Consent Management Platforms under the GDPR: processors and/or controllers?

Cristiana Santos, Midas Nouwens, Michael Toth, Nataliia Bielova, Vincent Roca

▶ **To cite this version:**

Cristiana Santos, Midas Nouwens, Michael Toth, Nataliia Bielova, Vincent Roca. Consent Management Platforms under the GDPR: processors and/or controllers?. APF 2021 - 9th Annual Privacy Forum, Jun 2021, Oslo, Norway. pp.47-69, 10.1007/978-3-030-76663-4_3 . hal-03169436

HAL Id: hal-03169436
https://inria.hal.science/hal-03169436v1

Submitted on 12 Apr 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Consent Management Platforms under the GDPR: processors and/or controllers?*

Cristiana Santos[2], Midas Nouwens[3], Michael Toth[1], Nataliia Bielova[1], and Vincent Roca[1]

[1] Inria, France
{nataliia.bielova,michael.toth,vincent.roca}@inria.fr
[2] Utrecht University, The Netherlands
c.teixeirasantos@uu.nl
[3] Aarhus University, Denmark
midasnouwens@cc.au.dk

Abstract. Consent Management Providers (CMPs) provide consent pop-ups that are embedded in ever more websites over time to enable streamlined compliance with the legal requirements for consent mandated by the ePrivacy Directive and the General Data Protection Regulation (GDPR). They implement the standard for consent collection from the Transparency and Consent Framework (TCF) (current version v2.0) proposed by the European branch of the Interactive Advertising Bureau (IAB Europe). Although the IAB's TCF specifications characterize CMPs as data processors, CMPs factual activities often qualifies them as data controllers instead. Discerning their clear role is crucial since compliance obligations and CMPs liability depend on their accurate characterization. We perform empirical experiments with two major CMP providers in the EU: Quantcast and OneTrust and paired with a legal analysis. We conclude that CMPs process personal data, and we identify multiple scenarios wherein CMPs are controllers.

Keywords: Consent management providers · IAB Europe TCF · data controllers · GDPR · consent.

1 Introduction

To comply with the General Data Protection Regulation (GDPR) [31] and the ePrivacy Directive (ePD) [20], 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 [60].

* A preliminary version of this paper is presented for discussion only, with no official proceedings at ConPro'21: https://www.ieee-security.org/TC/SPW2021/ConPro/.

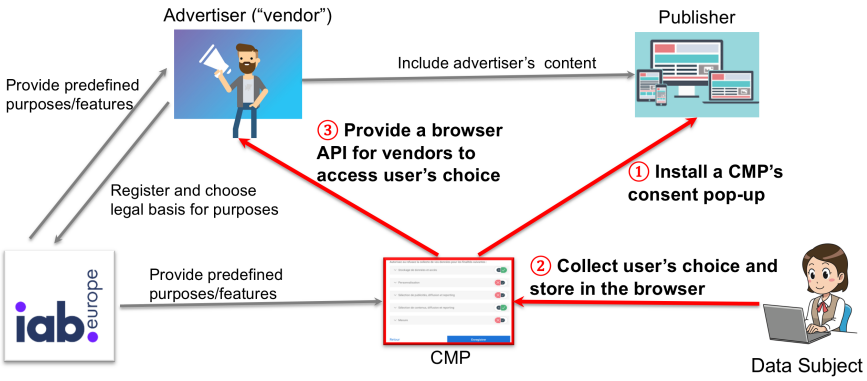

Fig. 1. Actors under IAB Europe TCF ecosystem: IAB Europe, Advertisers (called "vendors"), Consent Management Providers (CMPs), Publishers, Data Subjects. The IAB Europe defines the purposes and features that are shown to users. Registered vendors declare purposes and legal basis and the features upon 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.

To standardise[4] 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) [38]. 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 [6, 19, 35, 47, 48, 50, 52], *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.

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:

§2 When are CMPs processing personal data?

[4] Standardization is used within the meaning of streamline at scale consent implementation.

§3 When do CMPs act as data processors?
§4 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 [35, 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:

- 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, document analysis of the IAB Europe TCF,
- 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. [35].

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**:

- we conclude that CMPs process personal data,
- we analyse what exact behavior qualifies a CMP as a processor,
- we identify several scenarios wherein CMPs can qualify as controllers, and
- we provide recommendations for policymakers.

