on processing and selling of data, as inferred by advertisers bidding behavior. To opt-in, we enable all cookie controls mentioned in Section 3.3.1. For Didomi we call the Didomi.setUserAgreeToAll for OneTrust we call window. OneTrust.AllowAll, for CookieBot we click the opt-in button with id CybotCookiebotDialogBodyLevelButtonLevelOptinAlowAll, and for Quantcast we click the button with Accept or similar text.

3.4.4 Baseline Comparison with Opt-in. To understand the impact of regulations, we also establish a baseline by opting in to the processing and selling of data. Our rationale for opting in is to get the upper bound on processing and selling of data, as inferred by advertisers bidding behavior. To opt-in, we enable all cookie controls mentioned in Section 3.3.1. For Didomi we call

3 The bid values are expressed in CPM (cost per mille), which is the amount that an advertiser pays a website per one thousand visitors who see its advertisements.
the processing and selling of data. We opt-out of NAI’s offered controls by automatically navigating to their opt-out webpage [27] and by clicking OPT OUT OF ALL button. To evaluate advertisers offered controls, we select a different set of websites that support prebid.js but do not support CMPs. Specifically, we filter Alexa top-50 websites and identify 28 websites that support prebid.js but do not support any CMP’s under both GDPR and CCPA. It is important to select websites that do not support CMPs because otherwise we cannot distinguish between the impact of advertisers offered controls and state-enforced regulations.

4 RESULTS AND COMPREHENSIVES

ANALYSIS

In this section, we analyze advertisers compliance when users opt-out of data processing and selling. We compare and contrast targeting by advertisers across personas and configurations, make statistical observations, and draw conclusions from those observations about advertisers’ compliance under GDPR and CCPA. We present our findings at the granularity of individual CMP because some CMP’s might better handle user consent than the others. We measure advertisers compliance as follows:

(1) **Data usage.** Opting out should lead to lower bid values, in interest personas as compared to the control, from advertisers. If advertisers continue to bid higher, they may still be using user data when users opt out of data processing and selling.

(2) **Server-side data sharing.** Opting out should lead to lower bid values, in interest personas as compared to the control, from advertisers to whom data is not directly leaked. If advertisers to which data is not leaked bid higher, advertisers might still be sharing data when users opt out of data processing and selling.

(3) **Client-side data sharing.** Opting out should eliminate or significantly reduce cookie syncing events, in interest personas as compared to the control, from advertisers. If advertisers continue to sync cookie with each other, they may be sharing/selling user data when users opt out of data processing and selling.

As the steps of analysis in each CMP and NAI are similar, we only listed Cookiebot in this section, put the rest in Appendix A, and only remain the takeaway of each CMP and NAI except Cookiebot.

4.1 Cookiebot

**Data usage.** We evaluate reduction in data usage by analyzing advertisers bidding behavior. Table 3 presents advertisers bidding on personas when users opt-out and opt-in through Cookiebot under GDPR and CCPA. We note that all personas, with the exception of the Shopping where the bid value is same as the control under CCPA, receive higher bids as compared to the control persona. Even in the case of Shopping persona, the bid value is only 0.01 less than the control.

| Persona | GDPR | CCPA |
|---------|------|------|
| Avg. | Out | In | Avg. | Out | In |
| Adult | 0.37 | 0.33 | 1.85 | 0.08 | 0.37 | 0.34 | 2.64 | 0.06 |
| Arts | 0.35 | 0.32 | 2.65 | 0.06 | 0.38 | 0.31 | 6.64 | 0.11 |
| Business | 0.35 | 0.35 | 7.52 | 2E-03 | 0.36 | 0.32 | 3.08 | 0.06 |
| Computers | 0.35 | 0.36 | 3.71 | 0.05 | 0.37 | 0.30 | 0.51 | 0.12 |
| Games | 0.38 | 0.38 | 7.42 | 0.01 | 0.36 | 0.32 | 1.14 | 0.15 |
| Health | 0.35 | 0.34 | 6.38 | 0.02 | 0.38 | 0.38 | 5.36 | 0.03 |
| Home | 0.38 | 0.31 | 0.75 | 0.11 | 0.36 | 0.34 | 4.53 | 0.04 |
| Kids | 0.37 | 0.34 | 2.33 | 0.07 | 0.35 | 0.29 | 0.32 | 0.13 |
| News | 0.35 | 0.39 | 2.31 | 0.07 | 0.37 | 0.33 | 2.12 | 0.07 |
| Recreation | 0.37 | 0.35 | 4.43 | 0.04 | 0.36 | 0.31 | 1.71 | 0.08 |
| Reference | 0.37 | 0.33 | 1.50 | 0.08 | 0.37 | 0.32 | 0.89 | 0.10 |
| Regional | 0.38 | 0.34 | 2.34 | 0.07 | 0.35 | 0.30 | 0.93 | 0.10 |
| Science | 0.35 | 0.39 | 1.48 | 0.09 | 0.36 | 0.32 | 2.22 | 0.07 |
| Shopping | 0.37 | 0.35 | 7.33 | 0.01 | 0.32 | 0.32 | 5.08 | 0.03 |
| Sports | 0.37 | 0.37 | 7.91 | 1E-03 | 0.37 | 0.33 | 1.31 | 0.09 |

Table 3: Ad bidding under GDPR and CCPA after opt-out (Out) and opt-in (In) with Cookiebot. Avg. column represents the mean of all bid value, Std. indicates bid standard deviation. Light blue and dark blue indicate the bid value is lower than the control’s avg., respectively. Dark red and dark blue indicate bid values that are the control’s avg. ± std., respectively. Column p-val. and Eff. represent p-value and effect size, respectively.

**Client-side data sharing.** We evaluate reduction in client-side data sharing by measuring advertiser cookie syncing in network traffic. Table 4 presents advertiser cookie syncing behavior. Under GDPR, we note that there is substantial difference between advertisers cookie syncing behavior for opt-out and opt-in. Specifically, we only experience cookie syncing events in one persona (i.e., News) when we opt-out but we experience substantial more cookie syncing when we opt-in. Under CCPA, however, advertisers engage in cookie.

| Persona | GDPR | CCPA |
|---------|------|------|
| Avg. | Out | C-Sync | Avg. | Out | C-Sync |
| Adult | 0.37 | 0.25 | 0.37 | 0.14 |
| Arts | 0.35 | 0.7 | 0.37 | 4.3 |
| Business | 0.35 | 0.44 | 0.37 | 3.3 |
| Computers | 0.35 | 0.28 | 0.37 | 4.4 |
| Games | 0.38 | 0.27 | 0.36 | 0.4 |
| Health | 0.35 | 0.36 | 0.37 | 28.25 |
| Home | 0.38 | 0.36 | 0.36 | 14.4 |
| Kids | 0.37 | 0.41 | 0.36 | 5.26 |
| News | 0.35 | 3.22 | 0.37 | 3.3 |
| Recreation | 0.37 | 0.4 | 0.36 | 21.13 |
| Reference | 0.37 | 0.24 | 0.37 | 14.5 |
| Regional | 0.38 | 0.52 | 0.36 | 28.16 |
| Science | 0.35 | 0.26 | 0.37 | 29.18 |
| Shopping | 0.37 | 0.5 | 0.37 | 12.17 |
| Society | 0.37 | 0.5 | 0.37 | 5.7 |
| Sports | 0.37 | 0.43 | 0.33 | 5.7 |

Control | 0.33 | 0.20 | 0.32 | 0.30 | 0.50 | 0.01 |

Table 4: Ad bidding and cookie syncing under GDPR and CCPA after opt-out (Out) and opt-in (In) with Cookiebot. Avg. column represents the mean of all bid value from advertisers who did not bid or appear when we simulated personas but appeared and bid after we opt-out. Out and In under C-Sync. represent number of cookie syncing events after opt-out and opt-in, respectively.
Table 5: Most prevalent advertisers that participate in cookie syncing, when we opt-out under GDPR and CCPA. These advertiser appear in all personas across CookieBot, Didomi, Onetrust, Quantcast and NAI configurations. CB, DM, OT, QC and NAI columns represent the count of cookie syncing events under CookieBot, Didomi, Onetrust, Quantcast and NAI for each advertiser.

| Advertisers | Cookiebot | Didomi | GDPR | OneTrust | Quantcast | NAI | Cookiebot | Didomi | CCPA | OneTrust | Quantcast | NAI | Total |
|-------------|-----------|--------|-------|----------|-----------|-----|-----------|--------|------|----------|-----------|-----|-------|
| PubMatic    | 0         | 23     | 91    | 76       | 39        | 51  | 0         | 23     | 51   | 39       | 76        | 39  | 1522  |
| AT&T        | 3         | 12     | 24    | 51       | 36        | 51  | 0         | 12     | 36   | 51       | 24        | 51  | 918   |
| VerizonMedia| 0         | 0      | 0     | 0        | 0         | 0   | 0         | 0      | 0    | 0        | 0         | 0   | 0     |
| RichAudience| 0         | 0      | 0     | 0        | 0         | 0   | 0         | 0      | 0    | 0        | 0         | 0   | 0     |
| GumGum      | 0         | 0      | 0     | 0        | 0         | 0   | 0         | 0      | 0    | 0        | 0         | 0   | 0     |

