What are Consent Management Platforms under the GDPR: processors or controllers?

Cristiana Santos
Utrecht University
The Netherlands
c.teixeirasantos@uu.nl

Midas Nouwens
Aarhus University
Denmark
midasnouwens@cc.au.dk

Michael Toth, Nataliia Bielova, Vincent Roca
Inria
France
name.surname@inria.fr

***Abstract*—In order to comply with the legal requirements for consent stated by the ePrivacy Directive and the General Data Protection Regulation (GDPR), the Consent Management Providers (CMPs) companies propose consent pop-ups that are embedded in an increasing number of websites. The Interactive Advertising Bureau Europe (IAB Europe) that specifies the underlying framework for these consent pop-ups, characterizes CMPs as data processors. Our work argues that the factual activities of CMPs often qualifies them as data controllers rather than processors. Discerning their role is crucial since compliance obligations and CMPs liability depend on it. From empirical experiments with two major European CMPs, Quantcast and OneTrust, and paired with a legal analysis, we identify three scenarios wherein CMPs behave as controllers. In particular we argue that the use of manipulative design strategies, meant to maximize the user opt-in, qualifies the CMP as data controller.**

***Index Terms*—Consumer privacy, IAB Europe TCF, GDPR, consent**

I. Introduction

To comply with the General Data Protection Regulation (GDPR) [1] and the ePrivacy Directive (ePD) [2], a website owner needs to first obtain *consent* from users, and only then is allowed to process personal data when offering goods and services and/or monitoring the users' behavior. As a result, numerous companies have started providing "*Consent as a Service*" solutions to help website owners ensure legal compliance [3]. To standardise the technical implementation of these consent pop-ups, the European branch of the Interactive Advertising Bureau (IAB Europe), an industry organisation made up of most major advertising companies in the EU, developed a Transparency and Consent Framework (TCF) [4]. This framework (currently on version 2.0) was developed to preserve the exchange of data within the advertising ecosystem, which now requires being able to demonstrate how, when, from who, and on which legal basis that data is collected. The actors in this ecosystem are IAB Europe, advertisers (called "vendors"), Consent Management Providers (CMPs), publishers, and data subjects (see Figure 1).

Although recent work has started to address the complex technical and legal aspects of the IAB Europe TCF ecosystem [5]–[11], *neither prior work nor court decisions* have so far discussed the role of the CMPs. Therefore, it is currently unclear what the role of these CMPs is under the GDPR, and consequently what their legal requirements and liabilities are.

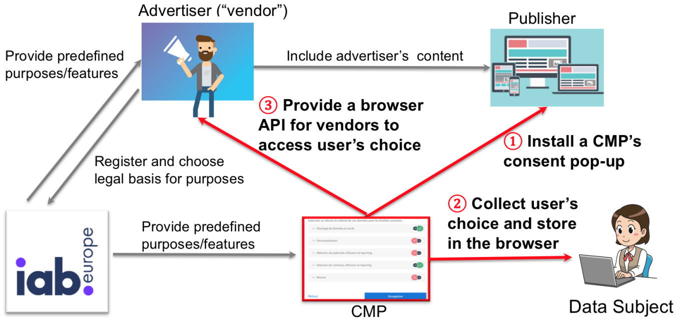

Advertiser ("vendor")
Publisher
Provide predefined purposes/features
Include advertiser's content
③ Provide a browser API for vendors to access user's choice
① Install a CMP's consent pop-up
Register and choose legal basis for purposes
② Collect user's choice and store in the browser
iab.europe
Provide predefined purposes/features
CMP
Data Subject

Fig. 1. **Actors under IAB Europe TCF ecosystem:** IAB Europe, Advertisers (called "vendors"), Consent Management Providers (CMPs), Publishers, Data Subjects. The IAB Europe defines the purposes and features that are shown to users. Registered vendors declare purposes and legal basis and the features upon which they rely. CMPs provide consent pop-up, store the user's choice as a browser cookie, and provide an API for advertisers to access this information.

If a CMP is established as a data processor and fails to comply with its obligations under the GDPR, then it can be held liable and fined (Articles 28(3)(f) and 32-36 GDPR). Moreover, if a false Consent Signal is stored and transmitted, it may well be considered an "unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed" [1, Art. 32(2)]. If instead a CMP is a controller, it is required to obtain personal data fairly, lawfully, and in compliance with any transparency requirements with respect to users. A breach of these obligations will make a CMP liable to sanctions (Article 28(10)).

This paper examines if and when CMPs can be considered a *data controller* – i.e., an actor responsible for determining the purposes and means of the processing of personal data (Art. 4(7) GDPR) – or a *data processor* – i.e., an actor which processes personal data on behalf of the controller (Art. 4(8) GDPR). Discerning the correct positioning of CMPs is crucial since compliance measures and CMPs liability depend on their accurate characterization (GDPR Recital 79). To determine the role of CMPs under the GDPR, in this paper we answer the following research questions:

§II When are CMPs processing personal data?
§III When do CMPs act as data processors?

The full version of this paper is to appear in the proceedings of Annual Privacy Forum (APF'2021): https://hal.inria.fr/hal-03169436.

§IV When do CMPs act as data controllers?

Note that the TCF is a voluntary framework: not all CMPs are part of it and abide by its policies. However, it has become a *de facto* standard used by a growing number of actors [5, Fig. 6]. This means that focusing on the CMPs within this ecosystem provides results that can more easily be generalised, compared to looking at the specific implementations of individual CMPs. Whenever we refer to CMPs in the rest of the article, we are referring to CMPs registered as part of the IAB Europe TCF. Our argumentation is based on: (1) legal analysis of binding legal sources (GDPR and case-law) and relevant data protection guidelines from the European Data Protection Board and Data Protection Authorities, (2) document analysis of the IAB Europe TCF, (3) empirical data gathered on our own website by deploying Quantcast and OneTrust – the two most popular CMPs in the EU, found respectively on 38.3% and 16.3% of the websites with a EU or UK TLD analyzed by Hils et al. [5].