2 When are CMPs processing personal data?

The *raison d'être* of CMPs is to collect, store, and share a *Consent Signal* [21,38] 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 [38, 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.

2.1 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 [31]). 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 [2].

2.2 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[5], 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 IAB Europe TCF are provided with a subdomain `<cmp-name>.mgr.consensu.org` that is "delegated by the Managing Organisation (IAB Europe) to each CMP" [37]. "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 [37]. The Consent Signal contains a non human-readable encoded version (base64 encoded) of:

- the list of purposes and features the user consented to;
- the list of third-party vendors the user consented for;
- 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

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

`<cmp-name>.mgr.consensu.org` "delegated by the Managing Organisation (IAB Europe) to each CMP" [37] (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 [**?**, 57]. 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 [46, 49] found that a user can, over time, get assigned a set of IP addresses which are unique and stable. Mishra et al. [49] 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 [14] 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 [14, 28] 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 [28]. 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) [39] as registered vendor #11. In the consent pop-up, their Privacy Policy [57], and their Terms of Service [55, 56], 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 [27] 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.

3 When are CMPs data processors?

3.1 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 [2], (Art. 28(3)(a)), Recital 81), and; (ii) a compliance with those instructions [26], which means they are not allowed to go beyond what they are asked to do by the controller [26].

3.2 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 [38, 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.

Responsibility of CMPs 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" [31, 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 [48,50], refusal being harder than acceptance [50] or not possible at all [48], choices of users not being respected [48], as well as more fine-grained configuration barriers such as aesthetic manipulation [33, Fig. 11], framing and false hierarchy [33, Fig. 12].

4 When are CMPs data controllers?

In this section we analyse when CMPs are data controllers. Firstly, in section 4.1 we provide the legal definitions necessary to qualify CMPs as data controllers.

In the following sections (4.2 – 4.5) we will map these legal definitions into practice. Although CMPs are explicitly designated as processors by the IAB Europe TCF specifications [38], we analyse four functional activities of CMPs that enables their qualification as data controllers. We include a technical description of such activities followed by a legal analysis. These activities refer to:

§4.2 Including additional processing activities in their tools beyond those specified by the IAB Europe;
§4.3 Scanning publisher websites for tracking technologies and sorting them into purpose categories;
§4.4 Controlling third-party vendors included by CMPs;
§4.5 Deploying manipulative design strategies in the UI of consent pop-ups.

Finally, in section 4.6 we determine the responsibility of a CMPs as data controllers.

4.1 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 [2] 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" [2, 22, 26] or "independent control" [40] 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) [2];
- factual influence based on factual circumstances surrounding the processing. (e.g. to contracts, and real interactions) [2];

- image given to data subjects and their reasonable expectations on the basis of this visibility [2];
- which actor "*organizes, coordinates and encourages*" data processing [22] (paragraphs 70, 71);
- interpretation or independent judgement exercised to perform a professional service [40].

"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) [30]. In relation to the determination of "means", the EDPB distinguishes between "essential" and "non-essential means" and provides examples thereof [2, 26]:

- "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.

Important notes on the assessment of controllers are referred herewith. The role of controller and processor are *functional* concepts [26]: the designation of an actor as one or the other is derived from their *factual roles and activities* in a specific situation [2], rather than from their formal designation [3]. Notably, access to personal data is not a necessary condition to be a controller [23, 24]. Moreover, the control exercised by a data controller may extend to the entirety of processing at issue, and also be limited to *a particular stage in the processing* [23].

4.2 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 [53] 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." [58]: 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 the domain

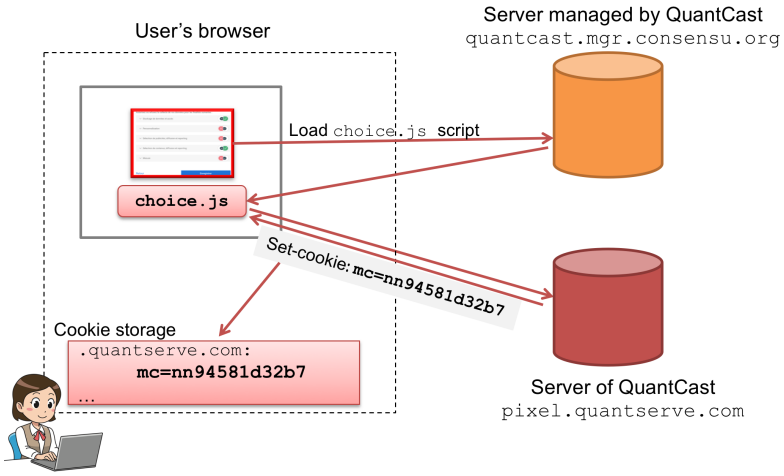

Fig. 2. Loading of invisible pixel by a QuantCast consent pop-up: the pixel sets a third-party cookie `mc` with a user-specific identifier that is further accessible to all subdomains of `quantserve.com`.