Table 6: Most prevalent advertisers that participate in cookie syncing, when we opt-in under GDPR and CCPA. These advertiser appear in all personas across CookieBot, Didomi, Onetrust, Quantcast and NAI configurations. CB, DM, OT, QC and NAI columns represent the count of cookie syncing events under CookieBot, Didomi, Onetrust, Quantcast and NAI for each advertiser.

| Advertisers  | Cookiebot | Didomi | GDPR | OneTrust | Quantcast | NAI | Cookiebot | Didomi | CCPA | OneTrust | Quantcast | NAI | Total |
|--------------|-----------|--------|-------|----------|-----------|-----|-----------|--------|------|----------|-----------|-----|-------|
| PubMatic     | 325       | 375    | 131   | 294      | 95        | 1522| 125       | 353    | 365  | 323      | 255       | 2641|       |
| AT&T         | 27        | 624    | 94    | 350      | 0         | 2596| 22        | 575    | 332  | 405      | 167       | 2596|       |
| VerizonMedia | 0         | 725    | 20    | 228      | 2         | 2513| 8         | 559    | 412  | 425      | 134       | 2513|       |
| RubiconProject| 20       | 651    | 17    | 422      | 0         | 1838| 0         | 470    | 36   | 162      | 60        | 1838|       |
| RichAudience | 0         | 221    | 0     | 224      | 0         | 960 | 0         | 224    | 67   | 212      | 25        | 960 |       |

syncing events on 12 personas when we opt-out and all 16 personas when we opt-in. The total number of cookie syncing events on average in both opt-out and opt-in remains the same.

We further investigate cookie syncing frequency of individual advertisers. Table 5 presents the top 5 most prevalent advertisers that participate in cookie syncing, when we opt-out under both GDPR and CCPA. It can be seen from the table that advertisers participate in as many as 3 and 128 cookie syncing events when we opt-out under GDPR and CCPA with Cookiebot, respectively. **Takeaway.** The effectiveness of opt-out under CCPA appears limited, with average bids comparable between opt-out and opt-in across all 16 personas settings. Additionally, the syncing events in opt-out are not significantly fewer than in opt-in for most personas settings. Conversely, under GDPR, bid differences between opt-out and opt-in suggest opt-out might not be effective. Nonetheless, the number of syncing events is consistently lower in opt-out than in opt-in, indicating its effectiveness. This means both GDPR and CCPA compliance may not be ensured on the same websites.

4.2 Didomi, Onetrust, Quantcast and NAI

For Didomi, Onetrust, Quantcast and NAI, we did similar client-side data sharing analysis and server-side data sharing analysis, as what we did for Cookiebot. The comprehensive analysis details can be found in Appendix A.

In Didomi, significant decreases in data utilization and sharing are observed when users choose to opt-out under the guidelines of GDPR and CCPA. The decline in data usage is more pronounced under CCPA than under GDPR. Conversely, the decrease in client-side data sharing is more prominent under GDPR compared to CCPA. While the utilization of Didomi for obtaining consent noticeably minimizes targeted activities, it does not entirely eradicate them. This is evident in the continued heightened bidding for certain user profiles and the involvement of advertisements in cookie synchronization. Consequently, achieving GDPR compliance might be feasible through Didomi, but ensuring CCPA compliance might not be guaranteed for the same set of websites.

In OneTrust, differences in advertiser behavior between GDPR and CCPA were observed when users opted out. Specifically, opting out did not result in a statistically significant difference in data usage under GDPR, but it did under CCPA. The prevalence of both server-side and client-side data sharing was higher under CCPA compared to GDPR. Surprisingly, advertisers synchronized more cookies (meaning they shared more data on the client side) under CCPA compared to GDPR. This implies that compliance with GDPR and CCPA might not be guaranteed on the same websites.

In Quantcast, significant decreases in data usage and sharing aren’t observed when users choose to opt-out. Advertiser bidding behavior undergoes notable changes for 5 user personas under GDPR, albeit with a minor impact. When users opt-in under GDPR, there’s a noticeable increase in cookie syncing events. This suggests that ensuring compliance with both GDPR and CCPA might not be assured on identical websites.

In NAI, the utilization of advertisers’ data remains relatively stable. Nevertheless, advertisers tend to offer lower bids under CCPA compared to GDPR. Likewise, we have observed a marked decrease in data sharing, both on the server-side and client-side, under CCPA. As a result, it is possible that websites might not be concurrently compliant with both GDPR and CCPA regulations.

In the majority of cases within four CMPs and NAI, compliance with GDPR and CCPA regulations is lacking. There is little distinction in bids between opt-out and opt-in scenarios, and the volume of syncing events remains comparable regardless of opt-out or opt-in choices. It is plausible that some advertisers adhered to GDPR and CCPA regulations, and the CMP or NAI systems effectively functioned. Nonetheless, these advertisers were not extensively involved in most bidding events and cookie syncing occurrences. To validate this presumption, our focus shifted to advertisers, and a more extensive analysis is presented in Section 4.4.
4.3 Advertisers Bidding Behavior with pre-opt-out
Under GDPR processing personal data is prohibited, unless the data subject has consented to the processing (Article 6). However, under CCPA, data selling and sharing should be stopped immediately when users opt-out of being tracked. Thus, to eliminate the impact of data collection and sharing prior to opting-out, we conduct additional experiments where we opt out prior to simulating personas. Similar to post-opt-out, we note that under both GDPR and CCPA advertisers continue to use data even when we opt-out prior to collecting bids. We discuss advertisers bidding behavior with pre-opt-out in detail in Appendix B.

Table 7: Average of bids data from 6 advertisers in cookie syncing, when we opt-out and opt-in under GDPR. CB, DM, OT, QC and NAI columns represent the count of cookie syncing events under CookieBot, Didomi, Onetrust, Quantcast and NAI for each advertiser.

| Persons   | CB Out In Avg | DM Out In Avg | OT Out In Avg | QC Out In Avg | NAI Out In Avg |
|-----------|----------------|---------------|---------------|---------------|---------------|
| Adult     | 0.52           | 0.11          | 0.20          | 0.38          | 0.16          |
| Arts      | 0.43           | 0.13          | 0.22          | 0.35          | 0.14          |
| Business  | 0.34           | 0.12          | 0.21          | 0.32          | 0.13          |
| Computers | 0.25           | 0.10          | 0.19          | 0.28          | 0.12          |
| Home      | 0.15           | 0.06          | 0.15          | 0.24          | 0.10          |
| Kids      | 0.12           | 0.05          | 0.13          | 0.21          | 0.08          |
| News      | 0.10           | 0.04          | 0.12          | 0.20          | 0.06          |
| Recreation| 0.09           | 0.03          | 0.11          | 0.19          | 0.05          |
| Reference | 0.08           | 0.03          | 0.10          | 0.18          | 0.04          |
| Regional  | 0.07           | 0.02          | 0.09          | 0.17          | 0.03          |
| Science   | 0.06           | 0.02          | 0.08          | 0.16          | 0.02          |
| Shopping  | 0.05           | 0.02          | 0.06          | 0.14          | 0.02          |
| Society   | 0.04           | 0.02          | 0.05          | 0.13          | 0.02          |
| Sports    | 0.03           | 0.02          | 0.04          | 0.12          | 0.02          |

4.4 Advertisers across CMPs
4.4.1 Cookie Syncing Advertisers. We have compiled a list of the top five advertisers from a pool of 53, based on the highest number of syncing events during the Opt-out phase (Table 5). Additionally, we have tabulated the event counts during the Opt-in phase in Table 8.

Table 8: Average of bids data from 6 advertisers in cookie syncing, when we opt-out and opt-in under CCPA. CB, DM, OT, QC and NAI columns represent the count of cookie syncing events under CookieBot, Didomi, Onetrust, Quantcast and NAI for each advertiser.

| Persons   | CB Out In Avg | DM Out In Avg | OT Out In Avg | QC Out In Avg | NAI Out In Avg |
|-----------|----------------|---------------|---------------|---------------|---------------|
| Adult     | 0.33           | 0.11          | 0.20          | 0.38          | 0.16          |
| Arts      | 0.24           | 0.13          | 0.22          | 0.35          | 0.14          |
| Business  | 0.15           | 0.06          | 0.19          | 0.28          | 0.12          |
| Computers | 0.10           | 0.04          | 0.12          | 0.20          | 0.06          |
| Home      | 0.09           | 0.03          | 0.11          | 0.19          | 0.05          |
| Kids      | 0.08           | 0.02          | 0.09          | 0.17          | 0.03          |
| News      | 0.07           | 0.02          | 0.08          | 0.16          | 0.02          |
| Recreation| 0.06           | 0.02          | 0.08          | 0.15          | 0.02          |
| Reference | 0.05           | 0.02          | 0.07          | 0.15          | 0.02          |
| Regional  | 0.04           | 0.02          | 0.06          | 0.14          | 0.02          |
| Science   | 0.04           | 0.02          | 0.06          | 0.13          | 0.02          |
| Shopping  | 0.03           | 0.02          | 0.05          | 0.12          | 0.02          |
| Society   | 0.02           | 0.02          | 0.04          | 0.11          | 0.02          |
| Sports    | 0.02           | 0.02          | 0.04          | 0.10          | 0.02          |

6. A noticeable trend emerges: under GDPR regulations, CookieBot, Didomi, and Quantcast have effectively curbed a substantial number of syncing events. However, in the case of OneTrust, the disparity in the number of syncing events between Opt-out and Opt-in appears minimal. When considering CCPA, Didomi and NAI emerge as more successful than Cookiebot, OneTrust, and Quantcast in preventing syncing events. Nevertheless, it’s worth noting that the counts of syncing events originating from websites utilizing Didomi and NAI are already quite high during the Opt-out phase.

