Drivers and Obstacles for the Adoption of Consent Management Solutions by Ad-Tech Providers

Paulina Jo Pesch
Department of Computer Science, Security and Privacy Lab
University of Innsbruck
Innsbruck, Austria
paulina.pesch@uibk.ac.at

***Abstract*—In the world of online marketing, Consent Management Providers (CMPs) are on the rise. CMPs collect online users' consent to the processing of their personal data by publishers and ad-tech vendors. At the same time, there are reasonable doubts about the compliance of the existing market standard with the General Data Protection Regulation (GDPR). This could potentially create compliance risks for the companies adopting the standard, in particular for ad-tech vendors that – in the pre-CMP era – were invisible to users.**

This paper reveals drivers and obstacles for the adoption of the Transparency & Consent Framework (TCF) by ad-tech-vendors, gained in semi-structured interviews with representatives of Global Vendors List (GVL) members. Presenting the first qualitative study of ad-tech vendors' perspectives, the paper provides novel insights into the CMP ecosystem. It particularly shows existing market pressure and reveals ad-tech vendors' confusion and doubts about the TCF's compliance with the GDPR.

***Index Terms*—Consent management, CMPs, ad-tech vendors, GDPR, TCF, online advertising, cookies**

I. Introduction

Ad-tech vendors are providers of technology solutions integrated in online-advertising supply chains. Their ad-tech solutions are embedded in websites by the website publishers. Since the personalisation of ads is widely believed to increase revenues [5] [33] [34] (but see [31]), many ad-tech vendors' business models require the processing of personal data. Before Consent Management Providers (CMPs) have been involved in the ecosystem, ad-tech vendors could not collect consent because they were invisible to the user. The user interacted with the website publisher only, and could see which advertisers' ads they were presented with. *Fig. 1*, for this set-up, illustrates the relationships between the user, the publisher and the ad-tech vendor in the pre-CMP era.

The General Data Protection Regulation (GDPR) [41] coming into effect was a significant driver in CMP adoption [22]. Albeit the GDPR has hardly changed the framework for the processing of personal data in comparison to the EU Data Protection Directive [17] and the national law it had been transposed to, the GDPR – most likely due to its heavy fines – has noticeably increased the collection of online users' consent. Now, online users come across CMPs' consent management dialogues constantly [22] [35] [38]. Through consent dialogues, users are informed about the use of cookies and asked to give their consent. In addition to an "accept"-button

Fig. 1: The relationship between user, publisher and ad-tech vendor in the pre-CMP era.

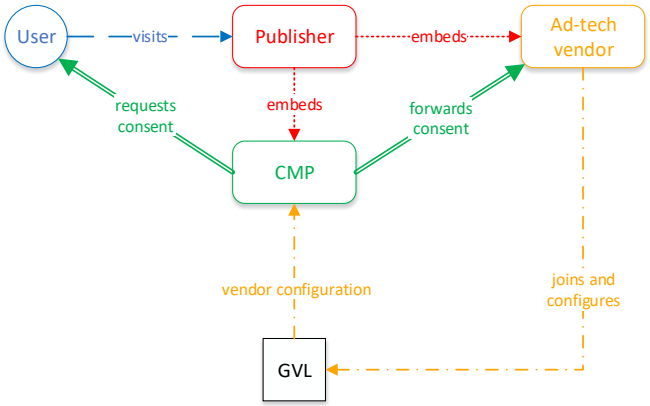

Fig. 2: The relationship between user, publisher, ad-tech vendor, and CMP in the CMP era.

the consent dialogue usually comprises a huge list of ad-tech vendors, a list of purposes that data are processed for, and the options to refuse consent or consent to the data processing for certain purposes or by certain ad-tech vendors only. *Fig. 3* shows a screenshot of a Quantcast [40] consent dialogue. *Fig. 4* shows a screenshot of the list of ad-tech vendors behind the "partners" link in this consent dialogue. Both screenshots were taken in July 2021. Even though designs and default settings diverge, most consent dialogues look fairly similar because they follow a common framework.

In order to create an industry standard approach to GDPR compliance, the Interactive Advertising Bureau (IAB) created the Transparency & Consent Framework (TCF) [26] [29] that consists of a set of technical specifications and policies for CMPs, ad-tech vendors and publishers [27]. *Fig. 2* illustrates the relationships between the user, the publisher, the CMP, and the ad-tech vendor after the adoption of the TCF. The publisher embeds not only ad-tech vendors but also a CMP.H

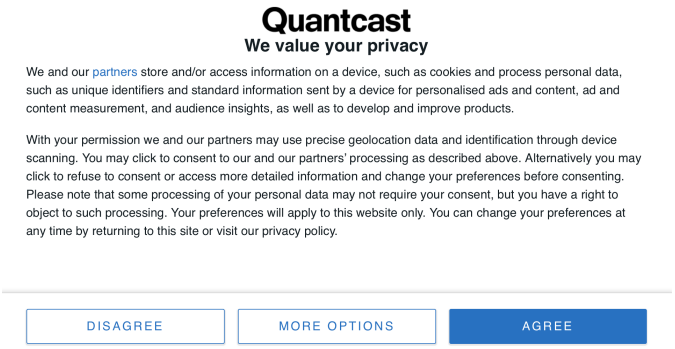

Fig. 3: Screenshot of the Quantcast consent dialogue embedded on Quantcast's own website.

