On dark patterns and manipulation of website publishers by CMPs

Michael Toth, Nataliia Bielova, Vincent Roca

Michael Toth*, Nataliia Bielova, and Vincent Roca

On dark patterns and manipulation of website publishers by CMPs

Abstract: Web technologies and services widely rely on data collection via tracking users on websites. In the EU, the collection of such data requires user consent thanks to the ePrivacy Directive (ePD), and the General Data Protection Regulation (GDPR). To comply with these regulations and integrate consent collection into their websites, website publishers often rely on third-party contractors, called Consent Management Providers (CMPs), that provide consent pop-ups as a service. Since the GDPR came in force in May 2018, the presence of CMPs continuously increased. In our work, we systematically study the installation and configuration process of consent pop-ups and their potential effects on the decision making of the website publishers. We make an in-depth analysis of the configuration process from ten services provided by five popular CMP companies and identify common unethical design choices employed. By analysing CMP services on an empty experimental website, we identify manipulation of website publishers towards subscription to the CMPs paid plans and then determine that default consent pop-ups often violate the law. We also show that configuration options may lead to non-compliance, while tracking scanners offered by CMPs manipulate publishers. Our findings demonstrate the importance of CMPs and design space offered to website publishers, and we raise concerns around the privileged position of CMPs and their strategies influencing website publishers.

Keywords: cookie banner, consent pop-up, CMP, dark pattern, nudge, sludge, user consent, influence, deceptive design, GDPR compliance, website publishers

DOI foobar

1 Introduction

While website publishers rely on data for statistics, advertising, monetisation, and optimisation of their websites, they tend to include tracking services in their websites. The ePrivacy Directive [1], amended in 2009 [2], and soon to be transformed into a Regulation, requires *user's consent* before any access or storage of any non-mandatory data, and hence any tracking technology, on the user's device. The European Union's General Data Protection Regulation (GDPR) [3], which went into effect on May 25, 2018, defines the rules on *valid consent* [3, Art. 4, 7]. Requirement for collecting consent on websites resulted in appearance of *consent pop-ups*, often referred to as "cookie banners", and such pop-ups have become increasingly popular among the EU-based websites [4, 5].

However, providing *legally-valid consent pop-up* to website users is a complex task as recently shown by Santos et al. [7], who identified 22 legal and technical requirements of valid consent on the Web based on legal sources, recommendations, and technical analysis. Collecting invalid consent have significant negative consequences for end users, such as unintentional sharing of personal information. As a result, the website publishers, who are considered legally responsible for compliance of their websites can face administrative fines up to 20 million euros, or up to 4% of the total worldwide annual turnover [3, Art. 83(5)], but also can suffer in terms of bad reputation and loss of trust. In the last two years, a number of website publishers were fined for *non-compliance* with the GDPR consent requirements on their websites as established by the EU Court of Justice in 2019 Planet49 case [8], as well as many EU Data Protection Authorities (DPAs) such as Dutch DPA [9], Spanish DPA [10], Danish DPA [11], French DPA [12–15]. Recently, in May 2021 the French Data Protection Authority (CNIL) has notified twenty popular websites in France of their violation of the EU law in the consent pop-ups on their websites [16].

As a result, website publishers often do not collect consent themselves, but prefer to delegate this task to privacy experts. This demand created a market need and opened a new business opportunity to emerg-

1 The work conducted by Nataliia Bielova was accomplished while she was at Inria PRIVATICS team prior to her joining the CNIL on 1 September 2021. The views expressed in this document do not necessarily reflect the views of the Commission or any individual Commissioner.

***Corresponding Author: Michael Toth:** Centre Inria de l'Université Grenoble-Alpes, michael.toth@inria.fr

Nataliia Bielova: Nataliia Bielova, LINC team, CNIL, France

Vincent Roca: Centre Inria de l'Université Grenoble-Alpes, vincent.roca@inria.fr

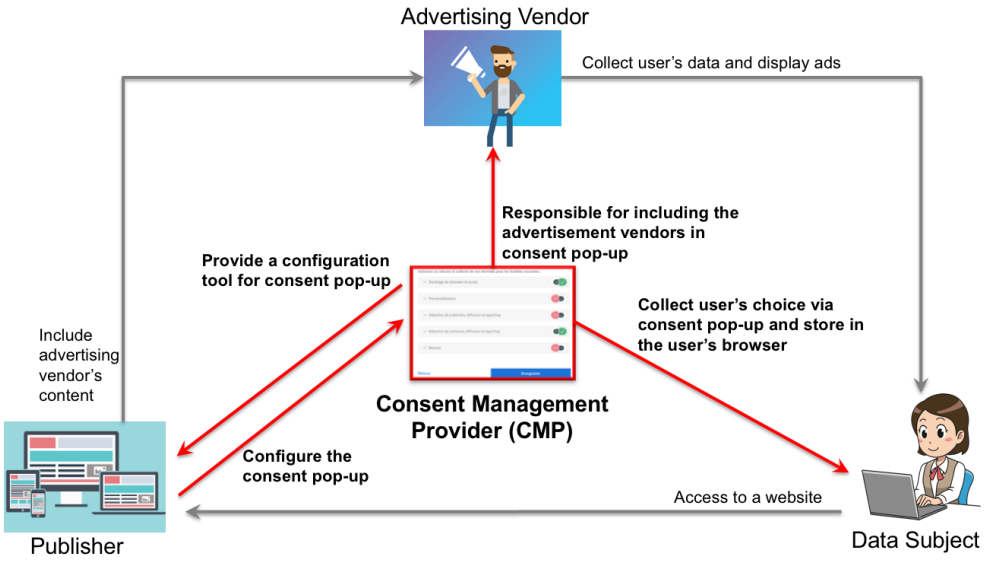

Fig. 1. Influence of CMPs on the main actors in the web advertising ecosystem: publishers, advertisers, and users. Figure inspired by the work of Santos et al. [6].

ing companies called Consent Management Providers (CMPs) that provide "*Consent as a Service*" solutions to website publishers. Such companies are becoming more and more popular, as demonstrated by the work of Hils et al. [17]: the usage of CMPs by websites has increased several times since the GDPR came into force on May 25, 2018. CMPs studied in most of the previous works [5, 6, 17–19] implement a common framework provided by the European branch of the Interactive Advertising Bureau (IAB Europe), called Transparency and Consent Framework (TCF) [20].

Previous works [5, 6, 19] demonstrated that CMPs occupy a specific, and rather central place in the web advertising ecosystem, as shown in Figure 1. Multiple studies analyzed how end users are manipulated towards giving their consent to collection of their data via consent pop-up interface, identifying *dark patterns* and other strategies and their impact on users' decision making [18, 21–24], often designed by the CMPs.

What was not studied so far, is the user journey of website publishers when they try to install the consent pop-ups provided by the CMPs: do CMPs *influence website publishers*? Are website publishers also *manipulated towards a specific design of consent pop-ups* to be installed on their websites? Moreover, do CMPs profit from such a central position and *collect users' data by their own services* as recently shown [6]? Such manipulation and integration can have a significant impact on the overall compliance of the website in question. Since from legal perspective website publishers are considered "data controllers" [6] in the scope of the GDPR, website publishers are legally responsible for the overall behavior and legal compliance of their websites, even when they use third party services, such as CMPs.

In this paper, we systematically study design properties of the installation and configuration process of consent pop-ups and their potential effects on the decision making of the website publishers. We make an in-depth analysis of the configuration process from ten services provided by five popular CMP companies and identify common dark patterns employed. Our research goal is to explore the design space for consent pop-up generation process to learn how to encourage website publishers to install a legally compliant consent pop-up mechanism. We conduct a study of consent pop-up services accessible to website publishers, by installing them on our empty experimental websites, registering and analysing all steps during installation and configuration processes, detecting dark patterns in the sense of Mathur et al. [25], evaluating overall compliance of pop-ups provided by default, and monitoring network communications to identify when consent pop-ups collect users' data for their own purposes.

The study contains four distinct investigations motivated by the following research questions. We first study the presence of dark patterns in the registration and configuration process of consent pop-ups; evaluate whether dark patterns of the default pop-up make the final pop-up compliant with the law; and study whether CMPs

use their position and large presence to collect data for their own use:

- **RQ1.** Do CMPs use ethically and/or legally problematic strategies known as "dark patterns" in the generation process of their consent pop-ups, to influence the publisher in their own interest?
- **RQ2.** Is a consent pop-up generated with the default options provided by the CMP compliant with EU legal requirements?
- **RQ3.** Do the default configuration options of consent pop-ups encourage publishers to comply with the requirements for collecting legally valid consent?
- **RQ4.** What are the functionalities and the impacts of tracker scanners provided by CMPs, regarding legal compliance, role of CMPs, and publishers behaviour?
- **RQ5.** Are CMPs abusing their central and privileged position and their presence on a large number of websites to collect data for their own use?

The central role of CMPs and the requirements for valid consent lead us to question the influence and potential manipulation techniques used by CMPs to nudge website publishers toward selecting the most advantageous options for the CMPs. While previous work tries to categorize the existing dark patterns, and measure their presence and impact on the behaviour of final users, no work so far analyzed how publishers can be influenced by the design choices in the installation and configuration process of consent pop-ups. In this article, we focus on the influence that CMPs can have on website publishers and their impact on the entire ecosystem.

Our work contains the following contributions:

- our work is the first to perform an *in-depth analysis of the configuration process* of consent pop-ups from the website publisher perspective by ten services provided by five popular CMP companies;
- we *identify manipulation of website publishers towards subscription to the CMPs paid plans*; installation of consent pop-ups that do not respect the freedom of choice, such as *consent walls* [24];
- by carefully analysing default consent pop-ups, we *detect integration of hundreds of advertising vendors*, registered in the IAB Europe TCF (i.e., the whole Global Vendors List) which makes it hard for website publisher to remove;
- we *identify lack of guidance for website publisher in the usage of "tracker scanner" services* provided by CMPs that impact the overall compliance of the consent pop-up and hence of the website in question. Moreover, we detect scanners that *use manipulative techniques*, such as fear of non-compliance, to nudge publishers toward subscribing to paid plans;
- finally, we detect CMPs that *include analytic services* in the consent pop-up or scanning report for *the data collection and further exploitation of end users' data for CMPs' own purposes.*

Based on the results of our study, we open a discussion on role and power of CMPs and conclude that not only did they not improve user privacy overall, but that they could create new important issues, such as the addition of new trackers, and sometimes use manipulative design techniques in their own economic interest.