Takeaway. In terms of obstructing cookie syncing, CMPs exhibit superior performance under GDPR compared to CCPA. Notably, cookie events persist post Opt-out in CCPA scenarios. Among all CMPs, OneTrust shows the weakest performance, as the event counts between Opt-out and Opt-in remain comparable.

Table 9: Number of bids data from 6 advertisers in cookie syncing, when we opt-out and opt-in under GDPR. CB, DM, OT, QC and NAI columns represent the count of cookie syncing events under CookieBot, Didomi, Onetrust, Quantcast and NAI for each advertiser.

Table 10: Number of bids data from 6 advertisers in cookie syncing, when we opt-out and opt-in under CCPA. CB, DM, OT, QC and NAI columns represent the count of cookie syncing events under CookieBot, Didomi, Onetrust, Quantcast and NAI for each advertiser.
extracted bids data from these shared four advertisers and the two unique advertisers from each table. This data was then employed to compile Table 7 and Table 8. Notably, certain scenarios, such as the “Arts” persona under Cookiebot, exhibit significantly higher bid counts in Opt-out compared to Opt-in. To provide a comprehensive overview, we calculated the bid quantities under similar circumstances, as detailed in Table 9 and Table 10.

Under GDPR regulations, both CookieBot and Didomi show reduced bid counts in Opt-out compared to Opt-in, whereas the figures remain relatively consistent for OneTrust, Quantcast, and NAI. Furthermore, the averages between Opt-out and Opt-in exhibit similarity for OneTrust, Quantcast, and NAI. In the context of CCPA, more bids emerge in Opt-out compared to GDPR, accompanied by greater bid values. The trend in bid counts between Opt-out and Opt-in under CCPA resembles that observed under GDPR.

**Takeaway:** A comparative analysis between GDPR and CCPA reveals that all four CMPs and NAI demonstrate superior bid-blocking performance for the six selected advertisers under GDPR. A CMP-to-CMP comparison under GDPR reveals the superior performance of Cookiebot and Didomi compared to OneTrust, Quantcast, and NAI. Bid value and bid count patterns remain consistent between Opt-out and Opt-in for OneTrust, Quantcast, and NAI. When contrasting CMPs under CCPA, Cookiebot and Didomi still outperform OneTrust and Quantcast. Bid values and counts remain comparable between Opt-out and Opt-in for OneTrust, Quantcast, and NAI, with substantially higher values observed in Opt-out scenarios.

**Table 11: Average of bids data from advertisers in cookie syncing and not in cookie syncing under GDPR. CB, DM, OT, QC and NAI columns represent the count of cookie syncing events under Cookiebot, Didomi, Onetrust, Quantcast and NAI for each advertiser.**

| Persona | CB Sync Avg. | CB Not Avg. | DM Sync Avg. | DM Not Avg. | OT Sync Avg. | OT Not Avg. | QC Sync Avg. | QC Not Avg. | NAI Sync Avg. | NAI Not Avg. |
|---------|--------------|-------------|--------------|-------------|--------------|-------------|--------------|-------------|--------------|-------------|
| Adult   | –             | 0.37        | –             | 0.16        | –             | 0.19        | 0.32         | 0.00        | 0.44         | 0.14        |
| Arts    | 0.53         | 0.37        | 0.39         | 0.51        | 0.26         | 0.00        | 0.20         | 1.76        | 0.58         | 0.17        |
| Business| 0.21         | 0.37        | 0.16         | 0.20        | 0.10         | 0.00        | 0.42         | 1.51        | 0.28         | 0.16        |
| Computers| –           | 0.37       | 0.45         | –           | 0.18         | 0.00        | 0.26         | 1.87        | 0.64         | 0.18        |
| Games   | –             | 0.16        | 0.35         | 0.38        | 0.31         | 0.00        | 0.16         | 1.50        | 0.34         | 0.18        |
| Health  | 0.44         | 0.37        | 0.22         | 0.22        | 0.43         | 0.00        | 0.49         | 1.42        | 0.62         | 0.32        |
| Home    | 0.02         | 0.36        | 0.19         | 0.45        | 0.11         | 0.00        | 0.26         | 1.76        | 0.29         | 0.18        |
| Kids    | 0.03         | 0.36        | 0.21         | 0.03        | 0.17         | 0.00        | 0.46         | 1.95        | 0.35         | 0.15        |
| News    | 0.01         | 0.37        | 0.16         | 0.29        | 0.10         | 0.00        | 0.41         | 1.89        | 0.29         | 0.15        |
| Recreation| 0.14       | 0.36        | 0.13         | 0.53        | 0.09         | 0.00        | 0.49         | 1.55        | 0.47         | 0.16        |
| Reference| 0.52        | 0.37       | 0.17         | 0.22        | 0.09         | 0.00        | 0.35         | 1.86        | 0.31         | 0.17        |
| Regional| 0.03         | 0.36        | 0.22         | 0.27        | 0.37         | 0.05        | 0.36         | 1.41        | 0.38         | 0.16        |
| Science | 0.11         | 0.37        | 0.18         | 0.22        | 0.17         | 0.00        | 0.37         | 2.17        | 0.36         | 0.16        |
| Shopping| 0.39         | 0.31        | 0.19         | 0.26        | 0.20         | 0.00        | 0.40         | 1.89        | 0.31         | 0.17        |
| Society | 0.37         | 0.24        | 0.20         | 0.37        | 0.07         | 0.00        | 0.33         | 2.99        | 0.27         | 0.14        |
| Sports  | 0.32         | 0.13        | 0.17         | 0.18        | 0.26         | 0.00        | 0.23         | 1.64        | 0.54         | 0.34        |

**Table 12: Average of bids data from advertisers in cookie syncing and not in cookie syncing under CCPA. CB, DM, OT, QC and NAI columns represent the count of cookie syncing events under Cookiebot, Didomi, Onetrust, Quantcast and NAI for each advertiser.**

4.4.3 **Syncing versus Non-Syncing.** The subsequent analysis compares advertisers engaged in cookie syncing to those not involved, specifically focusing on Opt-out settings. The averages of bid values for both cookie syncing and non-participating advertisers under GDPR and CCPA are presented in Table 11 and Table 12. Additionally, Table 13 and Table 14 display the bid count originating from advertisers who either participated or did not participate in cookie syncing under both GDPR and CCPA regulations.

(1) In Cookiebot, bids from syncing advertisers are significantly fewer than those from non-syncing counterparts. Notably, for personas such as Arts, Health, Reference, and Shopping, the average bid from syncing advertisers surpasses that from non-syncing advertisers under CCPA. Remarkably, the bid count remains comparable between GDPR and CCPA scenarios.

(2) In Didomi, the number of bids is notably limited under GDPR. Conversely, under CCPA, an overwhelming majority of bids originate from syncing advertisers, with the average bid value showing parity between syncing and non-syncing participants.

(3) OneTrust showcases a trend where bids predominantly stem from non-syncing advertisers under both GDPR and CCPA, with a notable shift towards syncing advertisers under CCPA compared to GDPR. Additionally, the bid values from syncing advertisers considerably surpass those from non-syncing counterparts under both GDPR and CCPA.

(4) Quantcast exhibits a situation where nearly all bids arise from syncing advertisers under GDPR. Meanwhile, under CCPA, bids are sourced from both syncing and non-syncing advertisers, with syncing advertisers accounting for a larger share. Interestingly, under CCPA, the bid values from non-syncing advertisers are notably greater than those from syncing participants.

(5) For NAI, the bid count from non-syncing advertisers surpasses that from syncing advertisers. Remarkably, the bid count maintains similarity between GDPR and CCPA contexts. In the context of GDPR, syncing advertisers yield lower values compared to non-syncing ones, whereas the reverse trend is observed under CCPA. Syncing advertisers exhibit lower values under GDPR compared to CCPA, while non-syncing advertisers display the opposite trend.

**Takeaway:** All 4 CMPs have a very small amount of bids from advertisers which participated in cookie syncing under GDPR, except NAI. There are still bids from non-syncing advertisers in CookieBot and Onetrust under GDPR. There are more bids under CCPA, especially in Didomi(Syncing), Onetrust(Syncing), and Quantcast(Both Syncing and no-Syncing), except NAI. NAI has a similar number of bids under GDPR and CCPA. The bid value is higher under CCPA than under GDPR, except Cookiebot and NAI. Cookiebot has similar average bids from no-syncing under GDPR and CCPA. NAI has opposite value comparison trends between syncing advertisers and no-syncing ones under both GDPR and CCPA.
5 DISCUSSION & LIMITATIONS

5.1 Overall Trends Across CMPs

Overall we note that under CMPs most personas receive higher bids compared to control when users opt-out of data processing and selling under GDPR and CCPA. The variability in bid values, particularly higher bids as compared to control, indicates that the leaked user interests are used to target ads to users, despite users’ consent to opt-out of data processing as part of the regulations. We also note that opt-out is not statistically different from opt-in. The similarity in bid values for opt-in and opt-out indicates that the user consent in most cases does not have any effect on processing and selling of data. However some CMPs perform better than the others. For example, advertisers bidding behavior significantly changes under CCPA when the consent is conveyed through Didomi.