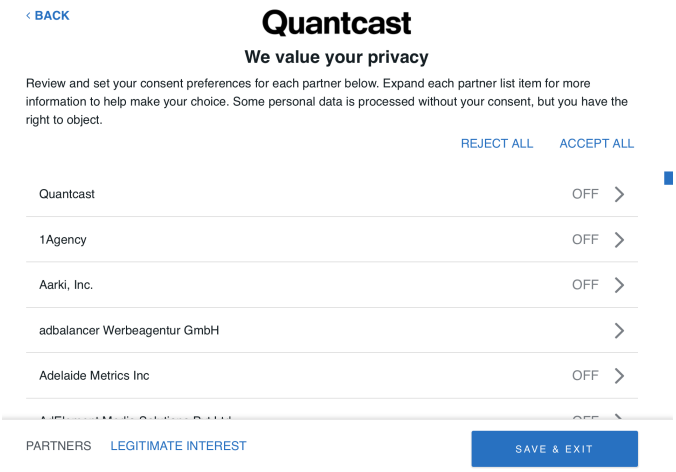

Fig. 4: Screenshot of the list of partners linked in the Quantcast consent dialogue.

Ad-tech vendors who wish to operate under the TCF, must join the Global Vendors List (GVL) that is steadily growing, listing 730 members in May 2021 [25]. They configure their membership by declaring the purposes they process data for, choosing from the purpose definitions in Appendix A of the TCF Policies [27]. Also, the ad-tech vendors, with their configuration, decide for which of these purposes they claim legitimate interest, i.e. for which purposes they process data even without users' consent. When a user visits the publisher's website they are presented with the CMP's consent dialogue. The CMP

- informs the user about the ad-tech vendors that shall receive the user's personal data,
- the purposes they process data for,
- to which extent legitimate interest is claimed, and
- requests the user to consent to the processing of their data for the purposes the ad-tech vendors wish to collect consent for. If the user clicks that they accept the data processing, an affirmative consent signal is created and forwarded to the ad-tech vendor.

In May 2021 the IAB lists 125 CMPs [24]. The number of publishers operating under the TCF is unspecified large, cf. [22]. The TCF consent signal is now the dominant type of privacy preference signal and the first one that has been widely adopted among ad-tech vendors [23]. There is some evidence that implies ad-tech vendors could incentivise publishers to adopt the TCF.

First legal analyses have come to the conclusion that widely adopted consent management solutions are not compliant with the GDPR [35] [36] [38] [44]. Also, some national supervisory authorities have issued publications [13] [30] and made decisions [14] [15] [19] [20] that indicate that common consent dialogues do not meet the legal requirements. Furthermore, some national supervisory authorities imposed heavy fines for the processing of personal data based on insufficient consent [15] [19] [20] [21]. This potentially exposes companies in the online-advertising ecosystem to compliance risks. While users' behavior has been subject to research [32] [43] the decisions of online marketing companies are not yet understood well. Aiming at filling this research gap, ad-tech vendors are the most promising starting point. Since ad-tech vendors expose themselves through TCF adoption, their behavior under the TCF is well measurable, and they are likely to provide crucial insights to drivers and obstacles of TCF adoption. Therefore, this paper focuses on the perspective of ad-tech vendors. It presents the first qualitative study on ad-tech vendors views on TCF adoption and compliance.

Section II presents the high-level research questions. Section III explains the empirical approach. I summarise the interview results in section IV. Eventually, in section V I draw a conclusion and outline future work.

II. High-level research questions

I had two high-level research questions regarding the decision-making of ad-tech vendors in the context of the TCF. Firstly, I aimed to find out about ad-tech vendors' reasons for joining the GVL and the considerations that led them to their specific configuration (section II-A). Secondly, I wanted to know whether ad-tech vendors see compliance risks of the GVL membership (section II-B).

A. What drives GVL adoption and configuration?

In order to learn about ad-tech vendors' perspectives on consent management under the TCF, I want to know why ad-tech vendors join the GVL, and what is their reasoning when setting their configuration.

a) Why ad-tech vendors join the GVL: It is questionable why ad-tech vendors decide to join the GVL. One possible reason is GDPR compliance, specifically the use of CMPs for consent collection. However, it seems possible that publishers are driving forces. Ad-tech vendors depend on being embedded by publishers that therefore potentially influence ad-tech vendors' decisions. There are sound reasons for publishers to prefer collaborating with GVL members. CMPs offer a free service enabling publishers not only to collect consent to the processing of personal data by all GVL members, but also to obtain it in a standard format that can be transferred across firms [45].

b) How ad-tech vendors set their configuration: Also, it is questionable what drives ad-tech vendors' configuration decisions. These comprise, in particular, the selection of data processing purposes out of the list of purposes defined in Appendix A of the TCF Policies [27], and legal bases. The French data protection authority (CNIL) has found the purpose definitions unclear, not comprehensible for users, and thus not ensuring informed consent [14]. This led me to the question what ad-tech vendors think about the TCF purpose definitions.