`pixel.quantserve.com` (see Figure 2). 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 [29], 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 [29, Fig. 6].

In the documentation that describes the QuantCast CMP, they mention that their CMP also contains a "QuantCast Measure" product [58] that is labeled as *"audience, insight and analytics tool"* for *"better understanding of audience"* [59]. 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. 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.

4.3 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" [12]). 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"* [10, 11] (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). 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 [9], Crownpeak [15], TrustArc [63] and Signatu [61].

Legal analysis. 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 [26], 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

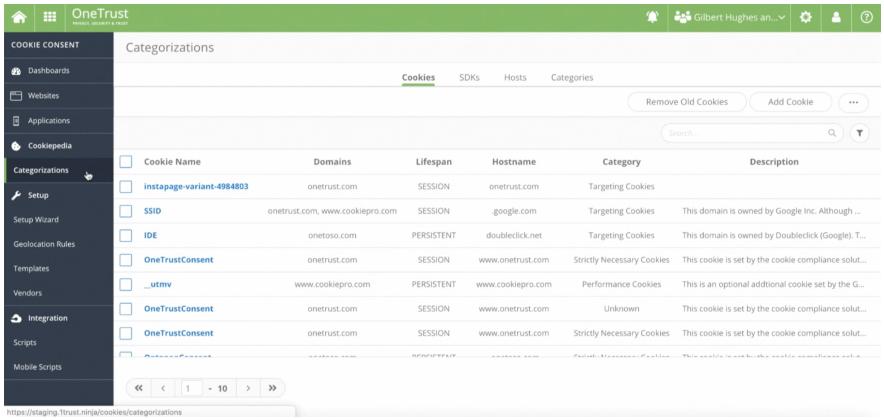

Fig. 3. CookiePro's configuration back-end designed for the publisher, when logged. After completing a scan for trackers on the publisher's website, this screen shows the trackers that were found together with a category they are assigned with.

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* [23, 24]: 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 [26].

Such joint responsibility does not necessarily imply equal responsibility of both operators [24], 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 [23].

4.4 Controlling third-party vendors included by CMPs

Technical description. Upon installation of a CMP, the website publisher generally has the possibility to decide which vendors (third-party advertisers) to include in the consent pop-up. From more than 600 vendors currently registered at IAB Europe TCF [39], only the selected vendors will be then stored in the Consent Signal when the user interacts with the consent pop-up. In practice,

the way the publisher effectively exercises this choice of vendors depends on the options available in the configuration tool provided by the CMP.

The IAB policies explicitly state that a CMP cannot have preferential treatment for one vendor or another [38, paragraph 6(3)]. Hence, CMPs cannot preselect or treat vendors differently, unless *a publisher explicitly asks* a CMP to include/delete some vendors from the list of all vendors.

Herewith we analyse two case studies of QuantCast and OneTrust. Figure 4 shows an installation process of QuantCast CMP, which gives some power to publishers. It includes by default *around 671 vendors registered in the IAB Europe TCF*, but allows a publisher to remove some of the vendors from this list. This power given to publishers is, however, limited: publishers must either manually search and *select one-by-one the vendors they want to exclude*.

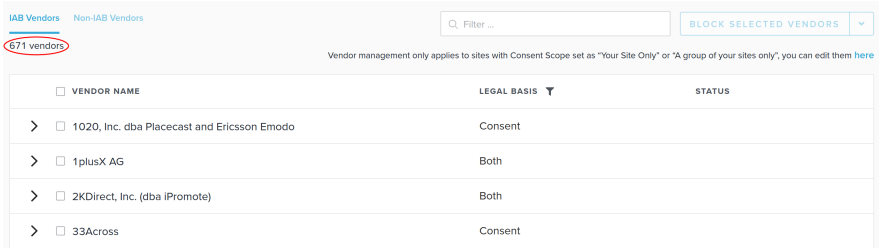

Fig. 4. Installation process of QuantCast CMP [Captured on 5 Feb. 2021]. A publisher has to manually search and exclude one-by-one the vendors from the list of 671 vendors registered in IAB Europe TCF.