2 Related Work

This section lists the major related works dealing with consent management process, classification and legal definition of dark patterns applied to data protection and consent, user studies and automated measurements focusing on CMPs or the IAB TCF Framework.

Measurement studies on prevalence of CMPs. In 2019, Nouwens et al. [18] studied five popular CMPs according to UK data provided by the advertising company Adzerk (now renamed Kevel) [26], and the impact of the design of consent pop-ups on the requirement for "freely given" consent. They found almost 90% of consent pop-up didn't meet the minimal legal requirements, and the absence of a "refuse" button on the first layer of the consent pop-up increases positive consent by about 22 percentage points. Hils et al. [17] analyzed 4.2 million domains between June 2018 and 2020 in order to measure CMP adoption over time. They estimate that CMPs prevalence on websites has doubled in 2019 and again in 2020, in particular on mildly-popular websites, as a result of compliance with the EU data protection regulation. Degeling et al. [4] monitored the prevalence of CMPs on websites during the five month before the GDPR came into force. They measured an overall increase from 50.3% to 69.9% across all 28 EU Member States, and a 16% increase in consent pop-ups' adoption before and after the GDPR. Complementary to these studies, Santos et al. [6] analysed the legal role of CMPs under the GDPR: they studied in which cases CMPs were determining purposes and means of the processing, which would qualify them as data controllers.

Classification of dark patterns. Brignull [27] coined dark patterns ten years ago as a generic term to describe deceptive design of a User Interface (UI), made to influence users and their decision-making abilities. He also built the first taxonomy of these designs with examples. Gray et al. [28] further presented a broader categorization of Brignull's taxonomy and clustered these dark patterns into five categories: Nagging, Obstruction, Sneaking, Interface Interference and Forced Action. Chromik et al. [29] discuss dark patterns of explainability, transparency and control, focusing on intelligent systems. They conclude that the legal right to explanation provided by the GDPR is not sufficient, and advocates for "specific guidelines and standards". All these classifications also address the manipulative design only by testing pop-ups displayed to end-users.

Impact of dark patterns in consent pop-up interfaces on users' choices. Nouwens et al. [18] were the first to study the presence of dark patterns in the user interface of five popular CMPs, as well as a user study with 40 participants evaluating the effect of specific design on users' consent choices. Utz et al. [21] studied the influence of common graphical nudges such as changes in the position or color of the consent pop-up on more than 80,000 visitors of a German e-commerce website.

Luguri et Strahilevitz [23] did a large-scale experiment to compare the influence of "mild" and "aggressive" dark patterns on different categories of American consumers. They found "mild" dark patterns to generate less negative feelings, and less educated people to be more influenced. In 2021, Gray et al. [24] highlight connections between HCI, design, privacy and data protection on consent pop-ups, focusing on three different types of dark patterns and their influence on end users. Mathur et al. [25] use the combined approaches of psychology, economics, ethics, philosophy, and law to formulate a general definition of dark patterns and their effects on users. Machuletz and Böhme [30] set up a user study on 150 Austrian students. They evaluated the impacts of the number of options and the presence or absence of a "Select all" button in post-GDPR consent pop-ups. Soe et al. [31] manually collected banners from 300 Scandinavian and English-speaking news services, they found wide presence of "unethical practices". In particular, 43% of the tested websites containing dark patterns were using obstruction, and 45.3% were using interface interference.

Summary. All the previous works focus on the influence of dark patterns on *end-users*. However, no studies so far have evaluated whether CMPs include manipulative practices or dark patterns that *nudge website publishers* towards installing a particular design of their consent pop-up services.

3 Methodology

Selection of Consent Management Providers (CMPs). To decide which CMPs to investigate, we used the most recent work in the field. Hils et al. [17] showed that Quantcast and OneTrust are the two most popular CMPs in the EU and in the US. Their presence was found respectively on 38.3% and 16.3% of the websites with a EU or UK TLD [17, Fig. 6], followed by TrustArc, Cookiebot, and Crownpeak. These five identified CMPs were also examined by the recent work of Nouwens et al. [18] and resulting as most popular in the latest version of the Kevel CMP tracker [32], a prevalence ranking service that was used by Nouwens et al. [18]. Therefore, we have build a preliminary list of five companies – Quantcast, OneTrust, TrustArc, Cookiebot, and Crownpeak – based on previous work and Kevel service. We then added LiveRamp CMP [33], already studied by Hils et al. because of its novelty, which is linked to a major data broker [34]. Finally, we interviewed with a Data Protection Officier (DPO) who works for EU and US companies: they pointed us to Cookie Script CMP [35], which is particularly popular among Small and Medium Enterprises (SME). We preselected both free and paid services, including "premium" ones (see Table 1).

Installation of preselected CMPs. We contacted six of the identified companies – Quantcast, OneTrust, TrustArc, Cookiebot, Crownpeak, LiveRamp – via their websites using contact forms or provided emails, and received different types of responses. Quantcast replied that their paid CMP was discontinued, and that all the functionalities were now integrated into the free one [36]. OneTrust did a presentation call with us, but after that declined to give us access to their trial version for research purposes. However, we studied three versions of their self-service CookiePro brand, accessible via online subscription: free unlogged (no account), free logged (with mandatory account), and paid standard service. TrustArc took more than one month to reply, which prevented us to include the study of their consent pop-ups in this work. Crownpeak initially did the same, and then added an online subscription option for their

CMP	Contact details	Installation results
CookiePro by OneTrust	OneTrust declined to give access to trial version of its paid service for academic research, but we successfully installed the two free services and later the standard paid service of their CookiePro brand.	Paid service: ✓ Free (logged) serv.: ✓ Free (unlogged) serv.: ✓
Quantcast	Free service called "Choice" was successfully installed.	Free service: ✓
TrustArc	The company did not respond in the span of one month.	Paid (Premium) serv.: ×
Cookiebot	Installation through the company website was accessible without any additional requirement. Both free and paid services were successfully installed.	Paid ✓ Free service: ✓
Crownpeak	First the company did not respond in the span of one month. Then, they added an online subscription to their website, giving us the possibility to install the "Business" service.	Paid (Premium) serv.: ✓
LiveRamp	Company scheduled an online meeting, but declined to provide its service for academic research motivating that their service was "only for publishers". The company did not recontact within one month after the meeting.	Unknown ×
Cookie Script	Installation through the company website was accessible without any additional requirements. Free and paid services were successfully installed.	Paid (Plus) serv.: ✓ Paid (Lite) serv.: ✓ Free service: ✓

Table 1. Preselected list of 7 CMPs identified via prior work [17, 18] and commercial service [32], with contact details, in particular when a direct contact with the CMP team is needed to install the service, and installation results: ✓ or × . When a service is an order of magnitude more expensive than the average, it is labeled as "Premium".

"Business" CMP service, that we successfully installed. During a presentation call, LiveRamp said they would come back to us to say if it was possible to test their service that was "only for publishers", but they failed to do so after six weeks. Cookiebot and Cookie Script CMP services were directly available on the website and we installed their consent pop-ups directly. We studied both the free and paid versions of Cookiebot. For Cookie Script, we studied three services: the free version, plus the cheapest (Lite) and most expensive (Plus) paid versions.

Summary of selected CMPs. After removing the CMPs that refused installation for research purposes or did not respond in one month, we obtained ten different services provided by five CMPs: Quantcast, CookiePro, Cookiebot, Cookie Script, and Crownpeak (Table 2). For our analysis of the registration process (further described in Section 4.1), we also used results from some of the preselected CMPs to highlight their manipulative strategies during the registration.

Configuration used for experiments. For our tests, we used a dedicated version of Mozilla Firefox (v84.0) with an independent profile [37], running on GNU/Linux Ubuntu 18.04.5 LTS. To avoid interpretation errors resulting from different browser versions, we blocked automated updates of the used browser. We have also enabled all third-party cookies and disabled the "Enhanced Tracking Protection" of Firefox to avoid interference with our experiments. We install the extension Ernie [38] on this browser, that is able to detect 6 categories of cross-site tracking via cookies, including several types of cookie synchronizations. This extension, that implements cookie-based tracking detection proposed by Fouad et al. [39], enables us to detect and flag cookies according to their behaviour.

We performed our first measurements in April and May 2021, from a French institution. We did a second group of measurements between September and November 2021, in which one paid version of CookiePro, the two paid versions of CookieScript, and Crownpeak were added. In all cases, the new rules regarding the terms and conditions for refusing consent were already enforced by the French DPA, since they came in force on April 1^{st}, 2021 [40]. In other words, publishers must offer to the users the possibility of accepting and refusing read and/or write operations, such as the implantation of cookies in their terminal, with the same degree of simplicity [41, par. 30 p. 8].

3.1 Detecting manipulation by CMPs

To answer the research questions listed in Section 1, we built the following experiments. The different parts of our study are summarized in Figure 2 and further explained in the rest of this section.

(1) Registration and (2) Configuration processes. In order to evaluate CMPs while minimizing possible interferences, we created one empty web-

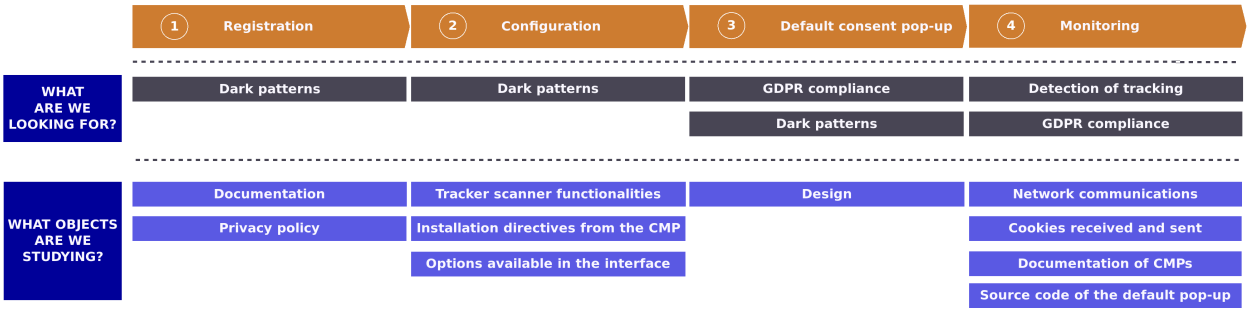

Fig. 2. Study of legally and/or technically problematic design choices. This flowchart identifies the elements analyzed in this article.

site per studied CMP under our EU institution's 2nd level TLD: `cmp-name-version.inrialpes.fr`. For each available consent pop-up version (free, paid, etc. – see Table 2) of a studied CMP, we installed one version pop-up per dedicated website hosted on `cmp-name-version.inrialpes.fr`.