Also, ad-tech vendors' choices of legal bases are worth examining. The TCF allows for both, requesting consent (Art. 4 No. 11, Art. 6 (1) (a) GDPR [41]), and claiming legitimate interest (Art. 6 (1) (f) GDPR [41]) [27]. While consent requires a decision of the user, legitimate interest can be claimed where the processing of the personal data is "necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject" (Art. 6 (1) (f) GDPR [41], also see [2]).

It is noteworthy that the TCF includes the option of "flexible purposes." Ad-tech vendors who use this option for certain purposes select a default legal basis, but leave the decision whether to collect consent or to claim legitimate interest to the publishers. This suggests that publishers might influence ad-tech vendors' selection of legal bases. As publishers generate revenues by placing ads on their websites, they have an own interest in the data processing. They could either prefer to claim legitimate interest since users do not need to consent where legitimate interest is claimed. Or they could want to collect consent to avoid risk: Where legitimate interest can be claimed, basing data processing on consent is legal. By contrast, where consent is necessary, claiming legitimate interest is insufficient. Alternatively, they could seek to collect commoditised consent as an asset that can be transferred and monetised [45].

B. Do ad-tech vendors see compliance risks of the GVL membership?

Apart from ad-tech vendors' drivers for TCF adoption and configuration, I aimed to learn about their obstacles, particularly compliance risks of the GVL membership itself.

a) Lawfulness of the processing: A compliance risk could result from unlawful processing of personal data under the TCF. It has been pointed out that the consent collection under the TCF does not meet the requirements of the GDPR [41], laid down in Art. 4 No. 11, Art. 7, recitals 32, 42, particularly

- where cookies are stored before the user has made their choice [35],
- where cookies are stored even if the user has clicked a reject button [35],
- where the option to refuse or manage consent is hidden / requires more clicks [13] [38],
- because the withdrawal of consent is not as easy as giving it [44],
- because of the obscurity of purpose definitions [14] [36], and
- because consent is collected for too many ad-tech vendors [30] [44].

Also, the UK's data protection authority ICO, in the context of real-time bidding, has stated that the use of advertising cookies always required consent, i.e. companies cannot claim legitimate interest as a legal basis for the processing [30]. The German Federal Supreme Court has ruled [7] that advertising cookies used to create user profiles required consent, arguing with Art. 5 para. 3 of the ePrivacy Directive [16] (on the interplay between the ePrivacy Directive and the GDPR see [18]).

Against this background, I wanted to learn about ad-tech vendors' perspective on the consent collection under the TCF, and the compliance of the TCF and the companies adopting it.

b) Liability as joint controllers: Furthermore, the roles and responsibilities of ad-tech vendors and others in the framework are subject to legal uncertainty. Only a few papers have addressed the potential responsibility of companies operating under the TCF as joint controllers [6] [42] [44]. The CJEU interprets both terms, "controllership" [8] and "joint control" [9] [10] [11] broadly. Ad-tech vendors could be considered joint controllers with publishers or CMPs, and thus be subject to the specific transparency requirements laid down in Art. 26 GDPR [41]. In fact, the Danish supervisory authority *Datatilsynet* has stated the Danish weather forecast website *DMI.dk* and Google are joint controllers regarding advertising cookies used for Google banner ads [15]. I wanted to know whether ad-tech vendors take a potential joint controllership with others under the TCF into consideration.

III. Empirical Approach

Firstly, I had a look at the "bigger picture" based on measuring data on ad-tech vendors' GVL configurations (section III-A). Secondly, based on the measurement data, I selected, approached and interviewed ad-tech vendors (section III-B).

A. Measurement basis

In a first step, I gained insights into ad-techs vendors' behavior from data that I was provided with by *Hils et al*. *Hils et al.* gathered data through browser crawls, by systematically downloading the GVL, and in a field experiment with real consent dialogues [22] (also see [23]). Reaching back to September 2019, the weekly updated data particularly comprise, for each GVL member, the TCF v2.0 [29] purposes and legal bases for the data processing, and, if used, the "flexible purposes". The data reveal some ad-tech vendors, over time, changed the legal bases for certain purposes, and many use the "flexible purpose" option, several even for purposes they collect consent for by default (see section II-A b). I used the GVL data for both, selecting potential interview partners, and preparing for each interview.

B. Vendor interviews

In a second step, I carried out semi-structured interviews. I decided to conduct semi-structured interviews rather than a questionnaire based on the experience that interviewees are more likely to build trust and provide me with deeper insights in a more natural, conversational atmosphere. Based on my high-level research questions (see section II), I prepared interview guidelines (see Appendix) covering three areas of GDPR compliance:

- The first part includes general questions on data protection compliance, such as questions about the persons involved in compliance decisions, experiences with user requests or supervisory authorities.
- The second part concerns the GVL membership, e.g. the decision to join the GVL and compliance risks arising from the membership itself.
- The third part covers details of the membership, particularly the configuration of purposes and legal bases and the compliance of others operating under the TCF.