A legal analysis is done by a co-author with expertise in Data Protection Law, and a technical analysis by Computer Science co-authors.

In this paper, we make the following **contributions**: i) we conclude that CMPs process personal data; ii) we analyse what exact behavior qualifies a CMP as a processor; and, iii) we identify several scenarios wherein CMPs can qualify as controllers.

II. When are CMPs processing personal data?

The *raison d'être* of CMPs is to collect, store, and share a *Consent Signal* [4], [12] of a data subject. The Consent Signal is a text-based digital representation of the user's consent in a standardised format, stored in the user's browser, and provided to third-party vendors by the CMP [4, paragraph 17, page 9]. Before discussing whether a CMP can be considered a data controller or processor, we first need to establish whether it even falls under the GDPR, which depends on whether it can be considered to process personal data. To answer this question, we first explain the definition of personal data under the GDPR, and then investigate which data CMPs process in practice and whether such data qualifies as personal data.

A. Legal definitions

Personal data is *"any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly. In particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"* (Article 4(11) GDPR [1]). Recital 30 asserts that online identifiers provided by their devices, such as IP addresses, can be associated to a person, thus making them identifiable.

Processing consists of *"any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"* (Article 4(2) GDPR). In practice, this means that almost any imaginable handling of personal data constitutes processing [13].

B. Mapping legal definitions into practice

Consent Signal. CMPs provide a consent pop-up, encode the user's choice in a Transparency and Consent (TC) string[1], store this value in a user's browser and provide an API for advertisers to access this information.

IAB Europe TCF specifies that when Consent Signal is "globally-scoped" (shared by CMPs running on different websites), the Consent Signal must be stored in a third-party cookie `euconsent-v2` set with `.consensu.org` domain. CMPs who register at TCF are given a subdomain `<cmp-name>.mgr.consensu.org` that is "delegated by the Managing Organisation (IAB Europe) to each CMP" [14]. "Globally-scoped" Consent Signal allows all CMPs who manage content on their `<cmp-name>.mgr.consensu.org` domains to also have access to the Consent Signal that is automatically attached to every request sent to any subdomain of `.consensu.org`. As a result, other consent pop up providers, who are not registered at IAB Europe, are not in a position to receive the Consent Signal stored in the user's browser because they have no access to any subdomain of `.consensu.org`, owned by IAB Europe. For non-global consent, a CMP can freely choose which browser storage to use for Consent Signal [14].

The Consent Signal contains a non human-readable encoded version (base64 encoded) of: (1) the list of purposes and features the user consented to; (2) the list of third-party vendors the user consented for; (3) the CMP identifier and version, together with other meta-data.

IP address. While the Consent Signal does not seem to contain personal data, CMPs additionally have access to the user's IP address. In order to include a consent pop-up, publishers are asked to integrate in their website a JavaScript code of a CMP (see step (1) in Figure 1). Such code is responsible for the implementation of a consent pop-up and in practice is loaded either: (1) directly from the server owned by a CMP (OneTrust's banner is loaded from the OneTrust's domain `https://cmp-cdn.cookielaw.org`), or (2) from the server `<cmp-name>.mgr.consensu.org` "delegated by the Managing Organisation (IAB Europe) to each CMP" [14] (Quantcast's script for consent pop-up is loaded from `https://quantcast.mgr.consensu.org`).

As an inevitable consequence of an HTTP(S) request, the server (of a CMP or controlled by a CMP via a DNS delegation by IAB Europe) is thus able to access the IP address of a visitor in this process. Additionally, CMP declare in their privacy policies the collection of IP addresses [15], [16].

[1] For the sake of uniformity, we call it "Consent Signal" in the rest of the paper.

Therefore, from a technical point of view, a CMP is able to record the IP address of the user's terminal in order to fulfil its service. Hereby we conclude that CMPs can have access to the user's IP address.

An IP address can be a cornerstone for data aggregation or identifying individuals. Empirical studies [17], [18] found that a user can, over time, get assigned a set of IP addresses which are unique and stable. Mishra et al. [18] found that 87% of users (out of 2,230 users over a study period of 111 days) retain at least one IP address for more than a month. 2% of user's IP addresses did not change for more than 100 days, and 70% of users had at least one IP address constant for more than 2 months. These assertions render IP addresses as a relatively reliable and robust way to identify a user.

Even though these results denote IP address stability (specially static IP addresses), the data protection community and case law diverge in the understanding of "dynamic" IP addresses as personal data. An IP address would be personal data if it relates to an *identified* or *identifiable* person. It was decided [19] that a dynamic IP address (temporarily assigned to a device) is not necessarily information related to an *identified* person, due to the fact that "such an address does not directly reveal the identity of the person who owns the computer from which a website was accessed, or that of another person who might use that computer".

The question that follows is *whether an IP address relates to an identifiable person for this IP address* to be considered personal data. In order to determine whether a person is *identifiable*, account should be taken of *all the means that can reasonably be used* by any entity to identify that person (Recital 26 GDPR). This risk-based approach [19], [20] means that anyone possessing the means to identify a user, renders such a user identifiable. Accordingly, CMPs have the means to collect IP addresses (as declared in their privacy policies) and to combine all the information relating to an identifiable person, rendering that combined information (IP address and, in some cases, Consent Signal) personal data.

Since identifiability of a person depends heavily on context, one should also take into account any other reasonable means CMPs have access to, for example, based on their role and market position in the overall advertising ecosystem [20]. One important aspect to consider, then, is the fact that these CMP providers can simultaneously also play a role as an advertising vendor, receiving the Consent Signal provided by their own CMP and (if positive) the personal data of the website visitor. Quantcast, for example, appears in the Global Vendor List (GVL) [21] as registered vendor #11. In the consent pop-up, their Privacy Policy [15], and their Terms of Service [22], [23], Quantcast mentions a large number of purposes for processing personal data, such as "Create a personalised ads profile", "Technically deliver ads or content", and "Match and combine offline data sources". The Evidon Company Directory [24] labels Quantcast as "Business Intelligence, Data Aggregator/Supplier, Mobile, Retargeter", and also mentions a large list of possible personal data collection from them. According to the same source, Quantcast also owns a retargeter called Struq. In view of this fact, CMPs seem to have reasonable means to combine information relating to an identifiable person, rendering that information personal data.