When installing a CMP service, we select GDPR-compliant version of consent pop-ups when asked. CookiePro proposes to either set up a consent pop-up directly on their website without creating an account (we call it "unlogged" version) or by creating an account ("logged" version) – in this case, we studied both versions.

When necessary, we distinguish between the *registration* process, which consists for the publisher to fill a form to get access to the CMP services, and the *configuration* process, which consists to configure the consent pop-up according to the needs of the publisher. In each case, we take screenshots during the whole process, matching our observations with known dark patterns [28, 42, 43] and legal requirements from previous works [7]. We list problematic behaviour observed, such as "dark patterns" in both processes, and categorize them from legal and design point of views using previous work definitions (Taxonomies from Gray et al. [28] and Mathur et al. [43], CNIL recommendation [44], list of legal requirements from Santos et al. [7, Table 6]).

(3) Default consent pop-up. For each service that we installed (Table 2), we followed the instructions of the CMP and installed the version of the pop-up proposed by CMP *by default*, that is without any modifications in the proposed interface or alternations to the source code of the proposed code snippet to be added to our experiments website (we used one subdomain per CMP service, as explained in the beginning of this section). In each installed consent pop-up, that we now call *default consent pop-up*, we identify potential manipulative strategies in the configuration process as well as potential violations of legal requirements for GDPR-valid consent in the default consent pop-up obtained.

(4) Monitoring and analysis of the network communications. To detect tracking cookies and other suspicious behaviors, we rely on the Firefox web developer tools as well as Ernie extension [38], and visit the subdomain `cmp-name-version.inrialpes.fr`, one per each CMP service. We record all HTTP(S) requests and responses, cookies stored/sent that give indications of possible data collection. We open the page in the main and hidden tab of Ernie, a functionality that has the ability to detect shared identifiers. We check the findings of Ernie to display cookies associated with the page load, and detect if these cookies are performing one of the six types of user tracking described by Fouad et al. [39]. We then repeat the experiment, (1) giving a full consent by clicking "Accept all" on the consent pop-up, and (2) refusing to give any consent by clicking "Reject all" on the pop-up (when available). When no "Reject all" button or similar option was provided on the first page of the consent pop-up, we decline consent for all categories in the customization interface. We record our observations, and try to explain them with the help of the documents provided by the companies such as Privacy Policies and commercial documentation. We keep a record of these documents at the date of the consultation. We also search in the code of the consent pop-ups to find possible unnecessary data sent to third-parties.

Additionally, we take the name of each studied company as recorded in the CMP list [45] provided by the IAB Europe, and search for it in the Global Vendor List (GVL) [46] for a possible matching to identify companies that operates both as vendor (advertiser) and CMP. When a company is referenced in both lists, it indicates that it has both (1) an interest into using trackers as a vendor, and (2) the possibility to control the way trackers load on websites as a CMP. This dual position can lead to an ethically questionable situation.

CMP	Company location	Service tested	Price	Login required	Subdomain used for tests
CookiePro by OneTrust	UK (London) US (Atlanta)	Free CMP builder	Free	No	cookiepro-free.inrialpes.fr
		Free Account	Free	Yes	cookiepro-free-logged.inrialpes.fr
		Standard Account	$30/mo. ($360/y.)	Yes	cookiepro-paid-1.inrialpes.fr
Quantcast	US (San Francisco)	Choice	Free	Yes	quantcast-free.inrialpes.fr
Cookiebot	DK (Copenhagen)	Free Plan	Free	Yes	cookiebot-free.inrialpes.fr
		Premium Small	9 €/mo. (108 €/y.)	Yes	cookiebot-paid.inrialpes.fr
Crownpeak	US (Denver)	Business	$1,000/y. (Premium)	Yes	crownpeak-paid.inrialpes.fr
Cookie Script	LH (Vilnius)	Free (prev. "Starter")	Free	Yes	cookiescript-free.inrialpes.fr
		Lite	6 €/mo. (72 €/y.)	Yes	cookiescript-paid-1.inrialpes.fr
		Plus	9 €/mo. (108 €/y.)	Yes	cookiescript-paid-2.inrialpes.fr

Table 2. List of CMPs selected and installed for experiments. Prices indicated when publicly available on the companies' websites.

3.2 Ethical considerations

Our study was conducted on an empty website hosted by our French institution, and involved real companies registered as CMPs in the IAB Europe TCF Framework. Our study did not involve real users, but instead took the role and simulated the user journey of website publishers when installing services proposed by CMPs.

We installed a consent pop-up directly via a website of a CMP, whenever possible (which is the case of CookiePro Free CMP builder, "Free" account, and "Standard" account, Cookiebot free, Crownpeak Business, and Cookie Script Free, Lite and Plus). However, for TrustArc, and LiveRamp, we had to contact the companies via contact forms or emails. We intentionally shared our main purpose of the study, which is academic research, in order to provide transparency as to the purpose of the usage of selected CMPs. By doing so, we ensured not to deceive the CMP companies.

However, our experience demonstrates that OneTrust and LiveRamp decline to give us access to their paid services, even when we were ready to pay for their paid versions. We later managed to include CookiePro (by OneTrust) paid service when directly accessible online. TrustArc did not respond to us within one month, thus not allowing us to study their services. It should be noted that TrustArc is the only company to our knowledge that enforces a contractual "Acceptable use" policy preventing any "attempt to discover any source code or underlying ideas or algorithms of the Services" without a written prior agreement.

Open question for the research community. We therefore raise the question whether researchers need to inform the studied services of the purposes of their research or not. As our experience shows, transparency and openness about research goals often implies that only some of the services can be studied.

4 Findings

Our goal in this section is to analyze the whole process followed by website publishers when they want to add consent pop-ups to ensure GDPR compliance to their websites. We distinguish in our observations of the configuration process between the misleading nature of the process itself towards the publisher, and the presence of options that may lead publishers to deploy non-compliant consent pop-ups. In the latter case, we also highlight whether these options are active by default, or require an active action by the publisher, as well as the potential presence of any help or advice from the CMP. Therefore, we describe our findings from five different angles guided by our research questions from Section 1:

§4.1 The registration process of consent pop-ups via websites of CMPs;

§4.2 Compliance of default consent banners generated by CMPs;

§4.3 The configuration process of the consent pop-ups provided by CMPs;

§4.4 The use of tracking detection tools ("tracker scanners") provided by CMPs and their functionalities;

§4.5 The privileged position of CMPs and their potential collection of data for their own purposes.

4.1 Registration of consent pop-ups

In this section, we address the first research question by evaluating the registration process on CMP websites,

which is the first step that website publisher performs in order to install a given CMP:

– **RQ1.** Do CMPs use ethically and/or legally problematic strategies known as "dark patterns" in the generation process of their consent pop-ups, to influence the publisher in their own interest?

Despite this issue being less related to privacy, we think it is important to highlight as it contributes to the discussion regarding the manipulative role of CMPs. For each step of the registration process, we identify the presence of dark patterns aimed at manipulating website publishers and describe it using the terminology of the state-of-the-art works on dark patterns by Bosch et al. [22] and Mathur et al. [43].

Compliance vs. consent rate. First, we observed that several CMPs claimed that their consent pop-ups are "increasing consent rates." We have found one example of such behavior in our study of the Crownpeak CMP. Fig. 3 shows a screenshot of the Crownpeak commercial website, where this CMP explicitly states that their pop-ups are "Made for Marketers", while the CMPs of their competitors are instead "Made for Compliance/Privacy".

Fig. 4 shows an example from the website of CookiePro, a CMP further studied in our experiments. CookiePro argues that they can "maximize opt-in" and even provide an A/B testing service to compare consent rate between two pop-ups.

Indeed, the objectives of the services offered by these companies can be divided into two categories, depending on their role. The first, which stems from the obligations imposed by the various data protection laws, consists in assisting publishers in their compliance process with these laws. In particular, this involves guaranteeing the compliance of the collection of user consent. The second, which stems from their for-profit purpose and, sometimes, from their experience as digital marketers or data brokers, is to help publishers maximize their income from personalized advertising. These two roles often have antagonistic characteristics, as users refusal can reduce the volume and/or relevance of the data processed for marketing campaigns, and thus the revenues derived from them. It is in the interest of CMPs to use techniques that keep the rate of user consent high, while ensuring the validity of that consent. There is therefore a conflict of interest here that can lead to the use of deceptive designs to try to propose a product that can satisfy both legal and economical requirements, as explained by Santos et al. [6].

Nudging towards paid or logged-in versions. Some CMPs also encourage publishers to sign up for paid plans by using deceptive design techniques. On their pricing page, CookiePro publishes a comparison table [47] with their most expensive plan labelled as "popular". This dark pattern, called *Pressured Selling* by Mathur et al., is based on "defaults or often high-pressure tactics that steer users into purchasing a more expensive version of a product" [43]. CookiePro's website also shows a chatbot with preselected options which can redirect publishers to paid plans by proposing one month free trial coupons [48].

Finally, all studied CMPs except CookiePro Free CMP builder force the publishers to create an account on their platform to be able to access the service. This practice, labelled as *Forced registration* by Bosch et al. [22], consists of restricting access to certain features to registered and logged-in users, even when it is not necessary to provide the service. In the case of CMPs, while this choice may be justified when managing galaxies of websites with several sub-domains and users of various geographical origins, it may be questionable in the case of simple, entry-level services presented as free.