Regarding OneTrust's free, open access service called *CookiePro Free IAB TCF 2.0 CMP Builder* [13], it gives no control to the publisher over the list of vendors to include. As a result, when the user clicks "Accept" in a CookiePro banner we installed on our empty website, the Consent Signal contains 2 special features optin, 10 purposes under the legal basis of consent, 9 purposes under legitimate interest, *631 vendors for consent*, and 261 vendors under legitimate interest.

Relying on a publisher to manually remove the vendors with whom it does not have a partnership presupposes that publishers are willing to actively check and configure the list of vendors, which can require an active action from a publisher on a separate screen during the configuration process. Such assumption contends with relevant findings from behavioral studies regarding *default effect bias*, referring to the tendency to stick to default options [1, 42–44]. Thaler and Sunstein concluded that *"many people will take whatever option requires the least effort, or the path of least resistance"* [62]. It seems reasonable to argue that publishers will generally leave the list as is.

Legal analysis. CMPs are in a position to decide what decision-making power to award to website publishers regarding the selection of specific vendors. By

restricting the ability of the publisher to (de)select vendors, the CMP obliges the publisher to present to the user the full list of IAB Europe-registered vendors. We recall that when registering to the IAB Europe, each vendor declares a number of purposes upon which it wishes to operate, and hence it can be concluded that the CMP automatically increases the number of purposes displayed to – and possibly accepted by – the end-user. As a result, a CMP requires the publisher to present more processing purposes than necessary, which has direct consequences on the interface the end-user will interact with.

With such factual decision-making power over the display of purposes rendered to users, it can be observed that CMPs exert influence over the determination of purposes of data processing, turning it to a data controller. Relatedly, deciding on the third-parties that process personal data consists on the determination of *"essential means"* – a competency allocated only to controllers, which again consolidates our conclusion that CMPs are data controllers in the above mentioned scenario.

This practice of including by default hundreds of third-party vendors implies that CMPs seem to breach several data protection principles:
Transparency and fairness principle (Article 5(1)(a) GDPR) which mandates controllers to handle data in a way that would be reasonably expected by the data subjects. When users signify their preferences in the consent pop-up, they are not aware nor expect their data to be potentially shared with around 600 third-parties. Moreover, the inclusiveness by default of this amount of partners seems to trigger severe risks to the rights of users and thus this consent sharing needs to be limited (Recital 75 GDPR).
Minimization principle (Article 5(1)(c) GDPR) provides that data shall be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processes". This principle is generally interpreted as referring to the need to minimise the quantity of data that is processed. One may, however, also wonder whether the principle extends to other characteristics such as the number of recipients to which data is shared with. Moreover, according to the theory of choice proliferation, a large number of purposes can lead to the user experiencing negative effects. However, in the case of consent pop-ups, the critical threshold of presented purposes beyond which these effects occur is not yet known [45].

4.5 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 [38]. 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*" [53] 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" [54]. 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*" [51]. 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 [33,48,50] and that such strategies influence the users' consent decisions [50, 64]. 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 [64].

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 5 depicts the 2$^{\text{nd}}$ 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" [32].

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) [4,7,8,17,34,41]. 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"