I carried out seven interviews, in two rounds. Some of the interviews were held in English, and some in German. I asked the interviewees to participate in confidential interviews. In the first round, assuming ad-tech vendors might not want to share confidential information on their possibly noncompliant data processing in video calls, I approached a set of German ad-tech vendors that I could offer face-to-face meetings. In that first round, in July 2020, I invited 21 ad-tech vendors to confidential interviews. Four of them were willing to participate. I carried out all four interviews in July 2020.

Since the number of responses was low, in a second round, I approached international members of the GVL. In order to reasonably limit the number of contacted vendors, I approached only those who met the following criteria:

- The ad-tech vendor is processing data for at least seven purposes from the TCF Policies, Appendix A,
- claims legitimate interest for at least one of them, and
- uses the "flexible purpose" option where publishers can freely decide whether to ask users for consent or claim legitimate interest for the concerned purposes,
- while the "flexible purposes" are not identical with those the vendor, by default, claims legitimate interest for.

With this selection criteria I could reach ad-tech vendors with a rather broad data processing (for at least seven purposes) and a configuration that raises specific compliance issues (claiming legitimate interest and letting publishers flexibly claim legitimate interest even for purposes that they themselves seem to deem consent necessary for). In November, I could reach out to 37 of the 42 ad-tech vendors that met that criteria, and to eleven of these again via another channel. Eventually, in the second round of interviews, I carried out three interviews, one in December 2020, one in January 2021, and the last one in February 2021.

The three interviews cover approximately 7% of the GVL ad-tech vendors meeting the criteria. With seven interviews in total, I cover approximately 1% of all GVL ad-tech vendors (in May 2021). The ad-tech vendors interviewed had diverse business models and differed in size. The smallest company had less than 15 employees, the biggest had a team of more than 150 people.

The interview partners had different backgrounds and functions. The interviewees had academic backgrounds in computer science, business informatics, legal studies, social and political sciences and natural sciences. Four of them were in their companies' management, two served as their companies' data protection officers (DPOs). Thus, no interviewee could answer all questions. However, every interviewee was involved in TCF decision-making and/or configuration in their company. *Table I* provides an overview about the backgrounds and functions of the interviewees.

TABLE I: Backgrounds of interviewees

Backgrounds	**Fraction**
Computer science	2/7
Business informatics	1/7
Legal studies	1/7
Social and political sciences	2/7
Natural sciences	1/7
Functions	**Fraction**
Management (CEO or CTO)	4/7
DPO	2/7

Out of all seven ad-tech vendors, six use the "flexible purpose"-option. Only two use the option only for purposes they claim legitimate interest for by default. For all ad-tech vendors, the data shows changes in purposes and/or legal bases.

C. Research ethics

I anonymised all responses in publications to protect the participants. On the one hand, this ensures the privacy of the interviewees themselves, protecting them against potential consequences based on the individual statements they made in the interviews. On the other hand, keeping the companies participating in the interviews unidentifiable is necessary for fairness reasons. This study aims to understand system wide effects of the TCF and does not focus on individual actors. I do not expose those who were willing to participate in the interviews to a higher risk of facing negative legal or economical consequences than equally acting ad-tech vendors that did not participate. In order to keep the interviewees strictly anonymous, I do not reveal any specific information about the business models of the ad-tech vendors that participated in the study. Consequently, in this paper I do not assess specific legal statements of the interviewees against the background of their business models.

IV. Results

The depth of seven interviews revealed aspects of the decision-making helpful to understand the status quo.

A. Ad-tech vendors' drivers

a) GDPR compliance: GDPR compliance, in general, turned out to be an important aspect for all ad-tech vendors participating. Six out of seven interviewees stated that at least three persons in the company were involved in decisions related to GDPR-compliance. Only in two companies there is no lawyer involved, in one the lawyer is seldomly involved in the decision-making and not at all involved in the TCF configuration. Four of the interviewed companies involve external lawyers respective DPOs. Three explicitly stated that the management was involved. *Table II* provides an overview of the most important statements of the ad-tech vendors on GDPR compliance and decision-making.

TABLE II: GDPR compliance and decision-making

Statements	Fraction
High relevance of GDPR compliance	7/7
At least 3 people involved in GDPR-related decisions	6/7
Lawyers involved in GDPR-related decisions	5/7
External lawyers/DPOs involved in GDPR-related decisions	4/7

One interviewee stated that their company used 20 percent of the capacity for GDPR compliance in the last three years. The others could not quantify their effort for GDPR compliance in general. Two interviewees were able to quantify their effort regarding the TCF, though. For all of them, the initial implementation and configuration of the TCF, and the migration to version 2 [28] caused the biggest effort. One of the companies had an effort of 15 hours for implementing and configuring version 1, while changing to version 2 required them 50–60 hours of work. One company even had an initial implementation effort of a few person months.