Potential violation of 'specific" consent. When installing Quantcast and filling the contact form on their website [49] with a EU-based country name, the form displays a checkbox with the following statement:

> *"I wish to receive future informational and marketing communications from Quantcast, and I understand and agree to the privacy policy."*

Selecting this checkbox is not mandatory to validate the installation process of Quantcast, however the phrasing is misleading since the user has to agree to receive marketing communications and agree to the privacy policy at the same time. Using a single checkbox for the acceptance of the privacy policy, which is generally mandatory to use a service, and for the subscription to a newsletter, which is optional and requires to consent, may nudge the user toward checking the box, thinking that it is impossible to finalize the request otherwise. From legal perspective, such design raises a potential violation of a legal requirement for *specific consent* that requires separate consent per each specific purpose [3, Art.4(11),6(1)(a)], as described recently by Santos et al. [7, Sec. 5.3].

	Crownpeak Universal Consent Platform	Other Consent Platforms
Made for Marketers	Yes	No: Made for Compliance/Privacy
Automated list of all third-party profiling on your website	Yes	Limited. Only detects and manages cookie-based technologies
Real-time scanning for all first- and third-party technologies on your site, based on real user sessions	Yes	No

Fig. 3. Crownpeak comparative advertisement "Made for Marketers". Source: https://www.crownpeak.com/products/privacy-and-consent-management/, screenshot taken on 23 November 2021.

Fig. 4. CookiePro advertisement about "Consent Rate Optimization" with a trial coupon and A/B testing example. Source: https://app.cookiepro.com/, screenshot taken on 26 November 2021.

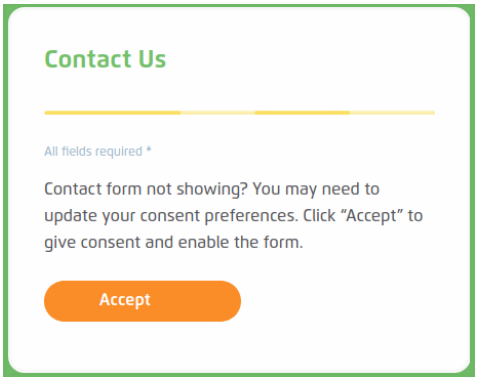

Fig. 5. LiveRamp contact form is not visible without giving a positive consent. Source: https://liveramp.com/contact/, screenshot taken on 24 November 2021.

We studied the registration process of LiveRamp CMP, that is however not included in the further analysis due to lack of installation (see Table 1). When the website publisher tries to access the CMP or create an account on their website, the publisher is presented with a consent pop-up with both "Accept" and "Deny all" options. However, if the visitor decides to deny all processing in the consent pop-up, the contact form [50] is not displayed. Instead, the form is replaced by a message asking for "update [of] consent preferences", as displayed in Figure 5. If the visitor selects the "Accept" option, the contact form displayed but it does not include any option to refuse subscription to automated prospection. After filling the form, the company sends on average two emails per week to the address used to contact them, all seeming to come from the same LiveRamp employee. Since the publisher cannot access the CMP service, create an account, or send a contact message without allowing the CMP to reuse their data for other purposes, this practice constitutes a *tracking wall* design strategy that potentially violates the requirement of *free consent* [3], as explained in 2020 by Santos et al. [7, Sec. 5.2].

4.2 Consent pop-up with default options and its compliance

In this section we study the compliance of the consent pop-ups proposed by various CMPs "by default". To obtain such "default" pop-up and install it on our experimental website, we follow the default options provided by the CMP without any modifications. We then study the following research question:

– **RQ2.** Is a consent pop-up generated with the default options provided by the CMP compliant with EU legal requirements?

We analyzed the ten default consent pop-ups generated by CMPs, and mapped our observations with one most discussed requirement for valid consent from Santos et al. [7, Table 7], called *Balanced choice*. Our goal was not to make an exhaustive evaluation of all consent pop-ups with relation to the 22 requirements listed in this work, but instead to focus on the most critical and important requirement instead. We also detect several practical issues around inclusion of advertising vendors and non-possibility to object to legitimate interest legal basis in the rest of this section.

Compliance on requirement for *Balanced choice*. Several DPAs have stated that users wishing to express their refusal should not encounter a disproportionate obstacle. For example, in the last version of their Guidelines on consent, the French DPA highlight that rejection should present the same level of simplicity that the one of acceptance [51, Art. 2(30)]. Santos et al. call this requirement *Balanced choice*, and give the following interpretation from Art. 7(3) of the GDPR and from publications of DPAs [7, Table 7]:

> *"From Article 7(4) of the GDPR which states that withdrawing consent should be as easy as giving it, we additionally interpret that the choice between "accept" and "reject" [browser-based tracking technologies] must be consequently balanced (or equitable)."*

We found out that six out of ten studied consent pop-ups – Quantcast, Cookiebot free, Cookiebot paid, and Cookie Script Free, Lite, and Plus – showed a difference between the "Accept" and "Reject" button by default, making the "Accept" choice more salient. CookiePro "logged" did not display the "Reject" button by default. Only the "unlogged" version of CookiePro shows in the first layer of its default banner both buttons with the same font, color, and size. However, the second layer of this service places "Allow All" on top of the page, while "Reject All" and "Confirm My Choices" on the bottom, making it hard for end users to reject or customize their preferences (see Fig. 6).

We therefore conclude that almost none of the studied services provide full compliance with the *Balanced choice* requirement and hence are introducing a violation to the *unambiguous consent* requirement [3, Art. 4(11)] and to a requirement that withdrawing consent should be as easy as giving it [3, Art.7(4)].

High number of vendors included by default. In Quantcast Choice, the management of vendors (partners) by the website publisher is made via a different tab of the CMP configuration interface. By default, the whole IAB Europe Global Vendors List is included, representing 751 companies as of 28 May 2021. Publishers can manually revoke them on an opt-out basis. Publishers can add the Google Ad Tech Providers (ATP) list, containing a total of 641 companies at the same date, and also add their own partners with a link to their privacy policy. The complete process is designed to make the inclusion of vendors easy (large number of vendors included by default, addition of Google vendors in one click) while blocking vendors needs to be done manually.

In the "Free CMP Builder" service offered by CookiePro, it is not even possible to customize the list of vendors at all. In the "logged" version of CookiePro free (used with an account), the CMP built by default a consent pop-up with an "Accept" button and no "Reject" on the first page, and an "Allow all" button on the top of the second page. Both lead to a bulk consent and close the pop-up.

On the opposite, Crownpeak Business (a "Premium" service), Cookiebot, CookiePro Standard, and Cookie Script include only the vendors that were found on the website when scanning it, or that were added manually by the publisher.

Delayed update of the vendor's list in the consent pop-up. After the initial configuration of the banner and its installation on the website, a publisher can still include additional trackers. Technically, this action by itself cannot trigger an immediate update of the vendor's list presented to the visitors in the consent pop-up. Depending on the service offered by the CMP, the publisher should either 1) manually add the tracker to the consent pop-up, 2) trigger a manual scan of the website, or 3) wait for the next automatic scan to occur. The first technique implies that a publisher has sufficient technical and legal knowledge of the ecosystem, which is not obvious. The second one is not always available, can have specific limitations (e.g., one scan per day for Cookie Script). The third one is only proposed at large time span (unless the publisher subscribes to additional fees with Cookiebot). Moreover the two first techniques require publishers to take an additional active action, which is unlikely for the least informed ones. This situation can lead to issues such as outdated and incomplete consent pop-ups remaining on websites for several weeks after the addition of new trackers, in violation of the legal requirements for valid consent.

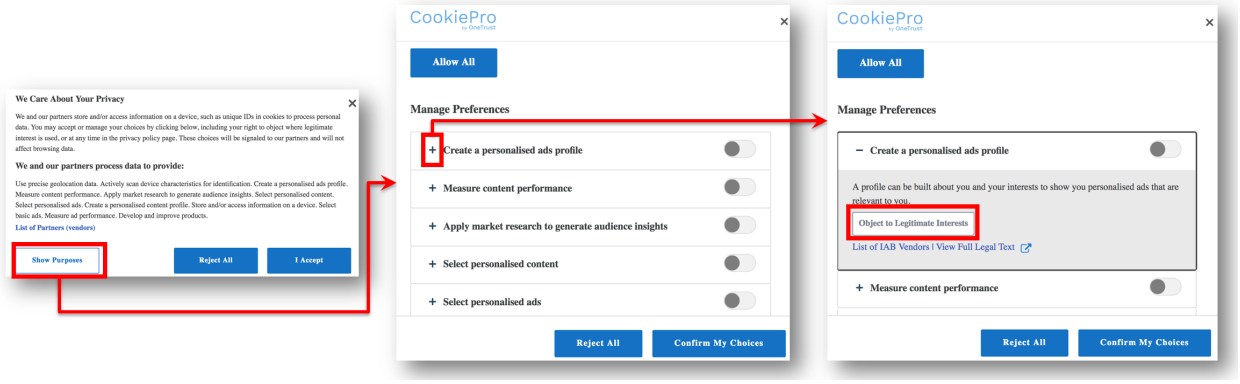

Fig. 6. CookiePro Free CMP builder "unlogged" consent pop-up. Objection to Legitimate Interest is becoming visible only after clicking on the "+" button in the 2^{nd} layer of the consent pop-up interface. Screenshot taken on our experimental domain on 22 November 2021.

Manipulative behaviour restricting objection to legitimate interest-based processing. According to the GDPR, processing of personal data can be performed lawfully only if one of the six *legal basis* of processing applies [3, Article 6(1)]: while the most known legal basis is *consent*, some advertisers rely on the other legal basis, called *legitimate interest*. The rules around application of this legal basis in practice are complex and understudied in the scope of Web applications. In this work, we raise our observations regarding the user interface of the consent pop-ups proposed by default and integration of *legitimate interest* legal basis. Even when the default consent pop-up is compliant with the legal requirements for consent, it can still contain manipulative strategies against the users' right to object to data processing based on the legal basis of *legitimate interest* [3, Art.21].