Summary. Although a Consent Signal itself does not seem to contain personal data, when the consent pop-up script is fetched from a CMP-controlled server, the CMP also processes the user's IP address, which the GDPR explicitly mentions as personal data. The possibility to combine both types of data renders a user identifiable. This possibility becomes particularly pertinent whenever a CMP also plays the role of a data vendor in the advertising ecosystem, which gives them access to more data that could be combined and increase the identifiability of a user.

III. When are CMPs data processors?

A. Legal definitions

A **processor** is an actor that processes personal data *on behalf* of the controller (Article 4 (8) GDPR). The relevant criteria that define this role are: (i) a dependence on the controller's instructions regarding processing activities [13], (Art. 28(3)(a)), Recital 81), and; (ii) a compliance with those instructions [25], which means they are not allowed to go beyond what they are asked to do by the controller [25].

B. Mapping legal definitions into practice

The main objectives of CMPs clearly correspond to the definition of data processors, because they act according to the instructions given by the website publisher with regards to the legal bases, purposes, special features, and/or vendors to show to the user in the consent pop-up. IAB Europe TCF also explicitly defines CMPs as data processors in the TCF documentation [4, page 10 (paragraph 8), page 11 (paragraph 11)]. The classification of the CMP as data processors is currently the widely shared consensus about their role.

CMPs responsability as processors. If a CMP is established as a data processor, it can be held liable and fined if it fails to comply with its obligations under the GDPR (Articles 28(3)(f) and 32-36 GDPR). Moreover, if a false Consent Signal is stored and transmitted, it may well be considered an "unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed" [1, Art. 32(2)].

Recent works reported numerous CMPs violating the legal requirements for a valid positive consent signal under the GDPR. For example, researchers detected pre-ticked boxes [6], [8], refusal being harder than acceptance [8] or not possible at all [6], choices of users not being respected [6], as well as more fine-grained configuration barriers such as aesthetic manipulation [26, Fig. 11], framing and false hierarchy [26, Fig. 12].

IV. When are CMPs data controllers?

A. Legal definitions

The primary factor defining a **controller** is that it "determines the purposes and means of the processing of personal data"

(Article 4(7) GDPR). We refer to the European Data Protection Board (EDPB) opinion [13] to unpack what is meant by 1) "determines", and 2) "purposes and means of the processing of personal data".

"Determines' refers to having the "determinative influence", "decision-making power" [13], [25], [27] or "independent control" [28] over the purposes and means of the processing. This concept of "determination" provides some degree of flexibility (to be adapted to complex environments) and the Court of Justice of the EU (CJEU), Data Protection Authorities (DPAs) and the EDPB describe that such control can be derived from:

- professional competence (legal or implicit) [13];
- factual influence based on factual circumstances surrounding the processing. (e.g. to contracts, and real interactions) [13];
- image given to data subjects and their reasonable expectations on the basis of this visibility [13];
- which actor "*organizes, coordinates and encourages*" data processing [27] (paragraphs 70, 71);
- interpretation or independent judgement exercised to perform a professional service [28].

"Purposes" and "means" refer to "why" data is processed (purposes) and "how" the objectives of processing are achieved (means). Regarding the determination of "purposes", the GDPR merely refers that purposes need to be explicit, specified and legitimate (Article 5(1)(b) [29]. In relation to the determination of "means", the EDPB distinguishes between "essential" and "non-essential means" and provides examples thereof [13], [25]:

- "Essential means" are inherently reserved to the controller; examples are: determining the i) type of personal data processed, ii) duration of processing, iii) recipients, and iv) categories of data subjects;
- "Non-essential means" may be delegated to the processor to decide upon, and concern the practical aspects of implementation, such as: i) choice for a particular type of hardware or software, ii) security measures, iii) methods to store or retrieve data.

B. Mapping legal definitions into practice

Although CMPs are explicitly designated as processors by the IAB Europe TCF specifications [4], in the following sections we analyse several functional activities of CMPs that can be considered to "determine the purposes and means of personal data processing", and thus designate them as data controllers for those activities:

§IV-C Including additional processing activities in their tools beyond those specified by the IAB Europe;
§IV-D Scanning publisher websites for tracking technologies and sorting them into purpose categories;
§IV-E Deploying manipulative design strategies in the UI of consent pop-ups.

C. Inclusion of additional processing activities

Technical description. When publishers employ the services of a CMP to manage consent on their website, the CMP provides the publisher with the necessary code to add their consent solution to the website. Although this code is ostensibly only for managing consent, it is possible for the CMP to also include other functionality.

As part of our empirical data gathering, we assumed the role of website owner (i.e., publisher) and installed a QuantCast CMP [30] on an empty website. Website owners are instructed by the CMP to "copy and paste the full tag" into their website header and "avoid modifying the tag as changes may prevent the CMP from working properly." [31]: the tag is the minimal amount of code necessary to load the rest of the consent management platform from an external source.

When installing the Quantcast CMP, we discovered that the "Quantcast Tag" script that deploys a consent pop-up on the website also loads a further script `choice.js` that integrates a 1x1 invisible image loaded from `pixel.quantserve.com` . When this image is loaded, it also sets a third-party cookie `mc` in the user's browser. By replicating the methodology to detect trackers [32], we analysed the `mc` cookie from `pixel.quantserve.com`; this cookie is *"user-specific"* – that is, its value is different for different website visitors – and comes from a third-party, allowing tracking across all sites where some content from `quantserve.com` or its subdomains is present. Such tracking by `quantserve.com` is prevalent in practice: recent research shows that third-party trackers from QuantCast are in top-10 tracking domains included by other trackers on 9K most popular websites [32, Fig. 6].