b) CMP use: While GDPR compliance is important for the ad-tech vendors, consent collection through CMPs did not turn out to be their main driver for TCF adoption. None of the interviewees specifically named the use of CMPs as a reason to adopt the TCF. One interviewee explicitly stated that CMP use was not their reason for joining the GVL even though they collected consent via CMPs. One interviewee said that their company did not collect consent via CMPs, another one said their company did not collect consent at all. This may be correct insofar as that CMPs are not embedded by ad tech vendors but by publishers, but ultimately ad-tech vendors receive users' consent information from CMPs (c.f. fig. 2). For example, I can see that the CMP Quantcast Choice [40] collects consent for all ad-tech vendors interviewed. I registered with this CMP as a publisher and see that, under the default settings, all GVL members would show up in the consent dialogue embedded to my website.

c) Market pressure: With respect to the TCF, the interviews revealed that regarding both, joining the GVL and deciding about their configuration, ad-tech vendors are subject to market pressure.

Of the seven interviewees, only three stated that their GVL membership was their independent decision. One of them made this choice to exploit synergies with others. The other two deemed a standardisation desirable. One of them gave the many different interpretations of the GDPR's rules as the main reason and pointed out a common standard mitigated the risk of getting fined under the GDPR. The interviewee explained that supervisory authorities would rather not target single companies for using a standard adopted by many. The other one added, leaving the TCF would cause high expenses, while the scalability of a standard would come with the problem of of a consent collection for too many companies at once. Four interviewees said their companies were not free to decide whether to join the GVL or not. One of them noted that their business model forced them to join the GVL because the use of the OpenRTB API (an open API by the IAB for real-time bidding) required being member of the GVL. Another interviewee, similarly, explained that leaving the GVL would be a "major blow" causing "parts of the value chain to collapse". One interviewee stated that advertisers demanded GVL membership – even though their own data processing would not require consent. By this, the advertisers themselves could directly get personal data. Another interviewee confirmed the pressure to be part of the GVL. They said, being member of the GVL was "business necessary". They explained that Supply Side Platforms (SSPs) in the real-time bidding ecosystem required GVL membership. They added that their company was forced to process personal data, since their business model did not require or substantially benefit from targeting. *Table III* provides an overview of the reasons given for joining the GVL.

TABLE III: Drivers for TCF adoption

Reasons given for joining the GVL	Fraction
Collecting consent through CMPs	0/7
Desirability of a market standard	2/7
Market pressure (from publishers, advertisers or SSPs)	4/7

Three of the seven interviewees stated that their configuration was also affected by market pressure. All of these three used flexible purposes because of the publishers. Two of them said the publishers required flexibility. One pointed out that some publishers did not want to claim legitimate interest but collected consent for all purposes. Another interviewee whose company uses flexible purposes claimed that their configuration did not matter because they did not collect consent at all. As pointed out in the context of CMP use, CMPs collect consent for all GVL members.

d) Experiences with user requests and supervisory authorities: While there is market pressure especially from publishers and advertisers, users or supervisory authorities do not put ad-tech vendors under significant pressure. It showed that the ad-tech vendors have hardly had any issues with user requests or supervisory authorities so far, neither before nor after TCF adoption. One said that even though the TCF was noncompliant, they were not afraid of the supervisory authorities since these would seek pragmatic solutions rather than fining single companies. Two stated that they have no experiences with supervisory authorities, one had one sin-

gle case of one data subject's complaint. Only one of the interviewees reported a substantial number of deletion or information requests. However, the interviewee explained that a high number of requests had occured in 2018 only, and, apart of that, the company had only "a fistful of deletion requests". Four interviewees quantified user requests. One interviewee stated that their company had received only 15 e-mails by users of whom none requested deletion of their personal data. Another ad-tech vendor had two requests for deletion all-time. One stated, they have been contacted directly by 1–2 users only and had gotten a few requests through service companies, and thus could easily handle their requests manually. Another ad-tech vendor stated their company had received requests only via advertising clients and CMPs. This interviewee said that they were surprised about the latter since the company did not use CMPs at all. As stated above in the context of CMP use, CMPs collect consent for all GVL members.

B. Ad-tech vendor's obstacles: Compliance risks of TCF adoption

Some ad-tech vendors identified risks associated with the TCF. Several interviewees are highly aware of serious deficiencies of the framework. However, the vast majority of the interviewees did not see compliance risks for themselves in being member of the GVL, although a majority of the interviewees deemed the TCF noncompliant. Only one interviewee saw compliance risks in the GVL membership itself, but did not expect a fine because the supervisory authorities would seek pragmatic solutions rather than fining companies. The interviewee particularly pointed out that the authentication of consent signals under the TCF was insufficient. Five interviewees did not see a compliance risk in being a GVL member. However, four of these interviewees also stated that the TCF itself was noncompliant.