Fig. 6 shows the free "unlogged" version of CookiePro, where the buttons for objecting legitimate interest-based processing are not visible by default, and the user needs to click on purposes to see them.

Quantcast consent pop-up also contains a problematic design by default. It includes the following text:

> *"With your permission we and our partners may use precise geolocation data and identification through device scanning. You may click to consent to our and our partners' processing as described above. Alternatively you may click to refuse to consent or access more detailed information and change your preferences before consenting. Please note that some processing of your personal data may not require your consent, but you have a right to object to such processing."*

This text does not indicate explicitly that a user who clicks on the "Disagree" button is only refusing to give an explicit consent to the processing based on it, but is not objecting to other processing, based on the legal basis of *legitimate interest*. To completely refuse any processing of her data, the user who wants to object should instead select *More options*, *Legitimate Interest*, and then object to several or all vendors. Therefore, users do not have information by default on how to object to legitimate interest-based processing in the Quantcast consent pop-up.

4.3 Configuration options leading to the deployment of manipulative and/or non-compliant consent pop-ups

In this section, we analyze the options offered by CMPs to configure their consent pop-ups, and we list the ones that can can nudge publishers towards deploying manipulative and/or non-compliant consent pop-ups. We respond to the following research question in this section:

– **RQ3.** Do the default configuration options of consent pop-ups encourage publishers to comply with the requirements for collecting legally valid consent?

Option to create consent wall with reduced service. The Quantcast configuration interface includes a field to add a "Non-consent redirect URL". This option can be used to set up a *consent wall* and *reduced service*, two design strategies described by Gray et al. [24].

A *consent wall* is designed to "block access to the website until the user express their choice regarding consent. This design choice allows a user to select between acceptance and refusal; however, the concrete use of the website is blocked until a choice has been made.". While it is an open question whether *consent wall* violates the

EU law [52], Gray et al. [24] argue that "such as blocking access to a website until a user expresses a choice — will force the user to consent and therefore it possibly violates a *freely given* consent", referring to the Article 7(4) and Recital 43 of the GDPR [3]. This design strategy is also criticized for introducing *obstruction* "in placing visual and interactive barriers between the target of the user's interaction" and the consent pop-up.

Reduced service is a consequence of a choice made by the user in the consent pop-up interface and means "the practice of a website offering reduced functionality – for example, allowing a user access to only limited number of pages on a website – based on their consent configuration options." From a legal perspective, Gray et al. [24] argued that such design strategy could be legally compliant only if "it clearly enables the user to choose between various options of access".

When Quantcast provides the options of *consent wall* and *reduced service* in its consent pop-up configuration, it also provides the following documentation [53]:

> *"Use this if you would like to send a user to an advertising-free version of your site, a minimized content experience, or to a page that explains why consent is important for specific features to function on your site."*

Based on the prior work [24], this configuration option can lead to a potential violation of the requirement for *freely given consent* [3, Art.7(4)]. Moreover, if the website publisher does not provide reject option, then such practice may constitute *tracking wall* (a consent wall that gives only one option: to consent and accept any terms offered by the website) recognized as unlawful by the majority of regulators and Data Protection Authorities in the EU [24, Sec. 4.1].

4.4 Problems in the configuration process involving a tracker scanner

In this section we study the "tracker scanner" functionality provided by CMPs. Tracker scanner allows website publishers to automatically detect trackers on their websites, and sometimes even to evaluate the overall compliance of their websites. Some scanners even propose automatic updates to the consent pop-up interface, taking into account the detected trackers and their purposes. While it is a very complex task to evaluate effectiveness of tracker scanners at scale because (1) such scanner tools are not open-sourced; (2) there is a lack of testing websites with all potential trackers integrated.

Therefore, we analyse the tracker scanner service provided by the CMPs on our empty website. An *honest scanner* should detect no tracking since our website does not contain any content. With this experiment, we aim at answering the following research question:

– **RQ4.** What are the functionalities and the impacts of tracker scanners provided by CMPs, regarding legal compliance, role of CMPs, and publishers behaviour?

We found out that four CMPs — CookiePro, Cookiebot, Crownpeak, and Cookie Script — propose tracker scanners. These scanners show notable differences regarding both their appearance and functionalities. The main observations are summarized in Table 3.

Scanners providing only a basic report. The CookieBot scanner allows to create a free account, but the scanning functionality is then limited to five pages per website. It sends the scan report as a HTML file by email. The information given is short and basic: date, domain name, server location, number of cookies found, detailed list by category (e.g. "Necessary"). The detailed view of a cookie contains only basic information: cookie name, provider, purpose (e.g. "Stores the user's cookie consent state for the current domain"), initiator (e.g. "Script tag"), destination of data, and evaluation of the adequacy of the international data transfer under the GDPR. The report does not provide detailed information about the vendors, nor does it make any suggestion for actions. Strangely, we noticed that the cookie for storing consent registered by CookieBot is included in the scanner report (and categorized as *Necessary*), even if we tested an empty website without any pop-up – CookieBot automatically assumes that we will install their pop-up on our website.

Scanners inciting publishers to subscribe to paid plans. The CookiePro unlogged scanner is proposed directly from the home page of the CMP [48]. The categorization is made by matching the cookies found with the Cookiepedia database (also owned by OneTrust). In order to perform an analysis, the publisher needs to fill a form with a name, an email address, and the URL of the website to scan. CookiePro scanner displays an overview of its finding in the browser, and sends the report by email as a PDF file. The first overview contains four sections: (1) a summary of the website, with the number of pages and the number of cookies found, (2) a *Privacy checklist* which indicates if the scanner was able to find a consent pop-up, cookie policy, and pri-

CMP	Service	Needs account	Gives report	Gives advices	Auto. updates purposes in pop-up	Auto. updates vendors in pop-up	Auto. updates cookie/privacy policy
CookiePro	Free unlogged	No (*)	✓	✓	×	×	×
	Free account	Yes	✓	✓	✓	✓	✓
	Standard account	Yes	✓	✓	✓	✓	✓
Cookiebot	Free	No (**)	✓	×	✓	✓	×
	Paid	Yes	✓	×	✓	✓	✓
Crownpeak	Business	Yes	×	×	✓	✓	×
Cookie Script	Free	No	✓	×	✓	✓	×
	Lite	Yes	✓	×	✓	✓	✓
	Plus	Yes	✓	×	✓	✓	✓

Table 3. Comparison table of tracker scanners' functionalities. (*) Name and email required (**) Email required but not stored

vacy policy, (3) a suggestion of paid plans and options, and (4) a detailed list of the cookies found (when applicable). The CookiePro's detailed PDF report contains the number and list of cookies, tags, forms, and webpages found, analyzed and sorted by categories such as first/third party, session/persistent, web object types, and cookie purposes. It also includes an analysis of the CMP with "Recommended actions".

Nevertheless, and despite our webpage being absolutely empty (no cookie, script, tag, or form), the CookiePro scanner still labels our empty website as *"High Risk"* because it doesn't find any privacy or cookie notice, nor any consent pop-up. It appears that the scanner tool *is not able to adapt to a website without cookies or other trackers*! The scanner makes scary misleading statements such as ''*Our scan reveals a particularly high risk with respect to with European ePrivacy Laws, which have requirements for transparency and consent related to the types of cookies you have on your site.*". In consequence, the scanner is nudging the website publisher to "contact legal advice" and "scan [our] site on a regular basis".

With the free version of Cookiebot, the drop-down list titled "scanning frequency" is present but is disabled (greyed). Only the default frequency (monthly scan) is visible. On the premium version of the same service, the list is activated, and the scanning frequency can be changed from monthly to daily, however this change is charged an additional €62 per month. Since the box is visible to publishers in the free version of the CMP, but the price of the additional feature is not visible until they have access to the premium version, this can lead publishers to subscribe to the premium plan first, thinking they will have access to highest levels of scan frequencies, and then to subscribe to the additional feature when they realize it is not included. This form of dark pattern is known as *Hidden Costs* [28, 42, 43].

CookiePro often provides "Free trial coupons" on their website and via their commercial emails. However, using this coupon for subscription requires providing credit card details, and giving authorization to the CMP to *"automatically charge this payment method whenever a subscription is associated with it"*. This dark pattern has been identified by Brignull as *Forced continuity* [42].

Delayed scan results. Finally, with Cookie Script, the scan is triggered by default when configuring the consent pop-up, and before the installation of the pop-up on the website. However, the scan report is displayed only some minutes later, and does not include the cookie set by the CMP itself, nor informs about its presence. In consequence, if the publisher does not launch a manual scan, they could install the consent pop-up without knowing anything about this cookie before the next automatic scheduled scan, which will happen one month later. However, nothing indicates that it has any tracking role. After scanning a website, the tool redirects to a report page prompting to *"Add cookie compliance"* with an exclamation mark, even if no cookie was detected on our empty website. Since our website does not include trackers, the usage of a consent pop-up is not mandatory and such solicitation, like in case of CookiePro, is not needed. Cookie Script also adds a link to the report in the consent pop-up, introducing confusion to the website visitors who might believe that the visited (empty) website contains trackers.

Regarding the detection process, we can therefore conclude that CookiePro and Cookie Script are not mentioning the presence of any cookie on our empty website, while Cookiebot mention its own consent cookie, assuming that we will install their banner.

4.5 CMP abusing its position to collect data for its own use

In this section we monitor the resulting empty web site (one per CMP service, as described in Table 2) that includes the CMP consent pop-up. Our goal is to assess if this integrated consent pop-up content could be leveraged to collect data for the CMP own use, and whether some CMPs exploit their privileged position to actually collect data for their own use. We therefore aim at answering the following research question:

– **RQ5.** Are CMPs abusing their central and privileged position and their presence on a large number of websites to collect data for their own use?

Case of Quantcast Choice. When a page including *Quantcast universal tag*, the Javascript code provided by Quantcast to provide Quantcast Choice CMP, is loaded by a browser, it sends 10 distinct third-party requests, aiming to 6 different subdomains. At the time of our first tests in April 2021, the requests to `edge.quantserve.com`, `pixel.quantserve.com` and `rules.quantcount.com` were even insecure (HTTP), despite the website being accessed in HTTPS. These different requests load content in the form of Javascript code hosted on CMP's managed domains. The most important part is the `choice.js` script, which controls the display of the consent pop-up and loads other parts.