In the documentation that describes the QuantCast CMP, they mention that their CMP also contains a "QuantCast Measure" product [31] that is labeled as *"audience, insight and analytics tool"* for *"better understanding of audience"* [33]. The `mc` cookie we detected is the only cookie present on our empty website *before interacting with the QuantCast pop-up*, and thus we conclude that this cookie is likely responsible for the audience measurement purpose of QuantCast.

Legal analysis and conclusion. The QuantCast script installs *both a consent pop-up and a tracking cookie*, and its technical implementation makes it impossible for website owners to split these two functionalities. Such joint functionality triggers consequences on its legal status. The tracking cookie enables the QuantCast CMP to process data for its own tracking and measurement purposes, regardless of any instructions from the publisher, nor from the specifications of the IAB Europe TCF. Hence, the independent and determinative influence of a CMP is based on factual circumstances surrounding the processing, which qualifies a CMP in this scenario as a data controller.

D. Scanning and pre-sorting of tracking technologies

Technical description. One of the services CMPs often provide to publishers is a *scanning technology* which identifies the tracking technologies currently installed and active on the publisher's website (e.g., "first- and third-party cookies, tags, trackers, pixels, beacons and more" [34]). This scan is generally the first step when installing a consent pop-up on the website, and can be configured to automatically repeat on a regular basis.

In addition to providing descriptive statistics on the trackers currently active (e.g., what type of tracking), the scan results also include a *pre-sorting* of each of these technologies *into a particular data processing category* which are then displayed in the banner. In the case of OneTrust's CookiePro scanner, which is integrated into the banner configuration procedure when it is performed with an account, trackers are *"assigned a Category based on information in the Cookiepedia database"* [35], [36] (a service operated by OneTrust itself). The scanning includes identifying trackers (and matching them with vendors using Cookiepedia) and categorising these trackers/vendors in specific purposes. The four common purposes of trackers of Cookiepedia are i) strictly necessary (which includes authentication and user-security); ii) performance (also known as analytics, statistics or measurement); iii) functionality (includes customization, multimedia content, and social media plugin); and iv) targeting (known as advertising). Any trackers which cannot be found in the database are categorised as "Unknown" and require manual sorting (see Figure 3 in the Appendix). From the setup guides, there seems to be no explicit or granular confirmation required by the publisher itself (although they can edit after the fact): once the scan is complete, the categorisation of trackers is performed automatically and the consent pop-up is updated. In other words, the CookiePro's consent pop-up interface is in part automatically configured by the scanning tool.

This kind of scanning and categorising feature based on a CMPs own database is also offered by several other CMPs such as Cookiebot [37], Crownpeak [38], TrustArc [39] and Signatu [40].

Legal analysis and conclusion. In this concrete scenario, through providing the additional services and tooling (besides consent management) of scanning and consequently presorting tracking technologies into pre-defined purposes of data processing, CMPs contribute to the definition of purposes and to the overall compliance of the publisher wherein the CMP is integrated. This level of control of a CMP in determining the purposes for processing personal data and means is a decisive factor to their legal status as data controllers.

Moreover, CMPs that offer this additional service can be potentially be qualified as a *joint controller* (Article 26 GDPR) together with the publisher, as both actors jointly determine the purposes and means of processing. In line with the criteria provided by the EDPB [25], these additional processing operations convey the factual indication of a pluralistic control on the determination of purposes from this concrete CMP and respective publisher embedding these services by default. The acceptance of scanning and categorization of purposes entails i) a *common and complementing* decision taken by both entities, wherein the categorization of purposes ii) is *necessary* for the processing to take place in such manner that it has a *tangible impact* on the determination of the purposes and means of the processing and on the overall and forthcoming data processing.

The provision of both consent pop-up and scanning tool services by a CMP to a publisher creates a situation of *mutual benefit* [41], [42]: CMPs provide a service that creates a competitive advantage compared to other CMP providers, and publishers are relieved of having to manually match trackers with vendors, purposes, and legal bases.

As joint controllers, both entities would then need to make a transparent agreement to determine and agree on their respective responsibilities for compliance with the obligations and principles under the GDPR, considering also the exercise of data subjects' rights and the duties to provide information as required by Articles 13 and 14 of the GDPR. The essence of such arrangement must be made available to the data subject [25].

Such joint responsibility does not necessarily imply equal responsibility of both operators [42], nor does it need to cover all processing, in other words, it may be limited to this particular stage in the processing of scanning and presorting of trackers [41].

E. Deployment of manipulative design strategies

Legal compliance vs. consent rates. When designing their consent pop-ups, CMPs have considerable freedom: The only constraint placed on them by the IAB's TCF is that they need to include the purposes and features exactly as defined by the IAB Europe [4]. From a UI perspective, CMPs thus enjoy a design space and can choose *how exactly these choices are presented to the end user*.

The primary service offered by CMPs is to ensure legal compliance, which largely determines how they exercise their design freedom. However, the advertising industry is also incentivised to strive for *maximum consent rates*. This is apparent when looking at how CMPs market themselves. For example, Quantcast describes their tool as able to "*Protect and maximize ad revenue while supporting compliance with data protection laws*" [30] and provides "Choice Reports" that detail "[h]ow many times Choice was shown, Consent rate and Bounce Rate and a detailed breakout if the full, partial or no consent given" [43]. OneTrust advertises that its CMP can "*optimize consent rates while ensuring compliance*", and "*leverage A/B testing to maximize engagement, opt-ins and ad revenue*" [44]. In other words, although the official and primary service provided by CMPs is legal compliance, in practice, their service consists in *finding the balance between strict legal compliance and maximum consent rates* (considered to be negatively correlated), and this balancing ability becomes a point of competition between them.

Manipulative design strategies in consent pop-ups. Recent works denote that many popular CMPs deploy manipulative design strategies in consent pop-ups [6], [8], [26] and that such strategies influence the users' consent decisions [8], [45]. In concrete, recent findings concernedly report the majority of users think that a website cannot be used without giving consent (declining trackers would prevent access to the website) and also click the ”accept” button of the banner out of habit [45].