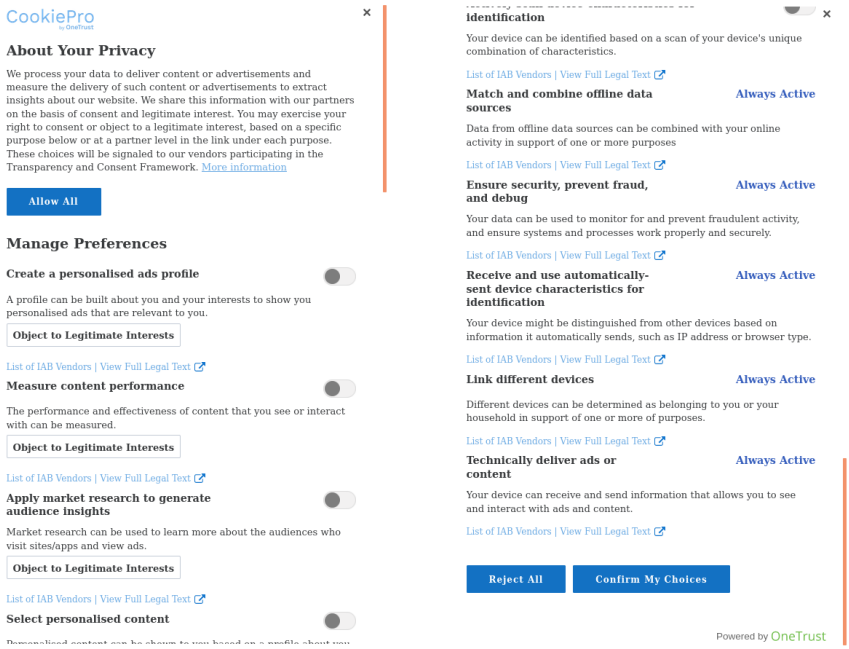

Fig. 5. 2nd layer of the default consent pop-up provided by CookiePro Free IAB TCF 2.0 CMP Builder (owned by OneTrust). [Captured on 13 Jan. 2021]. On the left, the top level of the page, displaying the "Accept All" button. On the right, the bottom of the same screen, displaying the "Reject All" and "Confirm My Choices" buttons, so the user needs to scroll down in order to see them.

that can be delegated to a processor (see Section 4.1). 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 [36]. 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 [25] 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 [22], 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.

Summary. 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.

4.6 What is the responsibility of a CMP as controller?

A CMP as a data processor that goes beyond the mandate given by the controller and acquires a relevant role in determining its own purposes, as shown in the scenarios in Section 4, becomes a controller with regard to those specific processing operations [2] and will be in breach of its obligations, hence subject to sanctions (Article 28(10)). The breadth of the parties responsibility, including the extent to which they become data controllers, should be analysed on a case by case basis [5] depending on the particular conditions of collaboration between publishers and CMPs, and then should be reflected in the service agreements.

One of their responsibilities as controllers include the obligation to comply with the principles of data protection, thereby they are required to obtain personal data fairly, lawfully and to comply with any transparency requirements with respect to users and obtain a valid consent.

Additionally, CMPs should offer design choices that are the most privacy-friendly, in a clear manner and as a default choice, in line with the principle of data protection by design and data protection by default (Article 25 of the GDPR). Finally, CMPs should respect the minimization principle – the use of compulsion methods (either in the manipulation of purposes, either pre-registering around 600 vendors) *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* [25, paragraph 27].

5 Recommendations

In this section, based on our legal and empirical analysis, we propose a number of recommendations for policy makers that could address the current ambiguity revolving the role of CMPs.

Concepts of controller and processor in the GDPR need to be clarified. We hope to provide influential stakeholders, such as the EDPB, with operational information that can inform its next guidelines on the concepts of controller and processor in the GDPR [26]. In particular, and in the context of the current paper, we would recommend to clarify the following aspects:

1. on defining purposes in practice: our work shows that a CMP influencing users decision-making with respect to accepting or rejecting pre-defined purposes actually renders such entity co-responsible for determining purposes;
2. on the role of deploying manipulative design in CMPs and whether this constitutes "essential means" of processing;
3. on the contractual agreement between publishers and CMPs: such agreement should mirror as much as possible the factual roles and activities they are involved in, pursuant to legal certainty and transparency;

Guidelines needed on "provision of services" for data processors. Data processors must limit its operations to carrying out the services for which the controller stipulated in the processing agreement. However, this design space is left to ambiguity and leeway in terms of what "providing the service" entails. Guidance is needed on what is considered to be *compatible and expected purposes* for the provision of their services/operations. For example, while security operations are surely expected, doubts remain regarding the provision of services which include other purposes that go beyond legal provisions and principles such as the compatibility between optimization of consent rate and legal compliance (as mentioned in Section 4.5); the EDPB [25, paragraph 27] mentions that such goal cannot be prioritized over the control of an individual's personal data: *an individual's control over their personal data is essential and there is a strong presumption that consent to the processing of personal data that is unnecessary, cannot be seen as a mandatory consideration in exchange for the performance of a contract or the provision of a service.*