Five interviewees made statements on the TCF purpose definitions, revealing confusion among ad-tech vendors. All of them considered the definitions very complex. Four of them said the purpose definitions were unclear. One of the four stated that they were "a bit messy". Two said, the purposes were hard to understand, one added that users could not understand the purposes. One interviewee admitted that their company just interpreted the purpose definitions in their own favor. This interviewee gave "performance measurement" as an example for an unclear purpose that could refer to the user performance "such as cursor position or user behavior" or to the "performance of the marketing KPI". One interviewee expressed that the unclear purpose definitions were a "huge problem in the industry" and many came up with "wild constructions" claiming legitimate interest for very targeted advertising. Two of the interviewees stated that the granularity of the purpose definitions in TCF v2.0 [29] was an improvement compared to TCF v1.1. One of them pointed out that users were not able to understand the definitions. This interviewee expressed the expectation that a new version would follow soon.

The interviews showed that ad-tech vendors are aware of unlawful behavior of others operating under the TCF while most do not systematically control others or take action in cases of unlawful behavior. Four interviewees stated that others behaved unlawfully under the framework. One of them said that they knew many publishers would design the consent dialogues in an unlawful way. One interviewee noted that the default-settings in the consent dialogues were often illegal, in particular, some publishers would use opt-out. *(The CJEU clearly stated this is noncompliant in [12], also see [1].)* One interviewee stated some publishers would send affirmative consent signals that are not based on a click of a user. One pointed out that ad-tech vendors' interpretations of the scopes of the purposes varied substantially, and that some even targeted users on the postal code level claiming legitimate interest. Another told me about an ad-tech vendor that created user profiles without consent, claiming legitimate interest. Another interviewee said, other ad-tech vendors, just as themselves, interpreted the unclear purposes in their own favor. One stated that for many users it was practically impossible to revoke consent because the option is hidden or not available. Another one stated that users could not directly revoke their consent because they could not assign consent signals to certain persons.

Only one of the interviewed ad-tech vendors said that they looked at consent dialogues systematically and found many unlawful designs. However, the interviewee stated this had no consequences because their company was too small and thus not influential enough. This interviewee even said they were thinking about an alternative framework for better data protection. Two interviewees made clear that their companies just assumed others under the TCF act compliant, despite having named specific noncompliant behavior of others in the course of the interview. *Table IV* provides an overview of the most important statements of the ad-tech vendors regarding compliance risks.

TABLE IV: Compliance risks

Statements	Fraction
Compliance risk posed by the GVL membership itself	1/7
Complexity of TCF purpose definitions	5/7
Unclarity of TCF purpose definitions	4/7
Unlawful behaviour of others under the TCF	4/7
Systematic monitoring of consent dialogues	1/7

Three interviewees – that did not see a risk in the GVL membership itself – considered their companies mere processors (Art. 28 GDPR [41]). None of the interviewees considered their company and others operating under the TCF being joint controllers without additional bilateral contracts. One interviewee explained agreeing on joint control contracts was one of the only changes with the GDPR. However they stated that their company only deemed necessary agreements with specific partners, but not with all publishers that collect consent for them via CMPs.

V. Conclusion and Future Work

My interviews provide initial answers to the high-level research questions. While GDPR compliance, in general, turned out to be important for the interviewees, the consent collection through CMPs was not their main driver for TCF adoption. The interviews revealed that market pressure is an important driver for both, TCF adoption and configuration. One could state, this constitutes a double "privacy paradox" (cf. [3] [4] [37]): On the one hand even privacy aware users' consent is collected, on the other hand even privacy friendly market actors participate in the framework and process more data than they would want to. Some companies feel forced to participate in the framework and to set their configuration in certain ways. The interviews particularly confirmed the big influence of publishers, but also advertisers.

The ad-tech vendors identified risks to TCF adoption. There is a high awareness of GDPR violations in the sector while none of the interviewees reported to take action in concrete cases of violations by others operating under the TCF. However, those ad-tech vendors who were aware of the weaknesses of the GVL itself, did not deem GVL membership a compliance risk for themselves. This seems to reveal cognitive dissonance but makes sense against the background of non-existent pressure from users and supervisors. The absence of consequences might also explain why two of the interviewees were not even aware of the fact, that a CMP collects consent for them. In the meantime, in May 2021, the NGO *noyb* ("none of your business") has initiated a large scale complaint wave against publishers using unlawful cookie banners [39]. The impact of this initiative remains to be seen.

Several open research questions call for further research. In order to gain a deeper understanding of the ecosystem, the empirical approach must be applied to a larger number of online marketing companies operating under the TCF. Based on the insights gained through the ad-tech vendor interviews, future work should especially focus on the perspective of publishers, but also take into account advertisers and CMPs. One next step is interviewing publishers to learn about their reasons for the adoption of the TCF, demanding certain configurations, and their opinions on compliance risks of TCF adoption. Data collected by *Hils et al.* [22] will enable me to select potential interview partners based on consent dialogue designs and the use of the flexible purpose option.

Future work should also include an in-depth legal analysis that was not part of this paper that focused on ad-tech vendors views and opinions. A thorough analysis of the consent collection through CMPs is still missing. Not all weaknesses of CMP consent collection have been carefully assessed yet. In particular, questions of controllership and particularly joint control have not been analyzed in detail. The insights gained in interviews with ad-tech vendors and others operating under the TCF form a basis for a profound legal analysis.

Both, an in-depth legal analysis and a deeper understanding of the ecosystem, will allow for the development of pragmatic concepts to strengthen data protection online.