Technical analysis of default consent pop-ups. We portray an illustrative example of the use of manipulative design strategies in a consent pop-up. We installed a free version of OneTrust consent pop-up, the *CookiePro Free IAB TCF 2.0 CMP Builder*, on our empty website. During the installation, we chose a default version of the banner without any customization. Figure 2 (see Appendix -A) depicts the 2nd layer of the CookiePro's default banner: the option to “Accept All” is presented on top of the banner, (hence making acceptance to all purposes prioritized), while “Reject All” and “Confirm My Choices” are located at the very bottom of the banner, only made available after scrolling down. This banner includes the dark patterns of “obstruction”, “false hierarchy” and “sneaking” [46].

Legal analysis. From a regulatory perspective, several guidelines have been issued by the EU Data Protection Authorities on consent pop-ups, suggesting UI should be designed to ensure that *user's choices are not affected by interface designs*, proposing a privacy by design and by default approach (Article 25 GDPR), wherein default setting must be designed with data protection in mind. Proposals of such design refer that options of the same size, tone, position and color ought to be used, so as to provide the same level of reception to the attention of the user) [47]–[52]. Although these guidelines are welcomed, they do not have enough legal power to be enforceable in court, and it is unclear whether they impact compliance rates. However, in practice a CookiePro default design convinces the user to select what they feel is either the only option (presented on top), or the best option (proposed in a better position), while other options (to refuse) are cumbersome and hidden.

Determination of means. The primary service of CMPs is to provide consent management solutions to publishers through consent pop-ups, and thus anything related to this service can be considered as part of the “non-essential means” that can be delegated to a processor (see Section IV-A). However, when CMPs decide to include manipulative design strategies – known as *dark patterns* – to increase consent optimization rate, these can be considered to go beyond their primary goal. Manipulating users decision-making to increase the probability of prompt agreement to consent for tracking is not strictly necessary to provide its consent management service. In particular, resorting to such interface design strategies does not seem to consist of ”basic features” or ”service improvement” that could be considered as normally expected or compatible within the range of a processor's services [53]. In fact, there are no technical reasons that could substantiate the recourse to these dark patterns. A CMP could devise design banners in a fair and transparent way and which complies with the GDPR. The EDPB [54] refers that *”compulsion to agree with the use of personal data additional to what is strictly necessary, limits data subject's choices and stands in the way of free consent.”* We conclude that the use of manipulative strategies does not qualify as a mere technical implementation or operational use to obtain lawful consent, and instead falls inside the “*essential means*” category, making them a data controller.

Determination of purposes. Following the cognition held by the CJEU on the Jehowa's Witnesses case [27], one decisive factor of the role of a controller consists in the determination of “*who organized, coordinated and encouraged*” the data processing (paragraphs 70, 71). CMPs have exclusive *judgement and control* to adopt manipulative design strategies. Such strategies have a real impact on users' consent decisions and ultimately impact the processing of their data. By deploying such strategies, CMPs do not act on behalf of any other actor (which would lead to them being recognized as “processors”), but instead have control over which purposes will be more likely to be accepted or rejected by users. In practice, CMPs' deployment of *dark patterns* that manipulate the user's final choice evidences a degree of *factual influence or decision-making power* over the processing activities that will follow.

Conclusion. CMPs exercise a dominant role in the decision-making power on eventual processing activities within the IAB Europe TCF ecosystem. We argue that whenever CMPs impose dark patterns to a publisher and similarly whenever CMPs propose a default banner that features dark patterns to a publisher, these facts strongly indicate a controllership status in its own right due to CMPs' influence on the determination of means and purposes of processing, even if only to a limited extent. However, the afforded discretion availed to CMPs requires a case by case analysis and is more likely to lead to divergent interpretations.

V. Conclusion

In this paper we discussed the requirements for CMPs to be qualified as processors and as controllers and concluded that such status has to be assessed with regard to each specific data processing activity. From an empirical analysis we concluded that CMPs assume the role of controllers, and thus should be responsible for their processing activities, in four scenarios: i) when including additional processing activities in their tool, ii) when they perform scanning and pre-sorting of tracking technologies, iii) when they include third-party vendors by default, and finally iv) when they deploy interface manipulative design strategies.

Acknowledgements

We would like to thank Daniel Woods, Triin Siil, Johnny Ryan and anonymous reviewers of ConPro'21 for useful comments and feedback that has lead to this paper. This work has been partially supported by the ANR JCJC project PrivaWeb (ANR-18-CE39-0008) and by the Inria DATA4US Exploratory Action project.

References

[1] 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) (text with eea relevance). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679.

[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 2019.10.31.

[3] Cristiana Santos, Nataliia Bielova, and Célestin 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*, pages 91–135, 2020.

[4] IAB Europe. IAB Europe Transparency & Consent Framework Policies, 2020. https://iabeurope.eu/wp-content/uploads/2020/11/TCF_v2-0_Policy_version_2020-11-18-3.2a.docx-1.pdf.

[5] M. Hils, Daniel W. Woods, and Rainer Böhme. Measuring the Emergence of Consent Management on the Web. *Proceedings of the ACM Internet Measurement Conference*, 2020.

[6] Célestin Matte, Nataliia Bielova, and Cristiana 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 (IEEE S&P 2020)*, 2020.

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

[8] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. In *CHI*, 2020.

[9] Hubert Pawlata and Gültekin Caki. The Impact of the Transparency Consent Framework on current Programmatic Advertising Practices, 2020. 4th International Conference on Computer-Human Interaction Research and Applications.

[10] Martin Degeling, Christine Utz, Christopher Lentzsch, Henry Hosseini, Florian Schaub, and Thorsten Holz. We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy. *Network and Distributed Systems Security Symposium*, 2019.