We note that advertisers participate in data sharing activities both at the server and the client side without user consent. At the server side, we received higher bid values from advertisers, who we did not explicitly leak user interests; which indicates potential selling and sharing from advertisers who leaked user data. At the client side, we notice that the advertisers share unique user identifiers in plain sight and share their data with as many other advertisers.

Advertiser-offered opt-out controls are also ineffective in curbing the processing and selling of user data despite user consent to opt-out. While advertisers at large do not honor their own opt-out controls, they slightly share less data as compared to the state-enforced regulations. The following is one example set of client-side data sharing.

Personas: Games, CMP: Onetrust, Location: California, Action: After Opt-out.

Example 1:

Current domain: https://d.agkn.com/pixel1t=7111?pid=130278&che=1660055860221&sk=20961080423800302664

Example 2:

Current domain: https://pixel.mathtag.com/syncimg?redir=https%3A%2F%2Fp%2F2Fx%2F2Features%2F3t3r%2F%3D375192%2Fpid%3D3D55B5MM%2FUID%3D5%3D

Example 3:

Current domain: https://image4.pubmatic.com/AdServer/SPug/?partnerID=161253&mpc=1&ppid=https%3A%2F%2Fmedia.grid.bidswitch.net%2Fsync%3Ftp_id%3D27%26tp_uid%3D3B55B7EA-493D-4230-AF83-29D023DAA37C

Shared data: tp_id=35912&pid=2239262f-6b26-4c09-9d4c-bf76b5b98c

5.2 Consent Handling by CMPs

At a high level, CMPs block or allow cookies to enforce user consent [10, 15]. As a first step, CMPs scan the website and identify all first and third-party cookies. After identifying the cookies, CMPs classify them into essential (i.e., necessary for websites to operate) and non-essential (e.g., advertising, tracking, marketing, etc.) cookies. To identify necessary cookies, CMPs rely on information from the website developers To identify non-essential cookies, CMPs classify it into essential and non-essential cookies. CMPs do not clearly disclose their techniques, but they might just be relying on information shared by advertising and tracking services about the purpose of their cookies (e.g., Google declares the purpose of their cookies [23]). Many CMPs, such as OneTrust and Cookiebot, consolidate the information across websites and maintain database of cookies and their purposes [10, 31]. Consolidating information allows CMPs to automatically identify essential and non-essential cookies on new websites.

CMPs typically take user consent and store it at the client side in first-party cookies. In addition to blocking cookies, CMPs also block execution of elements (e.g., scripts, iframes, videos, images) that might exfiltrate non-essential cookies before user consent is stored. To give website developers more control in order to accurately enforce user consent and avoid breakage by blocking essential cookies, CMPs allow website developers to block or allow cookies.
There are two main ways in which advertisers might be able to process and share user information despite negative consent. One, website developers may inaccurately deploy CMPs. For example, tracking code may execute first before CMPs even have a chance to block cookies; or website developers may inaccurately list non-essential cookies as essential. Two, advertisers may rely on side channel information to circumvent enforcement by CMPs. For example, advertisers may routinely change their cookies to avoid detection or they may rely on browser fingerprinting to track users [69]. Recently, Toth et al. [85] found that CMPs themselves may violate regulations and that their configuration options may lead to non-compliance.

5.3 Possible Recommendations

Our findings in general cast a serious doubt on the effectiveness of regulations as a sole means of privacy protection. Specifically, even after users opt-out through CMPs, their data may still be used and shared by advertiser. Unfortunately, in order to fully protect privacy, users still need to rely on privacy-enhancing tools, such as ad/tracker blocking browser extensions and privacy-focused browsers (e.g., Brave Browser). However, not all users may utilize privacy-enhancing tools to protect their privacy.

Website developers have an important role in enforcement of regulations. Specifically, they could deploy CMPs that are better at conveying and enforcing user consent. For example, research like ours could help inform the effectiveness of consent conveyance by different CMPs. Moving forward, we also recommended that CMPs, advertisers, website developers, and regulators should work together to define protocols for conveying and enforcing consent.

5.4 Limitations

Main page and subpages: In our experiment, the framework exclusively accessed the main pages of each training website. Discrepancies may arise between visits to main pages and the inclusion of subpages [52]. Our analysis indicates that opting out on testing websites does not prevent tracking when solely accessing their main pages. Our primary aim was to illustrate that opting out does not guarantee evasion of tracking. The possibility of training personas by exploring subpages of training websites remains a potential avenue for future exploration. Notably, the focus of visiting testing websites was to gather bid data, rather than persona training, which is why we limited our visits to main pages.

CCPA applicability criteria: CCPA applies to online services that meet its broad applicability criteria. Specifically, as per Section 1798.140 (c) (1), CCPA applies to online services, that have an annual revenue of more than $25 million, annually sell data of more than 50K California residents, or earn more than 50% of their revenue from the sale of personal data of California residents. Since most information required to determine applicability is not publicly available, it is challenging to determine the applicability criteria at scale [88]. Thus, for our study, we did not strictly follow the CCPA applicability criteria. However, it is noteworthy that the prevalent advertisers (Table 5) in our dataset are mostly large corporates with revenue exceeding hundreds of millions [38, 45].

Sample size: In comparison to prior work that analyzed ad bidding (e.g., Cook et al. [59] analyzed 25 websites), we analyze a substantially large number of websites (i.e., 352 that support Didomi, Quantcast, OneTrust, and CookieBot). We also repeat our measurements several times (i.e., 8 times) to reduce the chance of the sample size biasing our results. In future, researchers could further increase the sample size by incorporating websites that support various CMPs. We leave the non-trivial task of automating opt-outs from different CMPs at scale as future work. In future, researchers could also rely on alternative methodologies that use ad content e.g., [77], to eliminate the need to rely on ad bidding altogether for inference of data usage and sharing. Such techniques might allow researchers to audit online services at a much larger scale.

Server-side data sharing: We rely on the insight, also leveraged by prior research [53, 59], that the advertisers behavior is shaped by their pre-existing knowledge of the user. Using that insight, we make an inference that higher bids from advertisers to which data was not leaked indicates the sharing of data from advertisers to which the data was leaked. However, there may be other additional uncontrolled factors that might impact the bids.

Automated data collection: We rely on OpenWPM to automatically collect bids and use Amazon’s EC2 cloud platform to simulate crawls from Germany and California. In order to more accurately simulate real users, we enable hot mitigation in OpenWPM and also randomly wait between 10–30 seconds after loading each website. We also refrain from using public proxy servers, which may be black listed, and instead rely on Amazon EC2.

6 CONCLUSIONS

In this paper, we proposed a framework to audit regulatory compliance of online services at scale. We used the proposed framework to audit online advertising services on popular websites under GDPR and CCPA. Despite users exercising their rights under GDPR and CCPA to opt-out of processing and selling of their data using CMPs, we find that advertisers process user data to possibly target them and also share it with their partners both at the server and the client side. However, we find that some CMPs perform better than the others, i.e., advertisers bidding behavior significantly changes when the consent is conveyed. We also audited advertisers’ self-proposed opt-out controls, i.e., NAI’s opt-out, and found that they might be equally ineffective at curtailing processing and selling of user data. Overall, our measurements sadly indicate that the regulations may not protect user privacy, and advertisers might be in potential violation of GDPR and CCPA. To foster follow-up research, we will also release our code and data set at the time of publication.

ACKNOWLEDGMENTS

We would like to express our gratitude to the reviewers and the shepherd whose insightful comments and constructive feedback greatly contributed to the enhancement of this paper. The work of the second author is supported by the National Science Foundation under grant number CNS-2127369 (Computing Research Association for the CIFellows 2021 Project).