DPAs should scale up auditing of CMPs. Currently, DPAs primarily use labour-intensive, small-sample, qualitative methods to evaluate the legal compliance of CMPs (e.g., the Irish DPA analysed consent pop-ups of 38 websites via a "desktop examination" [18]). Although our normative stance is that compliance evaluations should not be outsourced to algorithms and always involve human oversight, data-driven and automated tools could help DPAs gain a broader understanding of CMP design and compliance trends within their jurisdiction. Auditing can be automated (for example, with scraping technologies) to analyse the presence or absence of certain consent options (e.g., a reject button), interaction flows (e.g., number of clicks to access an option), or default settings (e.g.,

checked or unchecked choices). Not all requirements for consent are as binary and can be measured in this way (such as the quality of purpose descriptions), but gathering and continuously monitoring those aspects can provide DPAs with initial indications. These insights can be used to decide which follow-up investigations are necessary, and also which aspects might provide the biggest impact if addressed.

Automated auditing of CMPs requires extension of consent signal. The IAB Europe has created a standardised format for consent signals and successfully implemented APIs that allow various entities to interoperate with each other. Such consent was created to simplify the exchange of the digital version of consent between CMPs and advertisers. They do not, however, contain elements that could help DPAs and users to evaluate the *validity of collected consent* through automated means. We strongly suggest these standards and APIs should be expanded (or new ones developed by neutral parties) to include information about the interface design of a consent pop-up. Such extended digital format of consent will make consent services computationally legible by more actors, such as regulators and researchers.

Additionally, in the current IAB Europe TCF system, third-party advertisers (vendors) just receive a Consent Signal as a part of HTTP(S) request or via browser APIs, but there is no proof whether such Consent Signal is valid and whether a vendor actually received it (or, for example, did not generate it by itself instead). We recommend IAB Europe TCF to change this practice and to propose solutions that demonstrate evidence of consent collection and its integrity.

Guidance needed on validity of pre-registration of vendors. Through our analysis, we identified that CMPs have the capability to "pre-register" about 600 vendors during the installation process on a website. This pre-registration of vendors means that if the user accepts some of the purposes presented in the consent pop up, then all the vendors will be automatically added to a Consent Signal (see an example of OneTrust in section 4.4, where 632 vendors are allowed when the user clicks "Accept"). Consent stored by CMP in this case *pre-authorizes* processing of personal data for around 600 vendors, even if those vendors are not present on the website, thus making consent being collected *for future and unforeseen potential processing*. Therefore, such practice may violate the principles of transparency, fairness and minimization principles. We hope our analysis of the IAB Europe TCF and the capability of CMPs to pre-register vendors that do not yet process personal data, will help policy makers to provide further guidance on the validity of such practice.

Further recommendations are needed due to the decision-making power of consent pop-up providers. In this article, we have analysed two most popular CMPs in the EU – QuantCast and OneTrust– and detected several scenarios when consent pop-up providers can be considered data controllers due to the

enormous power of CMPs that can inject any type of additional functionality at any time in the banner, without the publisher being in position to technically know or oppose to it. We hope that policy makers take these scenarios into account and provide recommendations for such providers (either withing or outside of IAB Europe TCF) identifying which practices render them as data controllers and in which conditions they will be recognized as data processors.

6 Related work

Previous work analysing the role of CMPs in the advertising ecosystem have examined its technical functioning and interaction designs related to the applicable regulation, but have not inquired how they relate to their role as processors or controllers under the GDPR.

Degeling et al. [19] monitored the prevalence of CMPs on websites from January 2018 until May, when the GDPR came into effect, and measured an overall increase from 50.3% to 69.9% across all 28 EU Member States. Taking a longer view, Hils et al. [35] showed how the rate of adoption doubled year over year between June 2018 and 2020, and that CMPs are mostly used by moderately popular websites (albeit with a long tail of small publishers). Nouwens et al. [50] studied the use of dark patterns in the five most popular CMPs in the UK and estimated that only 11.8% of banners meet minimum legal requirements for a valid consent (reject as easy as accept, no pre-checked boxes, and no implied consent).