[11] Nataliia Bielova and Cristiana Santos. Call for Feedback to the EDPB regarding Guidelines 07/2020 on the concepts of controller and processor in the IAB Europe Transparency and Consent Framework, 2020. http://www-sop.inria.fr/members/Nataliia.Bielova/opinions/EDPB-contribution-controllers-processors.pdf.

[12] IAB Europe. Transparency and consent string with global vendor CMP list formats (final v.2.0): About the transparency consent string (TC String), 2020. https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/TCFv2/IAB%20Tech%20Lab%20-%20Consent%20string%20and%20vendor%20list%20formats%20v2.md#about-the-transparency--consent-string-tc-string, accessed on 14 January 2021.

[13] 29 Working Party. Opinion 1/2010 on the concepts of "controller" and "processor" WP 169, 2010. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf.

[14] IAB Europe. Transparency and Consent String with Global Vendor and CMP List Formats (Final v.2.0), 2019. https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/TCFv2/IAB Tech Lab - Consent string and vendor list formats v2.md, accessed on 12 February 2021.

[15] Quantcast. Privacy Policy, Dec 2020. https://www.quantcast.com/privacy/.

[16] OneTrust. Privacy Notice, Oct 2020. https://www.onetrust.com/privacy-notice/.

[17] Gregor Maier, Anja Feldmann, Vern Paxson, and Mark Allman. M.: On Dominant Characteristics of Residential Broadband Internet Traffic. In *In: Proceedings of the 9th ACM SIGCOMM conference on Internet measurement conference*, pages 90–102, 2009.

[18] Vikas Mishra, Pierre Laperdrix, Antoine Vastel, Walter Rudametkin, Romain Rouvoy, and Martin Lopatka. Don't count me out: On the relevance of IP address in the tracking ecosystem. In Yennun Huang, Irwin King, Tie-Yan Liu, and Maarten van Steen, editors, *WWW '20: The Web Conference 2020, Taipei, Taiwan, April 20-24, 2020*, pages 808–815. ACM / IW3C2, 2020.

[19] Court of Justice of the European Union. Case 582/14 – Patrick Breyer v Germany, 2016. ECLI:EU:C:2016:779.

[20] Michèle Finck and Frank Pallas. They Who Must Not Be Identified – Distinguishing Personal from Non-Personal Data Under the GDPR. *International Data Privacy Law*, 10, 2020.

[21] IAB Europe. Vendor List TCF v2.0, 2020. https://iabeurope.eu/vendor-list-tcf-v2-0/.

[22] Quantcast. Quantcast Choice Terms of Service, 2020. https://www.quantcast.com/legal/quantcast-choice-terms-of-service/.

[23] Quantcast. Quantcast Measure and Q for Publishers Terms of Service, 2020. https://www.quantcast.com/legal/measure-terms-service/.

[24] Evidon. Quantcast-related pages on Evidon Company Directory, 2017. https://info.evidon.com/companies?q=Quantcast [Consulted on Jan. 8th, 2021.].

[25] European Data Protection Board. Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 1.0, 2020. https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en.

[26] Colin M. Gray, Cristiana Santos, Nataliia Bielova, Michael Toth, and Damian Clifford. Dark patterns and the legal requirements of consent banners: An interaction criticism perspective. In *ACM CHI 2021*, 2020. https://arxiv.org/abs/2009.10194.

[27] European Court of Justice. Case 25/17 Jehovan todistajat, ECLI:EU:C:2018:551.

[28] Information Commissioner's Office. Data controllers and data processors: what the difference is and what the governance implications are, 2018. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/controllers-and-processors/.

[29] Imane Fouad, Cristiana Santos, Feras Al Kassar, Nataliia Bielova, and Stefano Calzavara. On Compliance of Cookie Purposes with the Purpose Specification Principle. In *2020 International Workshop on Privacy Engineering, IWPE*, 2020. https://hal.inria.fr/hal-02567022.

[30] Quantcast. Quantcast Choice, 2020. https://www.quantcast.com/products/choice-consent-management-platform/.

[31] Quantcast. 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-.

[32] Imane Fouad, Nataliia Bielova, Arnaud Legout, and Natasa Sarafijanovic-Djukic. Missed by filter lists: Detecting unknown third-party trackers with invisible pixels. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2020, 2020. Published online: 08 May 2020, https://doi.org/10.2478/popets-2020-0038.

[33] Quantcast. Quantcast Measure, 2021. https://www.quantcast.com/products/measure-audience-insights/.

[34] CookiePro. Scanning a Website, Nov 2020. https://community.cookiepro.com/s/article/UUID-621498be-7e5c-23af-3bfd-e772340b4933.

[35] CookiePro. Lesson 3: Scan Results and Categorizing Cookies, Jul 2020. https://community.cookiepro.com/s/article/UUID-309d4544-c927-fe00-da50-60ed7668c6b5.

[36] Cookiepedia Official website. https://cookiepedia.co.uk/ .

[37] Cookiebot. Cookie scanner – revealer of hidden tracking, Sep 2020. https://www.cookiebot.com/en/cookie-scanner/.

[38] Crownpeak. Vendor categories, n.d. https://community.crownpeak.com/t5/Universal-Consent-Platform-UCP/Vendor-Categories/ta-p/665.

[39] TrustArc. Cookie Consent Manager, n.d. https://trustarc.com/cookie-consent-manager/.

[40] Signatu. Trackerdetect, n.d. https://signatu.com/product/trackerdetect/.

[41] European Court of Justice. Case C-40/17 Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV, ECLI:EU:C:2019:629.

[42] European Court of Justice. Case C-210/16 Wirtschaftsakademie Schleswig-Holstein, ECLI:EU:C:2018:388.

[43] Quantcast. Quantcast Choice – User Guide, 2020. https://help.quantcast.com/hc/en-us/articles/360052725133-Quantcast-Choice-User-Guide.

[44] OneTrust PreferenceChoice: Consent management platform (cmp). https://www.preferencechoice.com/consent-management-platform/, accessed on January 20, 2021.

[45] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. (Un)informed Consent: Studying GDPR Consent Notices in the Field. In *Conference on Computer and Communications Security*, 2019.