We first tested the Quantcast Choice service in January 2021: this service loads the `choice.js` script that further sends a request to `pixel.quantserve.com` to fetch a 1x1 gif image. Upon loading this image, `pixel.quantserve.com` sets a third-party cookie named `mc` with a random value, that is different across our session and private Firefox container, indicating that such cookie is *user-specific* (see the details of detection of such cookies in the description of Ernie extension we used for these experiments [38]). This cookie have an expiry time of one year. Notice that this tracking pixel was integrated *by default* in all Quantcast Choice banners *even before the user makes a decision regarding acceptance or refusal of consent in the pop-up interface*! This finding confirms the behaviour reported by Santos et al. [6]. The requests to these Quantcast servers are also flagged as tracking by tracking filter lists such as Disconnect [1].

After an update on March 5th, 2021, the behaviour of the `choice.js` script has changed: the request for 1x1 invisible pixel to `pixel.quantcount.com` does not set a tracking cookie anymore *unless the user gives a positive consent*, If the user does not consent, no `mc` cookie is set in the browser. If this new behavior fixes a major compliance issue (that is, tracking before consent), it also demonstrates the ability of CMPs to include content unrelated to consent management at any time, and without informing nor giving the publisher a possibility to oppose.

Notice that the Quantcast Choice today includes the tracking cookie (after user's consent) on an otherwise empty website without properly informing the website publisher. We have found only one possible explanation for the presence of this tracking technique in the consent pop-up: Quantcast merged the "Count and Measure" services in the "Universal Tag", as explained in Quantcast documentation [54]:

> *"The Universal Tag includes both Quantcast Choice & Quantcast Measure, our audience insights and analytics tool. This enables us to provide Quantcast Choice for free to all users and makes implementation of the combined tag easier."*

To conclude, even if it is possible that the `mc` cookie attached to the request made to `pixel.quantserve.com` is a part of Quantcast measure service, the CMP does not disclose any other information about this cookie in its privacy policy [55].

Case of Cookie Script Free. With Cookie Script free, the banner itself does not include any tracking request. However, it does include a link to the page of the last scan report ran on the website, previously described in Section 4.4. The tracker scan page includes a *Google Analytics* service, as well as social sharing buttons, all of which generating a total of 41 third-party requests and the deposit of 6 cookies without the user's prior consent according to Firefox developer tools. 16 of these requests are flagged as related to "known trackers" in the Disconnect list. Details are listed in Table 5, Appendix A.1.

5 Discussion

5.1 Main outcomes

In this section we discuss our findings (summarized in Table 4) and the situation in general.

1 https://github.com/disconnectme/disconnect-tracking-protection/blob/21134d05e7a407739d7db0b695cbbf359afffdd2/services.json#L5646

CMP	Service	Consent optimisation	Incitation to pay	Unspecific cons.	Unbalanced choice	Include all vendors	Delayed list update	Restrict objection	Redirect option	Tracking
Related sections		4.1	4.1/4.4	4.1	4.2	4.2	4.2	4.2	4.3	4.5
CookiePro by OneTrust	Free CMP builder					×				
	Free Account	×	×			×				
	Standard Account	×	×							
Quantcast	Choice			×	×	×		×	×	×
Cookiebot	Free				×					
	Premium Small				×					
Crownpeak	Business	×								
Cookie Script	Free		×		×		×			
	Lite		×		×		×			
	Plus		×		×		×			

Table 4. Summary of issues found in tested services. Identified problems are marked with × .

Related work has shown that end-users are highly susceptible to manipulation by dark patterns [21, 43]. They also showed the important role that CMPs have, at the crossroads of the digital advertising ecosystem [6]. Our work goes further by analysing the whole consent pop-up system, including the relationships between CMPs and website publishers. In a context where law and technology are rapidly evolving, these CMPs are trying to position themselves as privacy compliance experts. However, the reality is much more subtle.

First of all, we observed that CMPs often do not help improving user's privacy when visiting a website. On the one hand, *user consent is often wide, non-informed, and subject to manipulation.* More precisely, Quantcast and CookiePro tend to propose to the publishers by default the entire Global Vendors List provided by the IAB Europe, which contained 751 companies end of May 2021, potentially complemented with the Google Ad Tech Providers (ATP) list that is almost the same size. In their turn, the publishers, in particular when they rely on default settings, present the same list to the users, with several hundreds of companies. So if a user agrees, she explicitly accepts her personal data to be exchanged among hundreds of companies, instead of being limited to those present on the visited website. Then a user cannot comprehend such a long list, and Veale and Borgesius [56] have demonstrated that the "informed choice" requirement cannot be fully met in these circumstances, which theoretically voids the user consent. On the opposite, by default, the services of Cookiebot, Crownpeak, and Cookie Script do not include the whole list of vendors but instead customize it automatically by using the results of a scan, which clearly benefits to the end user.

In addition, many CMPs present themselves as being able to help publishers increase the consent rate of their web site visitors, which raises questions about the very function of consent pop-ups. Indeed, it implicitly validates that the purpose of these pop-ups is ultimately more about "extracting" positive consent than letting users make a free and informed choice.

On the other hand, *CMPs consent pop-ups can create additional privacy and security issues.* Our methodology involves creating an empty website that does not include any tracking tool. However, by adding a consent pop-up, we found analytics tools – presented as meant to provide statistics on consent rates – in Quantcast, and in a scan report page made available by Cookie Script – presented as meant to monitor views of the scan report page. This finding indicates that CMPs may actively participate in the overall rise of user tracking on the web. Then, the addition of a consent pop-up in a web site requires dynamically loading third-party scripts, which mechanically gives a lot of power to the CMPs as owner of the scripts. For instance, the CMP may add or remove a tracking tool at its own discretion (as we observed with Quantcast), and it is not clear whether the publisher would be either informed or able to refuse. The system could also be diverted by an attacker who may add a malicious script in the publisher's website. This situation raises privacy and security risks.

Secondly, CMPs themselves often use deceptive design schemes towards publishers, to entice them to subscribe to their paid plans. This happens even when the publishers do not include tracking content on their websites, and therefore do not formally require to include a consent pop-up. For example, the tracker scanner result can include messages such as "High Risk" CookiePro or "Add Compliance" Cook-

ieScript when it does not find a consent pop-up or privacy policy, sometimes even on a systematic basis. The CMPs also use iconography and color-code to play on the fear of non-compliance. Of course, a possible explanation for this behavior may come from their (presupposed) business model. They are private, for profit companies, whose existence directly depends on their ability to convince their clients, the publishers, of the need to subscribe to their paid offers. They may also be themselves linked to advertising/marketing groups (e.g., Quantcast), or data brokers (e.g., LiveRamp, new name of Acxiom Corporation, after purchasing the LiveRamp company).

Thirdly, CMPs should probably be considered as data controllers. The present work reinforces the findings of Santos et al. [6] by providing additional arguments to qualify CMPs as data controllers. For instance, this becomes obvious when considering a CMP manipulating the website publisher during various steps in the configuration process, or by recommending the publisher to include a consent pop-up in an empty website where it could be omitted, or by generating non compliant default consent pop-ups.

5.2 Recommendations

Despite the fact that CMPs are positioning themselves as compliance specialists, website publishers should keep a critical eye on the consent collection process. Indeed, they remain data controllers under the GDPR.

Regulators also have a major role. They can provide guidelines and recommendations to highlight good practices, as did the CNIL French DPA in [40, 41, 44]. They can illustrate them with examples of "do and don't" designs [57], and help publishers and CMPs to implement infrastructures to manage user choices that follow state-of-the-art legal and ethical recommendations.

5.3 Consent pop-ups beyond third-party cookie era

On their websites, several CMPs (OneTrust, Quantcast, LiveRamp) insist on the importance of preparing for the post third-party cookie era. This is a consequence of the use of blocking tools by end users, and the fact third-party cookies are increasingly blocked by default by web browsers (Apple/Safari in 2017, Mozilla/Firefox in 2019, potentially Google/Chrome in 2024). Consequently, "Cookie banners" have evolved to more generic "consent pop-ups" meant to inform users and collect their consent, regardless of the tracking technique in use.

CMPs and Ad Tech companies are working on alternatives: some of them already rely on CNAME cloaking ([58] explains that 9.98% of the top 10,000 websites rely on it in 2021); others (e.g., OneTrust, LiveRamp, Quantcast, Google) develop such alternatives as Server Side Tagging, Single Sign-On, or persistent identification [59–62]. IP-based tracking [63] and fingerprinting scripts [64] can also be used with first-party cookies to target non registered users who block or delete cookies. In their February 2021 report [59], the IAB Europe explores "Identity solutions" such as email-based Customer Relationship Management.

Such data is then aggregated in large databases, in a pseudonymized manner, often after hashing the user email address [59, 65]. Of course, this pseudonymization approach enables persistent, cross-device, and cross-site tracking, to the benefit of data brokers such as LiveRamp and their partners [65].

From a privacy viewpoint, in the long run, end users may lose visibility and have less control with this evolution, because an increasing part of the tracking process will happen directly on server side, and it is no longer a matter of storing or removing a cookie in the user's web browser, which is easily viewable. In any case, consent pop-ups are still legally required, the proof of valid consent being needed regardless of the tracking technique in use as reminded by the French DPA in [66].

6 Conclusion

In our work, we systematically studied the installation and configuration process of consent pop-ups and their potential effects on the decision making of the website publishers. We made an in-depth analysis of the configuration process from ten services provided by five popular CMP companies and identify common deceptive strategies employed.

By analysing CMP services on an empty experimental website, we identified manipulation of website publishers towards subscription to the CMPs paid plans and then detected that default consent pop-ups often violate the law. We have also shown that configuration options may lead to non-compliance, while tracking scanners offered by CMPs manipulate publishers. Finally, we identified a CMP that abuses its position to include an additional pixel, flagged as tracker, to the consent pop-up.