Focusing on the programmatic signals rather than user behaviour, Matte et al. [48] analysed 28,000 EU websites and found that 141 websites register positive consent even if the user has not made their choice and 27 websites store a positive consent even if the user has explicitly opted out. Additionally, Matte et al. [47] discuss the purposes and legal basis pre-defined by the IAB Europe and suggest that several purposes might not be specific or explicit enough to guarantee a valid legal basis, and that a large portion of purposes should require consent but are allowed by the TCF to be gathered on the basis of legitimate interest.

Data protection authorities across EU Member States have also reacted to the role and responsibility of CMPs, and issued various guidances. The Spanish DPA [4] asserts that as long as CMPs comply with the requirements for consent, they shall be deemed an appropriate tool. It recommends that CMPs " *must be submitted to audits or other inspections in order to verify that (...) requirements are complied with*". The Irish DPA [17] reiterates CMPs should be careful to avoid non-compliant designs already explicated as part of GDPR texts (e.g., pre-ticked boxes) and emphasises their accountability and transparency obligations (i.e., consent records) The Danish DPA asserts that whenever any entity integrates content from any third party (including CMPs), it is particularly important to be aware of its role in relation to its processing of personal data that takes place [16].

7 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 and APF'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. Deceived by design: How tech companies use dark patterns to discourage us from exercising our rights to privacy (2018), https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-by-design
2. 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
3. Advocate General Mengozzi: Opinion of Advocate General Mengozziin Jehovah's witnesses, C-25/17, ECLI:EU:C:2018:57, paragraph 68 (2018)
4. 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
5. Article 29 Working Party: Opinion 2/2010 on online behavioural advertising (WP 171) (2010), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf
6. Bielova, N., Santos, C.: 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
7. 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
8. 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

9. Cookiebot: Cookie scanner – revealer of hidden tracking (Sep 2020), https://www.cookiebot.com/en/cookie-scanner/
10. Cookiepedia Official website, https://cookiepedia.co.uk/
11. CookiePro: Lesson 3: Scan Results and Categorizing Cookies (Jul 2020), https://community.cookiepro.com/s/article/UUID-309d4544-c927-fe00-da50-60ed7668c6b5
12. CookiePro: Scanning a Website (Nov 2020), https://community.cookiepro.com/s/article/UUID-621498be-7e5c-23af-3bfd-e772340b4933
13. CookiePro by OneTrust: CookiePro Free IAB TCF 2.0 CMP Builder (nd), https://www.cookiepro.com/iab-tcf-2-builder/
14. Court of Justice of the European Union: Case 582/14 – Patrick Breyer v Germany (2016), ECLI:EU:C:2016:779
15. Crownpeak: Vendor categories (nd), https://community.crownpeak.com/t5/Universal-Consent-Platform-UCP/Vendor-Categories/ta-p/665
16. Danish DPA (Datatilsynet): Guide on consent. www.datatilsynet.dk/media/6562/samtykke.pdf (2019)
17. 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
18. Data Protection Commission (Irish DPA): Report by the DPC on the Use of Cookies and Other Tracking Technologies (2020), https://www.dataprotection.ie/en/news-media/press-releases/report-dpc-use-cookies-and-other-tracking-technologies
19. Degeling, M., Utz, C., Lentzsch, C., Hosseini, H., Schaub, F., Holz, T.: We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy. In: Network and Distributed Systems Security Symposium (2019)
20. 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
21. Europe, I.: 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.
22. European Court of Justice: Case 25/17 Jehovan todistajat, ECLI:EU:C:2018:551
23. European Court of Justice: Case C-40/17 Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV, ECLI:EU:C:2019:629
24. European Court of Justice: Case C-210/16 Wirtschaftsakademie Schleswig-Holstein, ECLI:EU:C:2018:388
25. 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
26. 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
27. Evidon: Quantcast-related pages on Evidon Company Directory (2017), https://info.evidon.com/companies?q=Quantcast [Consulted on Jan. 8th, 2021.]