Acknowledgment

I express my gratitude to Rainer Böhme, Maximilian Hils and Daniel Woods for making me aware of the research gap, helping me with the development of the empirical approach, providing me with data on ad-tech vendors' configurations under the TCF, and valuable comments. Also, I thank the anonymous reviewers for helpful remarks.

References

[1] Advocate General Szupunar on case C-673/17 (Planet49), 2019.

[2] WP 217 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC Adopted on 9 April 2014.

[3] A. Acquisti, and R. Gross, "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook", in: Privacy Enhancing Technologies, Proceedings of the 6th International Workshop, PET 2006.

[4] S. B. Barnes, "A privacy paradox: Social networking in the United States", First Monday, Volume 11, Number 9, 2006.

[5] H. Beales, "The Value of Behavioral Targeting, Network Advertising Initiative", 2010.

[6] N. Bielova, and C. Santos, "RE: Call for Feedback regarding Guidelines 07/2020 on the concepts of controller and processor in the GDPR", 2020.

[7] *Bundesgerichtshof*, Urt. v. 28.05.2020 – I ZR 7/16 (Cookie-Einwilligung II).

[8] Court of Justice of the European Union, judgement from 13 May 2014 – C-131/12 (Google Spain, Google).

[9] Court of Justice of the European Union, judgement from 5 June 2018 – C-210/16 (Facebook fan pages).

[10] Court of Justice of the European Union, judgement from 10 July 2018 – C-25/17 (Jehova's witnesses).

[11] Court of Justice of the European Union, judgement from 29 July 2019 – C-40/17 (Fashion ID).

[12] Court of Justice of the European Union, judgement from 1 October 2019 – C-673/17 (Planet49).

[13] Commission Nationale de l'Informatique et des Libertés, Délibération n° 2019-093 du 4 juillet 2019 portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture ou écriture dans le terminal d'un utilisateur (notamment aux cookies et autres traceurs) (rectificatif), 2019.

[14] Commission Nationale de l'Informatique et des Libertés, Décision MED-2018-042 du 30 octobre 2018.

[15] Datatilsynet, "DMI's behandling af personoplysninger om hjemmesidebesøgende", 11 February 2020, accessible under https://www.datatilsynet.dk/afgoerelser/afgoerelser/2020/feb/dmis-behandling-af-personoplysninger-om-hjemmesidebesoegende.

[16] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

[17] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

[18] European Data Protection Board, "Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities ", 2019.

[19] European Data Protection Board, "Polish DPA: Withdrawal of consent shall not be impeded", 2019, accessible under https://edpb.europa.eu/news/national-news/2019/polish-dpa-withdrawal-consent-shall-not-be-impeded_en.

[20] European Data Protection Board, "The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC", 2019, accessible under https://edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en.

[21] European Data Protection Board, "THE ITALIAN SUPERVISORY AUTHORITY FINES ENI GAS E LUCE EUR 11.5 MILLION - On account of unsolicited telemarketing and contracts", 2020, accessible under https://edpb.europa.eu/news/national-news/2020/italian-supervisory-authority-fines-eni-gas-e-luce-eur-115-million-account_en

[22] M. Hils, D. W. Woods, and R. Böhme, "Measuring the Emergence of Consent Management on the Web, in: Internet Measurement Conference (IMC)", ACM, 2020.

[23] M. Hils, D. W. Woods, and R. Böhme, "Privacy Preference Signals: Past, Present and Future", in: Proceedings on Privacy Enhancing Technologies, 2021.

[24] Interactive Advertising Bureau, accessible under https://iabeurope.eu/cmp-list/.

[25] Interactive Advertising Bureau, Global Vendor List, accessible under https://iabeurope.eu/vendor-list/.

[26] Interactive Advertising Bureau, Transparency & Consent Framework, accessible under https://iabeurope.eu/transparency-consent-framework/.

[27] Interactive Advertising Bureau, IAB Europe, Transparency & Consent Framework Policies, accessible under https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/.

[28] Interactive Advertising Bureau, Transparency & Consent Framework TCF v2.0 Switchover Q&A, accessible under https://iabeurope.eu/uncategorized/tcf-v2-0-switchover-qa/.

[29] Interactive Advertising Bureau, Transparency & Consent Framework TCF v2.0, accessible under https://iabeurope.eu/tcf-2-0/.

[30] Information Commissioner's Office, "Update report into adtech and real time bidding", 2019, accessible under https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf.

[31] N. Lomas, "Data from public broadcaster shows the value of ditching creepy ads", 2020, accessible under https://tcrn.ch/3huBy67

[32] D. Machuletz, and R. Böhme, "Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR", in: Proceedings on Privacy Enhancing Technologies, 2 (2020), 481–498.

[33] P Manchanda, J.-P. Dubé, K. Yong Goh, and P. K. Chintagunta, "The Effect of Banner Advertising on Internet Purchasing", Journal of Marketing Research, Vol. XLIII (February 2006), 98–108.