REFERENCES

[1] Adblock plus. https://adblockplus.org/.
[2] Adchoices. https://youradchoices.com/learn.
Table 15: Ad bidding under GDPR and CCPA after opt-out (Out) and opt-in (In) with Didomi. Avg. column represents the mean of all bid value. Gray and light blue indicate bid values that are higher and lower than Control’s avg., respectively. Dark red and Dark blue indicate bid values that are Control’s avg. ± std., respectively. Column p-val. and Eff. represent p-value and effect size, respectively.

| Persona | GDPR Out Avg. | GDPR In Avg. | Stat. Test | CCPA Out Avg. | CCPA In Avg. | Stat. Test |
|---------|----------------|---------------|------------|----------------|---------------|------------|
| Adult   | 0.11           | 0.17          | 7.3E-7     | 0.20           | 0.23          | 0.31       |
| Arts    | 0.05           | 0.18          | 6.3E-18    | 0.31           | 0.15          | 0.23       |
| Business| 0.11           | 0.19          | 3.9E-12    | 0.26           | 0.17          | 0.25       |
| Computers| 0.05          | 0.15          | 4.2E-17    | 0.29           | 0.13          | 0.25       |
| Games   | 0.05           | 0.16          | 3.4E-10    | 0.25           | 0.14          | 0.25       |
| Health  | 0.11           | 0.20          | 1.9E-11    | 0.23           | 0.17          | 0.23       |
| Home    | 0.05           | 0.23          | 9.2E-14    | 0.29           | 0.18          | 0.25       |
| Kids    | 0.14           | 0.18          | 2.2E-5     | 0.15           | 0.13          | 0.15       |
| News    | 0.09           | 0.17          | 4E-10      | 0.23           | 0.17          | 0.23       |
| Recreation| 0.06          | 0.16          | 3.9E-12    | 0.27           | 0.17          | 0.27       |
| Reference| 0.13           | 0.23          | 1.9E-12    | 0.37           | 0.18          | 0.37       |
| Science | 0.12           | 0.23          | 8.7E-14    | 0.27           | 0.18          | 0.27       |
| Shopping| 0.05           | 0.18          | 7.3E-10    | 0.25           | 0.15          | 0.25       |
| Society | 0.15           | 0.24          | 2.4E-12    | 0.26           | 0.18          | 0.26       |
| Sports  | 0.13           | 0.17          | 2.5E-12    | 0.23           | 0.17          | 0.23       |

Control 0.05 0.17 1.3E-20 0.33

Table 16: Ad bidding and cookie syncing under GDPR and CCPA after opt-out (Out) and opt-in (In) with Didomi. Avg. column represents the mean of all bid value from advertisers who did not bid or appear when we simulated personas but appeared and bid after we opt-out. Out and In under C-Sync. represent number of cookie syncing events after opt-out and opt-in, respectively.

| Persona | GDPR Out Avg. | GDPR C-Sync. Out | CCPA Out Avg. | CCPA C-Sync. Out |
|---------|----------------|------------------|---------------|------------------|
| Adult   | 0.12           | 36.13            | 0.12          | 36.13            |
| Arts    | 0.05           | 0.43             | 0.05          | 0.43             |
| Business| 0.15           | 0.12             | 0.15          | 0.12             |
| Computers| 0.05          | 0.19             | 0.05          | 0.19             |
| Games   | 0.05           | 0.16             | 0.05          | 0.16             |
| Health  | 0.15           | 0.17             | 0.15          | 0.17             |
| Home    | 0.05           | 0.18             | 0.05          | 0.18             |
| Kids    | 0.15           | 0.19             | 0.15          | 0.19             |
| News    | 0.05           | 0.16             | 0.05          | 0.16             |
| Recreation| 0.05          | 0.17             | 0.05          | 0.17             |
| Science | 0.15           | 0.18             | 0.15          | 0.18             |
| Shopping| 0.05           | 0.16             | 0.05          | 0.16             |
| Society | 0.05           | 0.17             | 0.05          | 0.17             |
| Sports  | 0.05           | 0.17             | 0.05          | 0.17             |

Control 0.05 0.18 0.42 0.17

[71] Mathias Lecuyer, Riley Sphun, Yannis Spiliopoulos, Augustin Chaintreau, Roxana Geambasu, and Daniel Hsu. Sunlight: Fine-grained targeting detection at scale with statistical confidence. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, 2015.
[72] Tom Lendacki. The platform for privacy preferences (p3p). https://www-archive.mozilla.org/projects/p3p.
[73] Pedro Giovanni Leon, Lorrie Faith Cranor, Alexecia M McDonald, and Robert McGuire. Token attempt the misrepresentation of website privacy policies through the misuse of p3p compact policy tokens. In Proceedings of the 9th Annual ACM Workshop on Privacy in the Electronic Society, 2010.
[74] Timothy Libert. An automated approach to auditing disclosure of third-party behavioral advertising ecosystem. In Privacy Enhancing Technologies Symposium, 2022.
[75] Rae Nadusen. When targeted ads feel a little too targeted. https://www.vox.com/the-goods/2020/4/9/21204425/targeted-ads-fertility-eating-disorder-coronavirus, 2020.
[76] The Office of the Attorney General. Cpa enforcement case examples. https://oag.ca.gov/privacy/cca/enforcement.
[77] Lakose Olejnik, Minh-Dung Tran, and Claude Castelluccia. Selling off privacy at auction. In Network and Distributed System Security Symposium (NDSS), 2014.
[78] Panagiotis Papadopoulos, Nicolas Kourtellis, and Evangelos P. Markatos. Cookie synchronization: Everything you always wanted to know but were afraid to ask. In The Web Conference (WWW), 2019.
[79] Rae Nadusen. When targeted ads feel a little too targeted. https://www.vox.com/the-goods/2020/4/9/21204425/targeted-ads-fertility-eating-disorder-coronavirus, 2020.
[80] Maaz Bin Musa and Rishab Nithyanand. Atom: A generalizable technique for inferring tracker-advertiser data sharing in the online behavioral advertising ecosystem. In Privacy Enhancing Technologies Symposium, 2022.
[81] Maggie Van Nortwick and Christo Wilson. Setting the bar low: Are websites complying with the minimum requirements of the ccpa? In Privacy Enhancing Technologies Symposium (PETS), 2022.
[82] Tobias Urban, Dennis Tatang, Martin Degeling, Thorsten Holz, and Norbert Pohlmann. Beyond the front page: Measuring third party dynamics in the field. In Proceedings of The Web Conference 2020, pages 1275–1286, 2020.
[83] Tobias Urban, Dennis Tatang, Martin Degeling, Thorsten Holz, and Norbert Pohlmann. A study on subject data access in online advertising after the gdpr. In Data Privacy Management, Cryptocurrencies and Blockchain Technology, Springer, 2019.
[84] John Wilander. Bounce tracking protection. https://github.com/privacycc/proposals/issues/6.

A ANALYSIS OF DIDOMI, ONETRUST, QUANTCAST AND NAI

A.1 Didomi

Data usage. We evaluate reduction in data usage by analyzing advertisers bidding behavior. Table 15 presents advertisers bidding on personas when users opt-out and opt-in through Didomi under GDPR and CCPA. We note that under GDPR, 3 personas bid higher than the control despite users opting out. In all 3 instances the bid values are even higher than the sum of average and standard deviation of bid values in control (i.e., 3E-3 std.), exceeding to as much as 8.2 times higher for the Science persona. However, it is important to note that other than the Science persona the differences for other personas is only 0.01. We also note that advertisers did not return any bids for 6 personas and in 2 personas the bid values are less than that of the control (with the difference of 0.02). Similarly, under CCPA, 7 personas bid higher than the control and for 2 personas, i.e., Arts and Computer, bid values are higher than the sum of average and standard deviation (i.e., 0.16). We also note that for 7 personas average bid value is less than that of the control, however, the difference is at most 0.03. Next, we analyze if there is statistically significant difference between advertisers bidding patterns when users opt-out or opt-in under GDPR and CCPA. It can be seen in Table 15 that under GDPR, advertisers bidding behavior does not significantly change when users opt-out, except for the personas where we did not receive any bidding. Under CCPA, advertisers bidding behavior significantly...
Table 17: Ad bidding under GDPR and CCPA after opt-out (Out) and opt-in (In) with OneTrust. Avg. column represents the mean of all bid value. Light blue and Dark blue indicate bid values that are higher and lower than Control’s avg., respectively. Dark red and Dark blue indicate bid values that are Control’s avg. ± std., respectively. Column p-val. and Eff. represent p-value and effect size, respectively.

| Persona | GDPR | CCPA |
|---------|------|------|
|         | Out Avg. | In Avg. | Stat. Test | Out Avg. | In Avg. | Stat. Test |
| Adult   | 0.02 | 0.01 | 8.00 | 0 | 1.09 | 0.46 | 2.3E-6 | 0.35 |
| Arts    | 0.04 | 0.03 | 5.00 | 0 | 0.99 | 0.81 | 0.47 | 0.11 |
| Business | 0.01 | 0.06 | 0.28 | 0.42 | 0.04 | 0.19 | 5.3E-11 | 0.50 |
| Computers | 0.02 | 0.01 | 2.01 | 0.28 | 1.02 | 1.40 | 4.50 | 0.05 |
| Games   | 0.02 | 0.03 | 5.00 | 0 | 0.99 | 0.81 | 0.47 | 0.11 |
| Health  | 0.03 | 0.15 | 0.11 | 0.78 | 0.98 | 0.70 | 7.7E-6 | 0.31 |
| Home    | 0.34 | 0.05 | 2.52 | 0.37 | 1.03 | 1.61 | 2.23 | 0.10 |
| Kids    | 0.02 | 0.02 | 0.62 | 0.44 | 0.91 | 0.66 | 1.2E-4 | 0.23 |
| News    | 0.04 | 0.02 | 0.32 | 0.64 | 0.95 | 0.73 | 0.66 | 0.10 |
| Recreation | 0.02 | 0.14 | 0.02 | 0.83 | 1.03 | 0.46 | 1.8E-11 | 0.39 |
| Reference | 0.20 | 0.07 | 0.31 | 0.31 | 1.10 | 0.72 | 3.7E-5 | 0.27 |
| Regional | 0.02 | 0.02 | 2.43 | 0.24 | 0.91 | 0.35 | 4.6E-11 | 0.39 |
| Science | 0.03 | 0.09 | 1.75 | 0.42 | 1.05 | 0.68 | 0.16 | 0.17 |
| Shopping | 1.20 | 0.13 | 3.84 | 0.35 | 1.00 | 0.77 | 0.37 | 0.10 |
| Society | 0.02 | 0.02 | 2.23 | 0.25 | 0.85 | 0.20 | 1.8E-5 | 0.37 |
| Sports  | 0.01 | 0.01 | 0.16 | 0.47 | 0.94 | 0.77 | 0.61 | 0.10 |
| Control | 0.02 | 0.02 | 8.00 | 0 | 0.88 | 0.69 | 1.94 | 0.09 |