[46] Colin M. Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, and Austin L. Toombs. The Dark (Patterns) Side of UX Design. In *Proceedings of the CHI Conference Human Factors in Computing Systems*, page 534, 2018.

[47] Commission Nationale de l'Informatique et des Libertés (CNIL). Shaping Choices in the Digital World, 2019. https://linc.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf.

[48] Commission Nationale de l'Informatique et des Libertés (French DPA). French guidelines on cookies: Deliberation No 2020-091 of September 17, 2020 adopting guidelines relating to the application of article 82 of the law of January 6, 1978 amended to read and write operations in a user's terminal (in particular to "cookies and other tracers"), 2020. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042388179.

[49] Greek DPA (HDPA). Guidelines on Cookies and Trackers, 2020. http://www.dpa.gr/APDPXPortlets/htdocs/documentSDisplay.jsp?docid=84,221,176,170,98,24,72,223.

[50] Information Commissioner's Office. Guidance on the use of cookies and similar technologies, 2019. https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf.

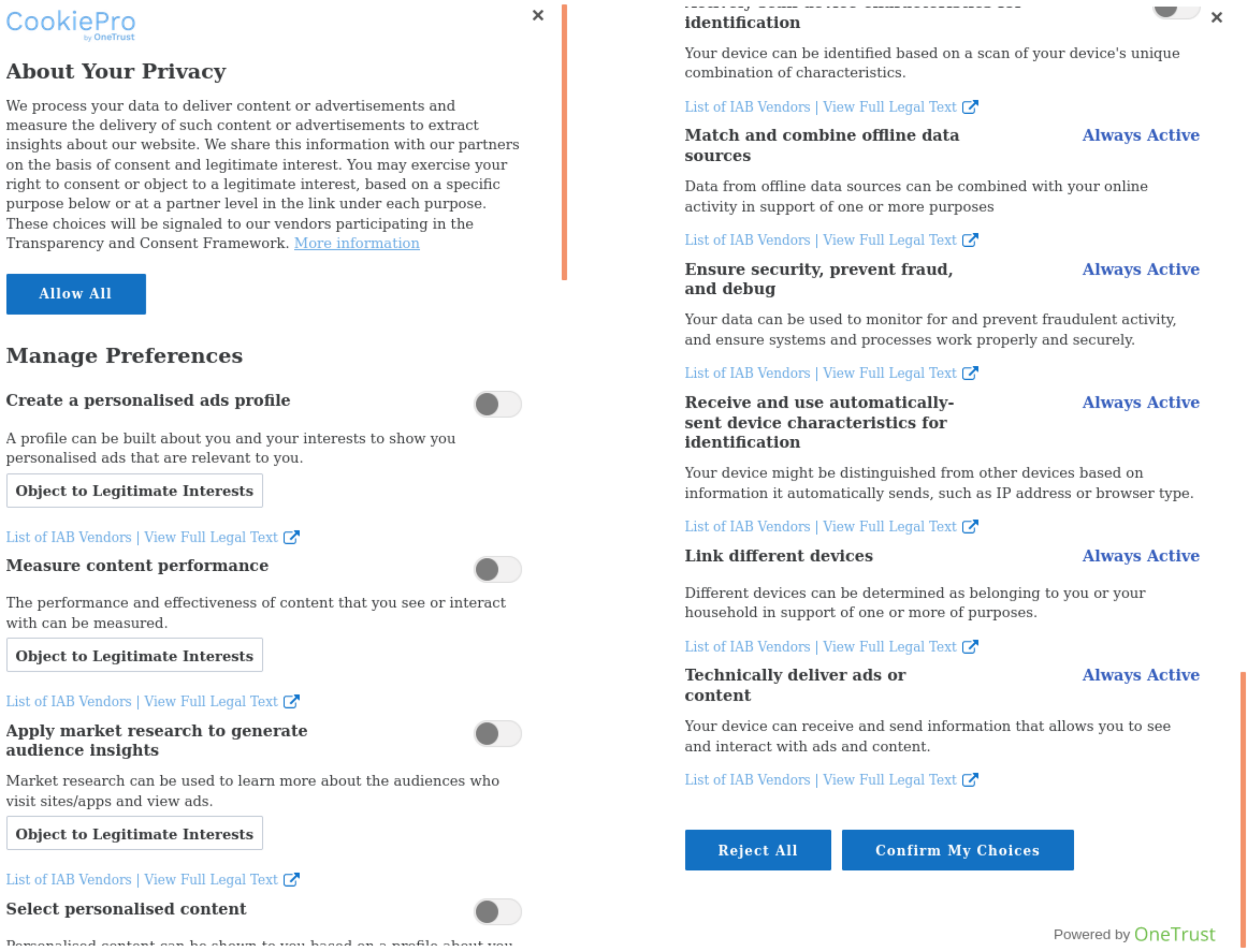
[51] Data Protection Commission (Irish DPA). Guidance note on the use of cookies and other tracking technologies, 2020. https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%20on%20cookies%20and%20other%20tracking%20technologies.pdf.

[52] Agencia Española de Protección de Datos (Spanish DPA). Guide on use of cookies, 2021. https://www.aepd.es/sites/default/files/2021-01/guia-cookies-en.pdf.

[53] Mike Hintze. Data controllers, data processors, and the growing use of connected products in the enterprise: Managing risks, understanding benefits, and complying with the gdpr. *Cybersecurity*, 2018.

[54] European Data Protection Board. Guidelines 05/2020 on consent, Version 1.1, adopted on 4 May 2020, 2020. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

A. Additional figures for Section IV



CookiePro by OneTrust

About Your Privacy

We process your data to deliver content or advertisements and measure the delivery of such content or advertisements to extract insights about our website. We share this information with our partners on the basis of consent and legitimate interest. You may exercise your right to consent or object to a legitimate interest, based on a specific purpose below or at a partner level in the link under each purpose. These choices will be signaled to our vendors participating in the Transparency and Consent Framework. More information

Allow All

Manage Preferences

Create a personalised ads profile

A profile can be built about you and your interests to show you personalised ads that are relevant to you.