Our findings demonstrate the importance of CMPs and we raise concerns around the privileged position of CMPs and their manipulative strategies versus website publishers. Finally, we open a discussion for regulators and policy makers to analyse the behavior, incentives and manipulative strategies of CMPs that affect thousands of websites and millions of end users via the design and configuration options proposed to the publishers.

7 Acknowledgments

This work was supported by the ANR JCJC project PrivaWeb (ANR-18-CE39-0008) and the H2020 SPARTA Cybersecurity Competence Network project.

We would like to thank the reviewers for their helpful comments, Vera Wesselkamp for her assistance with the ERNIE extension, Jean-François Scariot for his technical support, Cristiana Santos for providing useful legal resources, and Midas Nouwens for his help regarding the analysis of CMPs' plans.

References

[1] The European Parliament and the Council of the European Union, "Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)," 2002, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058, accessed 29 March 2021.

[2] "Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009," https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009L0136, accessed on 20 Apr 2021.

[3] "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679.

[4] M. Degeling, C. Utz, C. Lentzsch, H. Hosseini, F. Schaub, and T. Holz, "We value your privacy ... now take some cookies: Measuring the gdpr's impact on web privacy," *Network and Distributed Systems Security Symposium*, 2019.

[5] C. Matte, N. Bielova, and C. Santos, "Do cookie banners respect my choice? : Measuring legal compliance of banners from IAB europe's transparency and consent framework," in *IEEE Symposium on Security and Privacy*, 2020, pp. 791–809.

[6] C. Santos, M. Nouwens, M. Toth, N. Bielova, and V. Roca, "Consent management platforms under the GDPR: processors and/or controllers?" in *Annual Privacy Forum (APF'21)*, vol. 12703, 2021, pp. 47–69.

[7] C. Santos, N. Bielova, and C. Matte, "Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners," *Technology and Regulation*, pp. 91–135, 2020. [Online]. Available: https://doi.org/10.26116/techreg.2020.009

[8] "Judgment in Case C-673/17 Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v Planet49 GmbH," 2019, http://curia.europa.eu/juris/documents.jsf?num=C-673/17.

[9] "AP: veel websites vragen op onjuiste wijze toestemming voor plaatsen tracking cookies," 2019, gDPRHub: https://gdprhub.eu/index.php?title=AP_-_Consent_to_place_cookies, original source (in NL): https://autoriteitpersoonsgegevens.nl/nl/nieuws/ap-veel-websites-vragen-op-onjuiste-wijze-toestemming-voor-plaatsen-tracking-cookies, accessed on 30 May 2021.

[10] "Procedimiento No: PS/00264/2020, RESOLUCION DE PROCEDIMIENTO SANCIONADOR." 2021, gDPRHub: https://gdprhub.eu/index.php?title=AEPD_-_PS/00264/2020, original source (in ES): https://www.aepd.es/es/documento/ps-00264-2020.pdf, accessed on 30 May 2021.

[11] "Datatilsynet - 2020-31-3354," 2020, gDPRHub: https://gdprhub.eu/index.php?title=Datatilsynet_-_2020-31-3354, original source (in DA): https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2020/nov/ugyldigt-samtykke-paa-hjemmeside, accessed on 30 May 2021.

[12] Commission Nationale Informatique et Libertés (CNIL), "Cookies: GOOGLE fined 150 million euros," 2021, https://www.cnil.fr/en/cookies-google-fined-150-million-euros.

[13] ——, "Cookies: FACEBOOK IRELAND LIMITED fined 60 million euros," 2021, https://www.cnil.fr/en/cookies-facebook-ireland-limited-fined-60-million-euros.

[14] ——, "Cookies: penalty of 50,000 euros against SOCIETE DU FIGARO," 2021, https://www.cnil.fr/en/cookies-penalty-50000-euros-against-societe-du-figaro.

[15] ——, "Cookies: financial penalty of 35 million euros imposed on the company AMAZON EUROPE CORE," 2020, https://www.cnil.fr/en/cookies-financial-penalty-35-million-euros-imposed-company-amazon-europe-core.

[16] "Cookies equally easily accepted or refused: CNIL orders 20 organisations to comply," 2021, https://www.cnil.fr/en/cookies-equally-easily-accepted-or-refused-cnil-orders-20-organisations-comply.

[17] M. Hils, D. W. Woods, and R. Böhme, "Measuring the emergence of consent management on the web," in *Proceedings of the ACM Internet Measurement Conference*, 2020, pp. 317–332.

[18] M. Nouwens, I. Liccardi, M. Veale, D. Karger, and L. Kagal, "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence," in *CHI*, 2020.

[19] C. Matte, C. Santos, and N. Bielova, "Purposes in IAB Europe's TCF: which legal basis and how are they used by advertisers?" in *Annual Privacy Forum, APF*, ser. Lecture Notes in Computer Science, 2020, https://hal.inria.fr/hal-02566891.

[20] IAB Europe, "IAB Website," https://iabeurope.eu/transparency-consent-framework/, accessed on 20 Apr 2021.

[21] C. Utz, M. Degeling, S. Fahl, F. Schaub, and T. Holz, "(Un)informed Consent: Studying GDPR Consent Notices in the Field," in *ACM Conference on Computer and Communications Security*, 2019, pp. 973–990.

[22] C. Bösch, B. Erb, F. Kargl, H. Kopp, and S. Pfattheicher, "Tales from the dark side: Privacy dark strategies and privacy dark patterns," in *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2016, pp. 237–254.

[23] J. Luguri and L. Strahilevitz, "Shining a Light on Dark Patterns," *13 Journal of Legal Analysis 43*, 2021, university of Chicago Coase-Sandor Institute for Law & Economics Research Paper No. 879, U of Chicago, Public Law Working Paper No. 719, Available at SSRN: https://ssrn.com/abstract=3431205 or http://dx.doi.org/10.2139/ssrn.3431205.

[24] C. M. Gray, C. Santos, N. Bielova, M. Toth, and D. Clifford, "Dark patterns and the legal requirements of consent banners: An interaction criticism perspective," in *ACM Conference on Human Factors in Computing Systems (ACM CHI)*, 2021, pp. 172:1–172:18.

[25] A. Mathur, M. Kshirsagar, and J. R. Mayer, "What makes a dark pattern... dark?: Design attributes, normative considerations, and measurement methods," in *CHI*, 2021, pp. 360:1–360:18.

[26] Kevel (formerly Adzerk), "About us," n.d., https://www.kevel.co/about/ [Consulted on 29 April 2021].

[27] H. Brignull, "Dark patterns: User interfaces designed to trick people," 2014, http://talks.ui-patterns.com/videos/dark-patterns-user-interfaces-designed-to-trick-people.

[28] C. M. Gray, Y. Kou, B. Battles, J. Hoggatt, and A. L. Toombs, "The dark (patterns) side of UX design," in *Proceedings of the CHI Conference Human Factors in Computing Systems*, 2018, p. 534.

[29] M. Chromik, M. Eiband, S. T. Völkel, and D. Buschek, "Dark Patterns of Explainability, Transparency, and User Control for Intelligent Systems," in *Intelligent User Interfaces Workshops*, ser. CEUR Workshop Proceedings, vol. 2327, 2019.

[30] D. Machuletz and R. Böhme, "Multiple purposes, multiple problems: A user study of consent dialogs after GDPR," in *Proceedings on Privacy Enhancing Technologies*, vol. 2020, no. 2, 2020, pp. 481–498.

[31] T. H. Soe, O. E. Nordberg, F. Guribye, and M. Slavkovik, "Circumvention by design – dark patterns in cookie consent for online news outlets," in *NordiCHI*, 2020, pp. 19:1–19:12.

[32] Kevel (formerly Adzerk), "Consent Management Platform (CMP) 2021 Tracker," n.d., https://www.kevel.co/cmp/ [Consulted on 11 February 2021].

[33] LiveRamp, "LiveRamp | Data Connectivity Platform," https://liveramp.com/, [accessed on 20 May 2021].

[34] Liveramp, "Acxiom Marketing Solutions Sale Now Complete," 2018, https://investors.liveramp.com/news-and-events/press-release-details/2018/Acxiom-Marketing-Solutions-Sale-Now-Complete/default.aspx.

[35] Cookie Script, "Cookie-Script: GDPR | CCPA | ePR cookie compliance solution," https://cookie-script.com/, [accessed on 20 May 2021].

[36] Quantcast, "Quantcast Choice Supports TCF v2.0; Leading Consent Management Platform Now Offers Full Range of Premium Features in Free Solution," n.d., https://www.quantcast.com/about-us/press/press-release/quantcast-choice-supports-tcf-v2/ [Accessed on 20 May 2021].

[37] Mozilla Corporation, "Dedicated profiles per Firefox installation," https://support.mozilla.org/en-US/kb/profile-manager-create-remove-switch-firefox-profiles, [accessed on 20 May 2021].

[38] V. Wesselkamp, I. Fouad, C. Santos, Y. Boussad, N. Bielova, and A. Legout, "In-depth technical and legal analysis of tracking on health related websites with ERNIE extension," in *Proceedings of the 20th Workshop on Privacy in the Electronic Society (WPES)*, 2021, pp. 151–166.

[39] I. Fouad, N. Bielova, A. Legout, and N. Sarafijanovic-Djukic, "Missed by filter lists: Detecting unknown third-party trackers with invisible pixels," in *Proceedings on Privacy Enhancing Technologies (PoPETs)*, no. 2, 2020, pp. 499–518.

[40] Commission Nationale Informatique et Libertés (CNIL), "Nouvelles règles pour les cookies et autres traceurs : bilan de l'accompagnement de la CNIL et actions à venir," 2021, https://www.cnil.fr/fr/nouvelles-regles-cookies-et-autres-traceurs-bilan-accompagnement-cnil-actions-a-venir.

[41] ——, "Délibération No 2020-092 du 17 septembre 2020 portant adoption d'une recommandation proposant des modalités pratiques de mise en conformité en cas de recours aux « cookies et autres traceurs »," 2020, https://www.cnil.fr/sites/default/files/atoms/files/recommandation-cookies-et-autres-traceurs.pdf.

[42] H. Brignull, "Dark patterns," 2018, https://www.darkpatterns.org.