Table 18: Ad bidding and cookie syncing under GDPR and CCPA after opt-out (Out) and opt-in (In) with OneTrust. Avg. column represents the mean of all bid value from advertisers who did not bid or appear when we simulated personas but appeared and bid after we opt-out. Out and In under C-Sync. represent number of cookie syncing events after opt-out and opt-in, respectively.

| Persona | GDPR | CCPA |
|---------|------|------|
|         | Out Avg. | C-Sync. | Out Avg. | C-Sync. |
| Adult   | 0.02 | 0.02 | 19 | 20 | 3.64 | 85 | 128 |
| Arts    | 0.04 | 0.03 | 29 | 34 | 1.78 | 86 | 112 |
| Business | 0.01 | 0.02 | 50 | 56 | 1.37 | 115 | 120 |
| Computers | 0.02 | 0.02 | 15 | 17 | 1.80 | 110 | 106 |
| Games   | 0.02 | 0.02 | 16 | 22 | 1.56 | 95 | 58 |
| Health  | 0.03 | 0.03 | 15 | 25 | 1.37 | 115 | 120 |
| Home    | 0.34 | 0.05 | 8 | 15 | 1.63 | 110 | 106 |
| Kids    | 0.02 | 0.02 | 12 | 27 | 1.95 | 124 | 116 |
| News    | 0.02 | 0.02 | 8 | 27 | 1.76 | 98 | 47 |
| Recreation | 0.02 | 0.02 | 13 | 13 | 1.35 | 86 | 77 |
| Reference | 0.03 | 0.03 | 11 | 15 | 1.86 | 67 | 89 |
| Regional | 0.02 | 0.02 | 13 | 36 | 1.36 | 85 | 53 |
| Science | 0.03 | 0.03 | 1 | 1 | 2.92 | 114 | 106 |
| Shopping | 1.10 | 1.10 | 14 | 14 | 1.77 | 136 | 76 |
| Society | 0.04 | 0.04 | 10 | 23 | 1.83 | 89 | 87 |
| Sports  | 0.02 | 0.02 | 20 | 54 | 1.51 | 74 | 57 |
| Control | 0.02 | 0.02 | 8.00 | 0 | 0.88 | 0.88 | 88 | 88 |

Changes when users opt-in to data processing and sharing. However, we note that the difference in advertisers behavior is small, i.e., effect size is less than 0.3, except for Arts and Regional personas where the effect size is medium.

Server-side data sharing. We evaluate reduction in server-side data sharing by analyzing bidding from advertisers to which we do not leak data. Table 16 presents bids from advertisers to which we did not explicitly leak user data. Under GDPR, 3 personas bid higher than the control and 2 personas bid less than the control. However, the difference in bid values is less than 0.02, except for Science where it is 8 times higher than the control. Under CCPA, 6 personas bid higher and 8 personas bid less than the control. For two personas i.e., Arts and Computers the bid values are 2.5 times higher than the control and for Kids persona the bid value is 4.5 times less than the control.

Client-side data sharing. We evaluate reduction in client-side data sharing by measuring cookie syncing by advertisers in network traffic. Table 16 presents the cookie syncing participation of advertisers. Under GDPR, we note that there is difference between advertisers cookie syncing behavior for opt-out and opt-in. Specifically, we experience cookie syncing events in 6 personas when we opt-out but we experience substantial more cookie syncing when we opt-in. On average there are 3 and 223 cookie syncing events per persona when users opt-out and opt-in, respectively. Under CCPA, advertisers engage in cookie syncing events on all 16 personas regardless of whether the user opts-out or opts-in. However, number of cookie syncing events substantially increases from 42 to 170 when users opt-out.

We further investigate cookie syncing frequency of individual advertisers. It can be seen from Table 5 that advertisers participate in as many as 31 and 211 cookie syncing events when we opt-out under GDPR and CCPA with Didomi, respectively.

Takeaway. Significant decreases in data utilization and sharing are observed when users choose to opt-out under both GDPR and CCPA regulations. The decline in data usage is more pronounced under CCPA in comparison to GDPR. Conversely, the decline in client-side data sharing is more notable under GDPR than CCPA. Despite the utilization of Didomi for obtaining consent, which notably curbs targeting, it doesn’t entirely eradicate it. This is evidenced by the continued higher bids on certain user personas and the involvement of advertising in cookie synchronization. Consequently, while achieving GDPR compliance might be possible through Didomi, ensuring CCPA compliance on the same websites could be more challenging.

A.2 OneTrust

Data usage. We evaluate reduction in data usage by analyzing advertisers bidding behavior. Table 17 presents advertisers bidding on personas when users opt-out and opt-in through OneTrust under GDPR and CCPA. We note that under GDPR, 6 personas bid higher than control and 5 personas bid lower than control. Except for Home and Shopping personas where bid values substantially exceed when users opt-out, the difference between bid values as compared to the control is only 0.01. We also note that advertisers did not return any bids for the arts persona. In contrast, under CCPA, except for 2 personas, i.e., Business and Society, 14 personas receive bid values that are higher than that of the control.

Next, we analyze if there is statistically significant difference between advertisers bidding patterns when users opt-out or opt-in under GDPR and CCPA. It can be seen in Table 17 that under GDPR, for all personas, with the exception of Recreation persona, there is no statistically significant difference between advertisers bidding behavior. Under CCPA, for 8 personas here is no statistically significant difference between advertisers bidding behavior. For the other 8 personas, however, advertisers have statistically significant different advertising behavior (with medium effect size for 6 personas).

Server-side data sharing. We evaluate reduction in server-side data sharing by analyzing bidding from advertisers to which we do not leak data. Table 18 presents bids from advertisers to which we
Table 19: Ad bidding under GDPR and CCPA after opt-out (Out) and opt-in (In) with Quantcast. Avg. column represents the mean of all bid value. Light blue and Dark blue indicate bid values that are higher and lower than Control’s avg., respectively. Dark red and Dark blue indicate bid values that are Control’s avg. ± std., respectively. Column p-val. and Eff. represent p-value and effect size, respectively.

| Persona     | GDPR Out Avg. | GDPR In Avg. | CCPA Out Avg. | CCPA In Avg. | p-val. | Eff. |
|-------------|----------------|--------------|---------------|--------------|--------|------|
| Adult       | 0.22           | 0.15         | 0.25          | 0.16         | 0.01   | 0.12 |
| Arts        | 0.22           | 0.14         | 0.27          | 0.07         | 0.18   | 0.04 |
| Business    | 0.19           | 0.15         | 0.20          | 0.13         | 0.18   | 0.04 |
| Computers   | 0.28           | 0.16         | 0.31          | 0.06         | 0.48   | 0.02 |
| Games       | 0.46           | 0.34         | 0.25          | 0.09         | 0.21   | 0.01 |
| Health      | 0.41           | 0.15         | 0.31          | 0.04         | 0.38   | 0.01 |
| Home        | 0.25           | 0.14         | 0.21          | 0.02         | 0.06   | 0.09 |
| Kids        | 0.24           | 0.14         | 0.23          | 0.03         | 0.16   | 0.02 |
| News        | 0.22           | 0.14         | 0.20          | 0.02         | 0.06   | 0.07 |
| Recreation  | 0.31           | 0.15         | 0.27          | 0.09         | 0.21   | 0.03 |
| Reference   | 0.26           | 0.08         | 0.22          | 0.01         | 0.37   | 0.02 |
| Regional    | 0.27           | 0.16         | 0.24          | 0.04         | 0.19   | 0.01 |
| Science     | 0.36           | 0.15         | 0.23          | 0.03         | 0.15   | 0.06 |
| Shopping    | 0.13           | 0.02         | 0.22          | 0.14         | 0.02   | 0.02 |
| Society     | 0.39           | 0.16         | 0.18          | 0.05         | 0.16   | 0.04 |
| Sports      | 0.21           | 0.16         | 0.23          | 0.13         | 0.21   | 0.04 |
| Control     | 0.16           | 0.13         | 0.17          | 0.03         |        |      |

Table 20: Ad bidding and cookie syncing participation under GDPR and CCPA after opt-out (Out) and opt-in (In) with C-Sync. Avg. column represents the mean of all bid value from advertisers who did not bid or appear when we simulated personas but appeared and bid after we opt-out. Out and In under C-Sync. represent number of cookie syncing events after opt-out and opt-in, respectively.