Object to Legitimate Interests

List of IAB Vendors | View Full Legal Text

Measure content performance

The performance and effectiveness of content that you see or interact with can be measured.

Object to Legitimate Interests

List of IAB Vendors | View Full Legal Text

Apply market research to generate audience insights

Market research can be used to learn more about the audiences who visit sites/apps and view ads.

Object to Legitimate Interests

List of IAB Vendors | View Full Legal Text

Select personalised content

Personalised content can be shown to you based on a profile about you

identification

Your device can be identified based on a scan of your device's unique combination of characteristics.

List of IAB Vendors | View Full Legal Text

Match and combine offline data sources Always Active

Data from offline data sources can be combined with your online activity in support of one or more purposes

List of IAB Vendors | View Full Legal Text

Ensure security, prevent fraud, and debug Always Active

Your data can be used to monitor for and prevent fraudulent activity, and ensure systems and processes work properly and securely.

List of IAB Vendors | View Full Legal Text

Receive and use automatically-sent device characteristics for identification Always Active

Your device might be distinguished from other devices based on information it automatically sends, such as IP address or browser type.

List of IAB Vendors | View Full Legal Text

Link different devices Always Active

Different devices can be determined as belonging to you or your household in support of one or more of purposes.

List of IAB Vendors | View Full Legal Text

Technically deliver ads or content Always Active

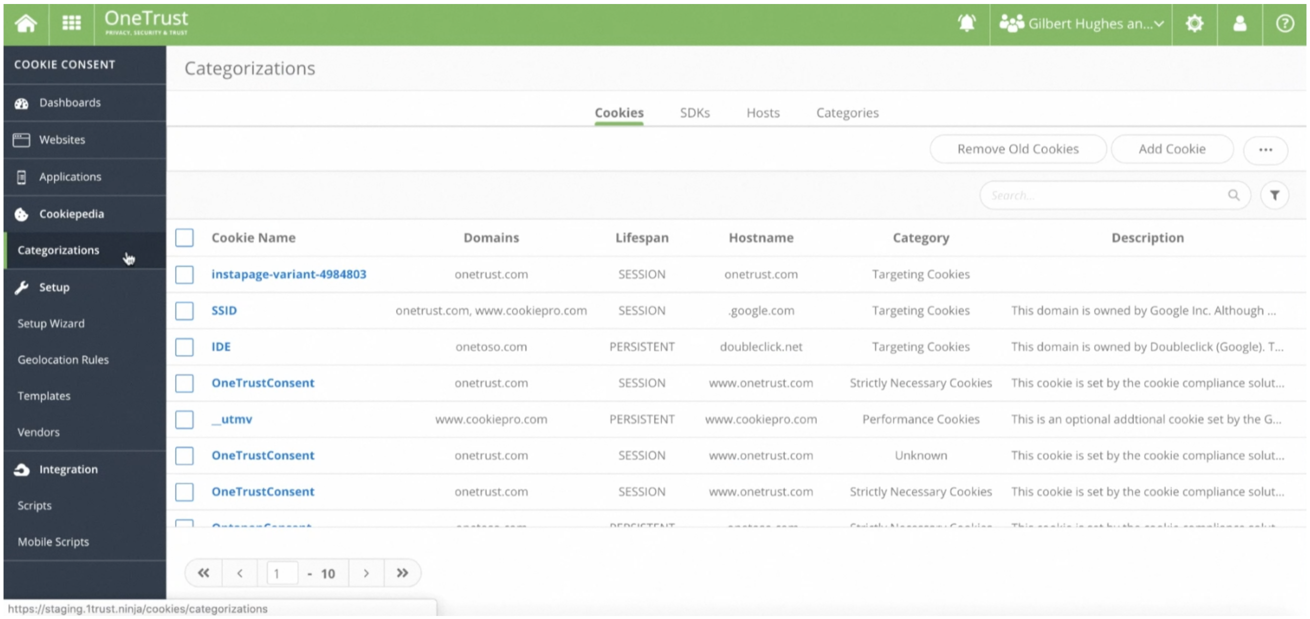
Your device can receive and send information that allows you to see and interact with ads and content.

List of IAB Vendors | View Full Legal Text

Reject All | Confirm My Choices

Powered by OneTrust

Fig. 2. 2^{nd} layer of the default consent pop-up provided by CookiePro Free IAB TCF 2.0 CMP Builder (owned by OneTrust). [Captured on 13 Jan. 2021]. On the left, the top level of the page, displaying the "Accept All" button. On the right, the bottom of the same screen, displaying the "Reject All" and "Confirm My Choices" buttons, so the user needs to scroll down in order to see them.



Categorizations

□	Cookie Name	Domains	Lifespan	Hostname	Category	Description
□	instapage-variant-4984803	onetrust.com	SESSION	onetrust.com	Targeting Cookies	
□	SSID	onetrust.com, www.cookiepro.com	SESSION	.google.com	Targeting Cookies	This domain is owned by Google Inc. Although ...
□	IDE	onetoso.com	PERSISTENT	doubleclick.net	Targeting Cookies	This domain is owned by Doubleclick (Google). T...
□	OneTrustConsent	onetrust.com	SESSION	www.onetrust.com	Strictly Necessary Cookies	This cookie is set by the cookie compliance solut...
□	__utmv	www.cookiepro.com	PERSISTENT	www.cookiepro.com	Performance Cookies	This is an optional addtional cookie set by the G...
□	OneTrustConsent	onetrust.com	SESSION	www.onetrust.com	Unknown	This cookie is set by the cookie compliance solut...
□	OneTrustConsent	onetrust.com	SESSION	www.onetrust.com	Strictly Necessary Cookies	This cookie is set by the cookie compliance solut...

Fig. 3. CookiePro's configuration back-end designed for the publisher, when logged. After completing a scan for trackers on the publisher's website, this screen shows the trackers that were found together with a category they are assigned with.