[43] A. Mathur, G. Acar, M. Friedman, E. Lucherini, J. R. Mayer, M. Chetty, and A. Narayanan, "Dark patterns at scale: Findings from a crawl of 11k shopping websites," *Proceedings of the ACM Human-Computer Interaction*, vol. 3, 2019.

[44] Commission Nationale Informatique et Libertés (CNIL), "On the practical procedures for collecting the consent provided for in article 82 of the french data protection act, concerning operations of storing or gaining access to information in the terminal equipment of a user (recommendation "cookies and other trackers")," https://www.cnil.fr/sites/default/files/atoms/files/draft_recommendation_cookies_and_other_trackers_en.pdf.

[45] IAB Europe, "TCF v2.0 CMP Service List," 2021, https://iabeurope.eu/cmp-list/.

[46] ——, "Vendor List TCF v2.0," 2020, https://iabeurope.eu/vendor-list-tcf-v2-0/.

[47] CookiePro by OneTrust, "Simple Pricing," n.d., https://www.cookiepro.com/pricing/ [Consulted on 27 April 2021].

[48] ——, "CookiePro," n.d., https://www.cookiepro.com/ [Consulted on 5 March 2021].

[49] Quantcast, ""Contact us" form," n.d., https://www.quantcast.com/#contact [Consulted on 6 April 2021].

[50] Liveramp, ""Talk to an Expert" form," n.d., https://liveramp.com/contact [Consulted on 6 April 2021].

[51] Commission Nationale Informatique et Libertés (CNIL), "Délibération No 2020-091 du 17 septembre 2020 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur (notamment aux « cookies et autres traceurs ») et abrogeant la délibération No 2019-093 du 4 juillet 2019," 2020, https://www.cnil.

fr/sites/default/files/atoms/files/lignes_directrices_de_la_cnil_sur_les_cookies_et_autres_traceurs.pdf.
[52] noyb, "News Sites: Readers need to "buy back" their own data at an exorbitant price," 2021, https://noyb.eu/en/news-sites-readers-need-buy-back-their-own-data-exorbitant-price [Consulted on 26 Nov. 2021].
[53] Quantcast, "Quantcast Choice – User Guide," Apr 2021, https://help.quantcast.com/hc/en-us/articles/360052725133-Quantcast-Choice-User-Guide [Consulted on 30 May 2021].
[54] ——, "Quantcast Choice - Universal Tag Implementation Guide (TCF v2)," 2021, https://help.quantcast.com/hc/en-us/articles/360052746173-Quantcast-Choice-Universal-Tag-Implementation-Guide-TCF-v2-.
[55] Quantcast, "Privacy Policy," 2020, https://www.quantcast.com/privacy/.
[56] M. Veale and F. Z. Borgesius, "Ad tech and Real-Time Bidding under European Data Protection Law," *German Law Journal*, 2021.
[57] Commission Nationale Informatique et Libertés (CNIL), "Data & Design by LINC-CNIL: Co-building user journeys compliant with the GDPR and respectful of privacy," https://design.cnil.fr/en/.
[58] Y. Dimova, G. Acar, L. Olejnik, W. Joosen, and T. V. Goethem, "The CNAME of the game: Large-scale analysis of DNS-based tracking evasion," in *Proceedings on Privacy Enhancing Technologies*, vol. 2021, 2021, pp. 394–412, https://www.sciendo.com/article/10.2478/popets-2021-0053.
[59] Lauren Wakefield and Helen Mussard, "A Guide to the Post Third-Party Cookie Era," IAB Europe, Tech. Rep., Feb 2021, https://iabeurope.eu/knowledge-hub/iab-europe-guide-to-the-post-third-party-cookie-era-updated-in-february-2020/.
[60] Heinz Baumann, "Our view on a post-cookie world and identity," Feb 2021, https://www.quantcast.com/blog/our-view-on-a-post-cookie-world-and-identity/.
[61] The Trade Desk, "What the Tech is Unified ID 2.0?" Feb 2021, https://www.thetradedesk.com/us/news/what-the-tech-is-unified-id-2-0.
[62] Bruce Biegel and Charles Ping, "Collaborative Data Solutions: The Evolution of Identity in a Privacy-First, Post-Cookie World," Jan 2021, https://liveramp.com/lp/eb/collaborative-data-solutions-evolution-identity-privacy-first-post-cookie-world-eb-ty/.
[63] V. Mishra, P. Laperdrix, A. Vastel, W. Rudametkin, R. Rouvoy, and M. Lopatka, "Don't count me out: On the relevance of IP address in the tracking ecosystem," in *ACM International World Wide Web Conference (WWW'20)*, 2020, pp. 808–815.
[64] A. Gómez-Boix, P. Laperdrix, and B. Baudry, "Hiding in the Crowd: an Analysis of the Effectiveness of Browser Fingerprinting at Large Scale," in *International World Wide Web Conference*, 2018, pp. 1–10, https://hal.inria.fr/hal-01718234.
[65] Criteo, "Identity Resolution & Criteo Shopper Graph Investor Presentation," 2019, https://criteo.investorroom.com/download/December+2019_Criteo+Shopper+Graph.pdf [Consulted on 30 Sept. 2021].
[66] CNIL, "Alternatives aux cookies tiers : quelles conséquences en matière de consentement ?" 2021, https://www.cnil.fr/fr/alternatives-aux-cookies-tiers-quelles-consequences-en-matiere-de-consentement.

A Appendix

A.1 HTTPS requests in the Cookie Script Free scanning report

Table 5 lists the HTTPS requests observed when visiting the Cookie Script scanning report website by following the link present in the consent pop-up. See Section 4.5 for the associated discussion.

#	Domain	File	Initiator	Tracker
1	cookie-script.com	css-99b62-55873.css	stylesheet	
2	cookie-script.com	cookie.svg	img	
3	cookie-script.com	css-b3740-22058.css	stylesheet	
4	cookie-script.com	text.svg	img	
5	static.mailerlite.com	webforms.min.js?v4a60e9ef938a7fa0240ac9ba567062cb	script	
6	cookie-script.com	js-cF177-34068.js	script	
7	cookie-script.com	helpscout.js	script	
8	cookie-script.com	css-079a7-66634.css	stylesheet	
9	www.googletagmanager.com	gtm.js?id=GTM-WZXWWWM	cookie-report:31 (script)	
10	static.mailerlite.com	ml_jQuery.inputmask.bundle.minjs?v3.3.1	webforms.min.js:1 (script)	
11	cookie-script.com	fb.svg	img	
12	cookie-script.com	tw.svg	img	
13	cookie-script.com	ig.svg	img	
14	cookie-script.com	footerarrow.svg	img	
15	cookie-script.com	fontawesome-webfont.woff2?v=4.6.3	font	
16	cookie-script.com	favicon.ico	img	
17	**platform-api.sharethis.com**	**sharethis.js**	**script**	**Yes**
18	cookie-script.com	apple-touch-icon.png	FaviconLoader.jsm:191 (img)	
19	cookie-script.com	favicon-16x16.png	FaviconLoader.jsm:191 (img)	
20	cookie-script.com	en.svg	js-cf177-34068.js:30 (lazy-img)	
21	**l.sharethis.com**	**pview?event=pview&hostname=cookie-script.com&location=/cookie-report&product=inline-share-buttons&url=https://cookie-script.com/cookie-report?identifier=Fa78 1 fc6540325F7b8c6bc93**	**sharethis.js:3297 (xhr)**	**Yes**
22	**www.google-analytics.com**	**analytics.js**	**gtmjs:36 (script)**	**Yes**
23	**buttons-config.sharethis.com**	**5e106537dd527900136b1728.js**	**sharethis.js:669 (script)**	**Yes**
24	**www.google-analytics.com**	**collect?v=1& _v=j96&a=1755241340&t=pageview &_s=1&dl=https://cookie-script.com/cookie-report?identifier=Fa7811fc6540325F7b8cébc93b5a7d9dc &ul=en-us&de=UTF-8&dt=Cookie report fc**	**analytics.js:44 (xhr)**	**Yes**
25	**platform-cdn.sharethis.com**	**skype.svg**	**sharethis.js:4501 (img)**	**Yes**
26	**platform-cdn.sharethis.com**	**facebook.svg**	**sharethis.js:4501 (img)**	**Yes**
27	**platform-cdn.sharethis.com**	**twitter.svg**	**sharethis.js:4501 (img)**	**Yes**
28	**platform-cdn.sharethis.com**	**pinterest.svg**	**sharethis.js:4501 (img)**	**Yes**
29	**platform-cdn.sharethis.com**	**whatsapp.svg**	**sharethis.js:4501 (img)**	**Yes**
30	**platform-cdn.sharethis.com**	**email.svg**	**sharethis.js:4501 (img)**	**Yes**
31	**platform-cdn.sharethis.com**	**messenger.svg**	**sharethis.js:4501 (img)**	**Yes**
32	**platform-cdn.sharethis.com**	**print.svg**	**sharethis.js:4501 (img)**	**Yes**
33	**platform-cdn.sharethis.com**	**gmail.svg**	**sharethis.js:4501 (img)**	**Yes**
34	**platform-cdn.sharethis.com**	**reddit.svg**	**sharethis.js:4501 (img)**	**Yes**
35	**platform-cdn.sharethis.com**	**linkedin.svg**	**sharethis.js:4501 (img)**	**Yes**
36	beacon-v2.helpscout.net	/	helpscout.js:5 (script)	
37	beacon-v2.helpscout.net	vendor.571a2921.js	1:1 (script)	
38	beacon-v2.helpscout.net	main.c78fc066.js	1:1 (script)	
39	d3hb14vkzrxvla.cloudfront.net	18437cb5-f086-491c-bd0d-4bcaze2c64b6	xhr	
40	d3hb14vkzrxvla.cloudfront.net	18437cb5-f086-491c-bd0d-4bcaze2c64b6	vendor.571a2921.js:1 (xhr)	
41	beacon-v2.helpscout.net	container-frame.f24f42a4.chunk.js	vendor.571a2921 js:1 (script)	

Table 5. List of HTTPS requests observed in the tracking report accessible from the Cookie Script Free consent pop-up. This report is stored on the CMP's website, not in the consent pop-up itself.