28. Finck, M., Pallas, F.: They Who Must Not Be Identified – Distinguishing Personal from Non-Personal Data Under the GDPR. International Data Privacy Law **10** (2020)
29. Fouad, I., Bielova, N., Legout, A., Sarafijanovic-Djukic, N.: 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
30. Fouad, I., Santos, C., Al Kassar, F., Bielova, N., Calzavara, S.: 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
31. 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
32. Gray, C.M., Kou, Y., Battles, B., Hoggatt, J., Toombs, A.L.: The Dark (Patterns) Side of UX Design. In: Proceedings of the CHI Conference Human Factors in Computing Systems. p. 534 (2018)
33. Gray, C.M., Santos, C., Bielova, N., Toth, M., Clifford, D.: Dark patterns and the legal requirements of consent banners: An interaction criticism perspective. In: ACM CHI 2021 (2020), https://arxiv.org/abs/2009.10194
34. 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
35. Hils, M., Woods, D.W., Böhme, R.: Measuring the Emergence of Consent Management on the Web. In: ACM Internet Measurement Conference (IMC'20) (2020)
36. Hintze, M.: 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)
37. 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.
38. 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
39. IAB Europe: Vendor List TCF v2.0 (2020), https://iabeurope.eu/vendor-list-tcf-v2-0/
40. 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/
41. 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
42. Jared Spool: Do users change their settings? (2011), https://archive.uie.com/brainsparks/2011/09/14/do-users-change-their-settings/
43. Johnson, E.J., Bellman, S., Lohse, G.L.: Defaults, Framing and Privacy: Why Opting In-Opting Out. Marketing Letters **13**, 5–15 (2002)

44. Johnson, E.J., Goldstein, D.G.: Do Defaults Save Lives? Science **302**, 1338–1339 (2003)
45. Machuletz, D., Böhme, R.: Multiple purposes, multiple problems: A user study of consent dialogs after GDPR. In: Proceedings on Privacy Enhancing Technologies (PoPETs). pp. 481–498 (2020)
46. Maier, G., Feldmann, A., Paxson, V., Allman, M.: M.: On Dominant Characteristics of Residential Broadband Internet Traffic. In: In: Proceedings of the 9th ACM SIGCOMM conference on Internet measurement conference. pp. 90–102 (2009)
47. Matte, C., Santos, C., Bielova, N.: 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
48. Matte, C., Bielova, N., Santos, C.: 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)
49. Mishra, V., Laperdrix, P., Vastel, A., Rudametkin, W., Rouvoy, R., Lopatka, M.: Don't count me out: On the relevance of IP address in the tracking ecosystem. In: Huang, Y., King, I., Liu, T., van Steen, M. (eds.) WWW '20: The Web Conference 2020, Taipei, Taiwan, April 20-24, 2020. pp. 808–815. ACM / IW3C2 (2020). https://doi.org/10.1145/3366423.3380161, https://doi.org/10.1145/3366423.3380161
50. Nouwens, M., Liccardi, I., Veale, M., Karger, D., Kagal, L.: Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. In: CHI (2020)
51. OneTrust PreferenceChoice: Consent management platform (cmp), https://www.preferencechoice.com/consent-management-platform/, accessed on January 20, 2021.
52. Pawlata, H., Caki, G.: The Impact of the Transparency Consent Framework on current Programmatic Advertising Practices (2020), 4th International Conference on Computer-Human Interaction Research and Applications
53. Quantcast: Quantcast Choice (2020), https://www.quantcast.com/products/choice-consent-management-platform/
54. Quantcast: Quantcast Choice - User Guide (2020), https://help.quantcast.com/hc/en-us/articles/360052725133-Quantcast-Choice-User-Guide
55. Quantcast: Quantcast Choice Terms of Service (2020), https://www.quantcast.com/legal/quantcast-choice-terms-of-service/
56. Quantcast: Quantcast Measure and Q for Publishers Terms of Service (2020), https://www.quantcast.com/legal/measure-terms-service/
57. Quantcast: Quantcast Privacy Policy (2020), https://www.quantcast.com/privacy/
58. 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-
59. Quantcast: Quantcast Measure (2021), https://www.quantcast.com/products/measure-audience-insights/
60. Santos, C., Bielova, N., Matte, C.: 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), https://doi.org/10.26116/techreg.2020.009
61. Signatu: Trackerdetect (nd), https://signatu.com/product/trackerdetect/
62. Thaler, R.H., Sunstein, C.R.: Nudge: Improving Decisions About Health, Wealth, and Happiness. Yale University Press (2008)

63. TrustArc: Cookie Consent Manager (nd), https://trustarc.com/cookie-consent-manager/
64. Utz, C., Degeling, M., Fahl, S., Schaub, F., Holz, T.: (Un)informed Consent: Studying GDPR Consent Notices in the Field. In: Conference on Computer and Communications Security (2019)