| Persona     | GDPR Out Avg. | GDPR C-Sync. Out Avg. | CCPA Out Avg. | CCPA C-Sync. Out Avg. | p-val. | Eff. |
|-------------|----------------|------------------------|---------------|------------------------|--------|------|
| Adult       | 0.19           | 24.20                  | 0.20          | 128.14                 |        |      |
| Arts        | 0.16           | 50.21                  | 0.29          | 108.14                 |        |      |
| Business    | 0.14           | 43.15                  | 0.19          | 118.17                 |        |      |
| Computers   | 0.21           | 52.19                  | 0.21          | 122.15                 |        |      |
| Games       | 0.64           | 61.18                  | 0.24          | 120.18                 |        |      |
| Health      | 0.17           | 37.14                  | 0.22          | 184.25                 |        |      |
| Home        | 0.16           | 45.15                  | 0.15          | 101.20                 |        |      |
| Kids        | 0.25           | 52.17                  | 0.25          | 136.12                 |        |      |
| News        | 0.20           | 36.14                  | 0.17          | 59.17                  |        |      |
| Recreation  | 0.18           | 42.17                  | 0.22          | 157.16                 |        |      |
| Reference   | 0.18           | 46.19                  | 0.22          | 143.14                 |        |      |
| Regional    | 0.13           | 49.13                  | 0.25          | 163.25                 |        |      |
| Science     | 0.37           | 40.19                  | 0.25          | 146.17                 |        |      |
| Shopping    | 0.15           | 47.19                  | 0.22          | 189.15                 |        |      |
| Society     | 0.12           | 35.12                  | 0.16          | 109.16                 |        |      |
| Sports      | 0.18           | 37.19                  | 0.19          | 83.16                  |        |      |
| Control     | 0.16           | 45.16                  | 0.17          | 130.17                 |        |      |

A.3 Quantcast

Data Usage. We evaluate reduction in data usage by analyzing advertisers bidding behavior. Table 19 presents advertisers bidding behavior for Quantcast. We note that under both GDPR and CCPA, all personas bid higher than control and in 9 such personas under GDPR and 1 persona under CCPA the bid value is higher than the average and standard deviation of the control (i.e., 0.08 std. under GDPR and 0.18 std. under CCPA). For Games, Health, and Science personas the bid values are higher than twice the bid value for the control persona under GDPR. For Health persona, the bid values are 3 times higher than that of the control under GDPR.

Next, we analyze if there is statistically significant difference between advertisers bidding patterns when users opt-out or opt-in to data processing and sharing/selling. It can be seen in Table 19 that under GDPR, for 11 personas advertisers behavior does not significantly changes regardless of whether users opt-out or opt-in. For 5 personas there are statistically significant differences in advertisers bidding, however, for all the cases the effect size is small. Under CCPA, for 14 personas advertisers behavior does not significantly changes regardless of whether users opt-out or opt-in. For Adult and Games personas there are statistically significant changes in advertisers behavior but the effect size is small.

Server-side data sharing. We evaluate reduction in server-side data sharing by analyzing bidding from advertisers to which we do not leak data. Table 20 presents bids from advertisers to which we did not explicitly leak data. Under GDPR, for 10 personas advertisers bid higher than the control and in 2 such cases the bid values are more than 2 times higher than that of the control. Only 4 personas receive bid values that are less than that of the control but the difference is only 0.04 at max. Under CCPA, 13 personas receive higher bid values, where bid values for Health persona are 3 times higher than that of the control. Only 2 persons receive bid values that are less than that of the control but the difference is only 0.01.

Client-side data sharing. We evaluate reduction in client-side data sharing by measuring cookie syncing by advertisers in network traffic. Table 20 presents the cookie syncing participation of advertisers. Under GDPR, we note that there is difference between advertisers cookie syncing behavior for opt-out and opt-in. Advertisers participate in cookie syncing across all personas in both cases when users opt-out and opt-in, however, when users opt-in, we did not explicitly leak data. Under GDPR, 5 personas bid higher than the control and 3 personas bid less than the control. However, the difference in bid values is at most 0.01, except for Home and Science, where the bid values are substantially higher. Under CCPA, all personas receive higher bid values than the average values in the control, where the bid values for Science persona are 2.3 times higher than that of the control.

Client-side data sharing. We evaluate reduction in client-side data sharing by measuring cookie syncing by advertisers in network traffic. Table 18 presents the cookie syncing participation of advertisers. Under GDPR, we note that there is difference between advertisers cookie syncing behavior for opt-out and opt-in. Advertisers participate in cookie syncing across all personas in both cases when users opt-out and opt-in, however, when users opt-in, we did not explicitly leak data. Under GDPR, 5 personas bid higher than the control and 3 personas bid less than the control. However, the difference in bid values is at most 0.01, except for Home and Science, where the bid values are substantially higher. Under CCPA, all personas receive higher bid values than the average values in the control, where the bid values for Science persona are 2.3 times higher than that of the control.
of advertisers for Quantcast. Under GDPR, we note that there is a substantial difference between advertisers in cookie syncing behavior for opt-out and opt-in. Specifically, we experience cookie syncing events in all personas when we opt-out but we experience substantial more cookie syncing when we opt-in. On average there are 45 and 169 cookie syncing events per persona when users opt-out and opt-in, respectively. Under CCPA, advertisers engage in cookie syncing events on all 16 personas, except for Kids persona when users opt-in, regardless of whether the users opt-out or opts-in. However, on average the difference in cookie syncing events between opt-out and opt-in is not significantly large as compared to GDPR. On average there are 130 and 174 cookie syncing events per persona when users opt-out and opt-in, respectively.

We further investigate cookie syncing frequency of individual advertisers. It can be seen from Table 5 that advertisers participate in as many as 170 and 317 cookie syncing events when we opt-out under GDPR and CCPA with Quantcast, respectively. 

**Takeaway.** Significant decreases in data usage and sharing are not readily apparent when users choose to opt-out. Within the framework of GDPR, there are noticeable shifts in advertisers’ bidding patterns for 5 different user personas, although these changes are only minor in terms of impact. When users opt-in under GDPR regulations, a notable increase in cookie syncing events becomes evident. This suggests that ensuring compliance with both GDPR and CCPA on the same websites might not be assured.

### A.4 NAI

We also analyze advertisers bidding behavior by exercising advertisers offered opt-out controls. Specifically, we opt-out through National Advertising Initiative (NAI) – an advertising consortium – provided controls to opt-out of targeted advertising [27]. Similar to state-enforced regulations, i.e., GDPR and CCPA, we evaluate whether opt-out through NAI reduces targeting, whether the reduction is statistically different, and whether advertisers share data without user consent.

**Data usage.** We evaluate reduction in data usage by analyzing advertisers bidding behavior. Table 21 presents advertisers bidding on personas when users opt-out and opt-in through NAI under GDPR and CCPA. We note that under GDPR, all 16 personas bid higher than that of the control. Note that advertisers do bid for control personas but with 0 values. Under CCPA, 5 personas bid higher than the control and 9 personas bid lower than control. For Health persona, the bid values are 3.14 times higher than the control. It can also be seen in Table 21 that under both GDPR and CCPA, for all personas there is no statistically significant difference between advertisers bidding behavior.

**Server-side data sharing.** We evaluate reduction in server-side data sharing by analyzing bidding from advertisers to which we do not leak data. Table 22 presents bids from advertisers to which we did not explicitly leak data. Under GDPR, 12 personas receive bids with 0 values but 4 personas still receive higher bids than the control when users opt-out. Under CCPA, however, all 16 personas receive lower bids than the control.

**Client-side data sharing.** We evaluate reduction in client-side data sharing by measuring cookie syncing by advertisers in network traffic. Table 22 presents the cookie syncing participation of advertisers for NAI. Under GDPR, there is no substantial difference between advertisers cookie syncing behavior for opt-out and opt-in. In fact, there are 3 more cookie syncing events on average when users opt-out. Under CCPA, advertisers engage in cookie syncing events on all personas regardless of whether the user opts-out or opts-in. However, when users opt-in, the number of cookie syncing events on average doubles from 26 to 48.

We further investigate cookie syncing frequency of individual advertisers. It can be seen from Table 5 that advertisers participate in as many as 107 and 190 cookie syncing events when we opt-out under GDPR and CCPA with Quantcast, respectively. 

**Takeaway.** The utilization of advertisers’ data remains relatively stable. Nevertheless, advertisers submit lower bids under CCPA in contrast to GDPR. Correspondingly, we have observed a marked
Table 24: Cookie syncing events by advertisers under CCPA in California after Pre-opt-out. Evt. column represents the number of cookie syncing events from advertisers, respectively.

| Persona     | Cookiebot Evt. | Didomi Evt. | CCPA OneTrust Evt. | Quantcast Evt. | NAI Evt. |
|-------------|----------------|-------------|--------------------|----------------|---------|
| Adult       | 17             | 39          | 107                | 125            | 31      |
| Arts        | 27             | 35          | 90                 | 90             | 24      |
| Business    | 23             | 36          | 77                 | 94             | 27      |
| Computers   | 16             | 34          | 79                 | 73             | 32      |
| Games       | 15             | 45          | 109                | 96             | 25      |
| Health      | 15             | 41          | 134                | 89             | 71      |
| Home        | –              | 37          | 46                 | 104            | 29      |
| Kids        | 26             | 57          | 111                | 90             | 59      |
| News        | 37             | 34          | 100                | 66             | 31      |
| Recreation  | 21             | 57          | 61                 | 83             | 45      |
| Reference   | –              | 35          | 64                 | 95             | 30      |
| Regional    | 18             | 32          | 106                | 137            | 43      |
| Science     | –              | 46          | 71                 | 86             | 49      |
| Shopping    | 13             | 37          | 62                 | 98             | 30      |
| Society     | 47             | 54          | 94                 | 91             | 56      |
| Sports      | 18             | 34          | 112                | 107            | 31      |
| **Average** | **18**         | **41**      | **89**             | **95**         | **40**  |

Table 23: Cookie syncing events by advertisers under GDPR in Germany after Pre-opt-out. Evt. column represents the number of cookie syncing events from advertisers, respectively.

| Persona     | Cookiebot Evt. | Didomi Evt. | GDPR OneTrust Evt. | Quantcast Evt. | NAI Evt. |
|-------------|----------------|-------------|--------------------|----------------|---------|
| Adult       | –              | 6           | 19                 | 27             | 16      |
| Arts        | –              | –           | 29                 | 24             | 17      |
| Business    | –              | –           | 46                 | 26             | 14      |
| Computers   | –              | 9           | 20                 | 37             | 29      |
| Games       | –              | 8           | 30                 | 20             | 15      |
| Health      | –              | 13          | 21                 | 12             | 5       |
| Home        | –              | –           | 46                 | 27             | 6       |
| Kids        | –              | 15          | 34                 | 41             | 13      |
| News        | –              | –           | 21                 | 25             | 13      |
| Recreation  | –              | –           | 4                  | 23             | 5       |
| Reference   | –              | –           | 34                 | 31             | 22      |
| Regional    | –              | 34          | 37                 | 21             |         |
| Science     | –              | –           | 16                 | 16             | 10      |
| Shopping    | –              | 7           | 41                 | 25             | 16      |
| Society     | –              | –           | 54                 | 21             | 7       |
| Sports      | –              | –           | 41                 | 27             | 1       |
| **Average** | **–**          | **4**       | **31**             | **26**         | **13**  |

decrease in data sharing, both on the server-side and client-side, under CCPA. This suggests that achieving compliance with both GDPR and CCPA might not be guaranteed on identical websites.

### B ADVERTISERS BIDDING BEHAVIOR WITH PRE-OPT-OUT

Under GDPR processing personal data is prohibited, unless the data subject has consented to the processing (Article 6). However, under CCPA, data selling and sharing should immediately stop once consumers opt-out (Section 798.120 (a), Section 7013 (a)). Thus to eliminate the impact of data collection and sharing prior to opting-out, we conduct additional experiments where we opt-out prior to simulating personas.

Table 25 and Table 26 present the ad bidding under GDPR and CCPA. Under GDPR, we note that advertisers bid higher for most personas than control across all four CMPs. In several instances the bid values are even higher than the sum of average and standard deviation of the bid values in control persona. Under CCPA, however, we note varying trends across CMPs. For Cookiebot, OneTrust, and Quantcast 16, 7, and 4 personas receive higher bid values from advertisers despite opting out, respectively. In the case of Didomi, only 1 persona receives higher bid values.

Table 23 and Table 24 present the cookie syncing events from advertisers under GDPR and CCPA. We note that advertisers participate in cookie syncing events despite users opting out under both GDPR and CCPA.

**Takeaway.** Similar to post opt-out, we note that under GDPR advertisers continue to use data even when we opt-out prior to collecting bids. Under CCPA, as compared to GDPR, less number of personas receive higher bid values than that of the control. However, there are still several personas where advertisers continue to bid higher than the control. In the case of client side data sharing, we did not notice any reduction in cookie syncing under both GDPR and CCPA.
Table 25: Ad bidding under GDPR in Germany. Avg. column represents the mean of all bid value. Std. represents the standard deviation of all bid value. Pre-opt-out represents the bids when we opt-out the usage of user data before we stimulate the persona, respectively. Light red and light blue indicate bid values that are higher and lower than Control’s avg., respectively. Dark red and Dark blue indicate bid values that are Control’s avg. ± std., respectively. Column p-val. and Eff. represent p-value and effect size, respectively.

| Persona | Cookiebot | Didomi | OneTrust | Quantcast | NAI |
|---------|-----------|-------|----------|-----------|-----|
|         | Avg. Std. | Avg. Std. | Avg. Std. | Avg. Std. | Avg. Std. |
| Adult   | 0.37 0.20 | 0.02 0.00 | 0.08 0.04 | 0.58 1.99 | 3.3E-4 1.8E-3 |
| Arts    | 0.37 0.20 | 0.71 0.08 | 0.56 0.22 | 0.16 0.08 | 4.0E-3 0.03 |
| Business| 0.37 0.20 | – – | 0.09 0.03 | 1.88 0.03 | 1.0E-2 0.04 |
| Computers| 0.38 0.20 | 0.01 0.00 | 0.05 0.03 | 0.16 0.07 | 0.01 0.06 |
| Games   | 0.37 0.20 | 0.01 0.00 | 0.07 0.05 | 0.16 0.07 | 6.4E-4 2.9E-3 |
| Health  | 0.37 0.20 | 0.12 0.11 | 0.11 0.05 | 0.16 0.07 | 1.0E-2 0.08 |
| Home    | 0.37 0.20 | – – | 0.08 0.05 | 0.23 0.23 | 1.7E-3 0.01 |
| Kids    | 0.37 0.20 | 0.01 0.00 | 0.13 0.04 | 0.06 0.21 | 2.1E-3 0.03 |
| News    | 0.37 0.20 | 0.04 0.04 | 0.08 0.02 | 0.55 1.97 | 1.0E-3 0.06 |
| Home    | 0.37 0.20 | – – | 0.12 0.01 | 0.34 2.01 | 1.5E-3 0.01 |
| Kids    | 0.36 0.21 | 0.01 0.00 | 0.17 0.10 | 0.35 2.17 | 0.01 0.09 |
| Society | 0.38 0.19 | – – | 0.14 0.19 | 0.16 0.07 | 0.01 0.08 |
| Sports  | 0.37 0.20 | – – | 0.07 0.10 | 0.16 0.07 | 0.01 0.08 |
| Control | 0.31 0.23 | 0.01 0.00 | 0.07 0.08 | 0.14 0.08 | 5.7E-4 2.7E-3 |

Table 26: Ad bidding under CCPA in California. Avg. column represents the mean of all bid value. Std. represents the standard deviation of all bid value. Pre-opt-out represents the bids when we opt-out the usage of user data before we stimulate the persona, respectively. Light red and light blue indicate bid values that are higher and lower than Control’s avg., respectively. Dark red and Dark blue indicate bid values that are Control’s avg. ± std., respectively. Column p-val. and Eff. represent p-value and effect size, respectively.

| Persona | Cookiebot | Didomi | OneTrust | Quantcast | NAI |
|---------|-----------|-------|----------|-----------|-----|
|         | Avg. Std. | Avg. Std. | Avg. Std. | Avg. Std. | Avg. Std. |
| Adult   | 0.38 0.21 | 0.13 0.08 | 0.38 0.68 | 0.18 0.26 | 0.07 0.12 |
| Arts    | 0.37 0.21 | 0.11 0.10 | 0.85 1.36 | 0.22 0.63 | 0.03 0.11 |
| Business| 0.36 0.22 | 0.10 0.07 | 1.26 1.49 | 0.17 0.11 | 0.05 0.12 |
| Computers| 0.36 0.20 | 0.11 0.10 | 1.12 1.33 | 0.32 1.66 | 0.05 0.15 |
| Games   | 0.37 0.20 | 0.15 0.11 | 0.73 1.07 | 0.19 0.19 | 0.04 0.11 |
| Health  | 0.38 0.20 | 0.09 0.08 | 0.61 0.86 | 0.44 0.86 | 0.52 1.25 |
| Home    | 0.37 0.20 | 0.16 0.35 | 0.80 1.12 | 0.18 0.17 | 0.06 0.14 |
| Kids    | 0.38 0.19 | 0.06 0.06 | 0.59 0.96 | 0.17 0.12 | 0.12 0.19 |
| News    | 0.37 0.19 | 0.12 0.09 | 0.66 1.10 | 0.17 0.10 | 0.04 0.11 |
| Recreation| 0.36 0.20 | 0.10 0.09 | 0.50 0.82 | 0.17 0.17 | 0.17 0.60 |
| Science | 0.38 0.20 | 0.13 0.15 | 0.81 1.17 | 0.20 0.58 | 0.05 0.12 |
| Shopping| 0.36 0.21 | 0.12 0.10 | 0.86 1.28 | 0.21 0.63 | 0.05 0.11 |
| Society | 0.35 0.21 | 0.13 0.11 | 0.31 0.37 | 0.20 0.18 | 0.03 0.07 |
| Sports  | 0.37 0.22 | 0.08 0.07 | 0.75 1.04 | 0.16 0.10 | 0.10 0.19 |
| Control | 0.35 0.21 | 0.15 0.14 | 0.74 1.10 | 0.21 0.82 | 0.07 0.17 |