[34] V. Marotta, C. Abhishek, and A. Acquisti, "Online Tracking and Publishers' Revenues: An Empirical Analysis", Workshop of Information Systems Economics (WEIS), Boston, 2019.

[35] C. Matte, N. Bielova, and C. Santos, "Do Cookie Banners Respect my Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework", in: IEEE S&P 2020, arXiv:1911.09964v2.

[36] C. Matte, C. Santos, and N. Bielova, "Purposes in IAB Europe's TCF: Which Legal Basis and How Art They Used by Advertisers?", in Proceedings of the 8th Annual Privacy Forum, APF 2020.

[37] P. A. Norberg, D. R. Horne, and D. A. Horne, "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors", in: Journal of Consumer Affairs, Vol. 41, No. 1 (2007), 100–126.

[38] M. Nouwens, I. Liccardi, M. Veale, D. Karger, and L. Kagal, "Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence", in: Proceedings of CHI '20 CHI Conference on Human Factors in Computing Systems, April 25–30, 2020, Honolulu, HI, USA.

[39] Noyb, "noyb aims to end "cookie banner terror" and issues more than 500 GDPR complaints", accessible under https://noyb.eu/en/noyb-aims-end-cookie-banner-terror-and-issues-more-500-gdpr-complaints.

[40] Quantcast, Quantcast Choice, a free consent management platform, accessible under https://www.quantcast.com/de/produkte/choice-consent-management-platform/.

[41] 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).

[42] C. Santos, M. Nouwens, M. Toth, N. Bielova, and V. Roca, "Consent Management Platforms under the GDPR: processors and/or controllers?", 2021, arXiv:2104.06861v1.

[43] C. Utz, M. Degeling, S. Fahl, F. Schaub, and T. Holz, "(Un)informed Consent: Studying GDPR Consent Notices in the Field, in: 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), London, ACM 2020.

[44] M. Veale, and F. Z. Borgesius, "Adtech and Real-Time Bidding under European Data Protection Law" [preprint], accessible under https://osf.io/preprints/socarxiv/wg8fq/.

[45] D. W. Woods, and R. Böhme "The Commodification of Consent", in: Workshop on the Economics of Information Security (WEIS), Belgium 2020.

APPENDIX: INTERVIEW GUIDELINES

A. General questions on GDPR compliance and decision-making

1) Please describe your internal GDPR compliance decision-making process. Who is involved, who initiates decisions?
2) Can you estimate the internal effort and expenses for GDPR compliance / for the decision-making and implementation relating to the GVL?
3) Do you involve external consultants?
4) Do you observe other companies' GDPR compliance strategies or consult with other companies? If so, which companies and why?
5) Have you made bigger changes because of the GDPR? Have you increased your budget for GDPR compliance? Regarding data protection, would you describe your company as an early adopter or rather a follower?
6) If you changed a lot because of the GDPR: Was that because the requirements for you changed (compared to the Directive and respective national law), or because the GDPR allows for huge fines in case of incompliance?
7) Have you been involved in any legal dispute or proceeding related to the GDPR? If so, can you tell me more about it (judicial or extra-judicial; any supervisory autority involved; what about)?
8) What are your experiences with user requests?

B. Consent and joining GVL

1) How have you learned about the GVL and the option to join? By whom and in which way was the GVL promoted?
2) How did you make the decision to join the GVL? Which persons in the company participated in the decision-making process?
3) Does the GVL membership pose any compliance risks?
   a) If so: Which risks (e.g. reputation, liability)?
   b) If so: Why do you take these risks?
4) Which role and responsibility do you consider your company to have under the GDPR, particularly in relation to publishers and CMPs? Do you think any of you are processors (that process data on behalf of controllers)? Do you think there are joint controllers (Art. 26)?
5) Do you have any data processing agreements or other contracts related to data protection law with the other actors that process data under the TCF (e.g. according to Art. 26)?
6) Do you collect user consent via CMPs only or also in other ways?
7) How do you document the consent collected via CMPs?
8) Do you also serve as a publisher, collecting consent for other GVL vendors? If not, how do you collect consent from users of your website?
9) If you are also a publisher but do not use a CMP under TCF there, what are the reasons for participating in the TCF as a vendor but not as a publisher?
10) Do you know how many vendors are members of the GVL? Do you think it is a problem when users are requested to consent to the processing of their data by so many ad-tech vendors?
11) Are you considering leaving the GVL or do you plan to remain a member? Are there any alternatives for you?
12) Can you determine the economic benefit of your GVL membership? If so, can you quantify it (budget/person months)? What would be the costs for your company if the GVL did not exist anymore tomorrow? How important is the GVL related business sector for you? How many jobs at your company depend on this business sector?
13) Do you systematically monitor developments with regard to the GVL (e.g. changes to TCF, changes of GDPR interpretation?) Do you analyze how partners and competitors handle TCF participation?

C. Details and configuration

1) The user data from how many publisher websites do you process?
2) How have you made the decision whether to claim legitimate interest or collect consent for certain purposes? Have publishers influenced your decision?
3) Are you using flexible purposes? If so, why?
4) Do you think the purposes under the TCF are clearly defined?
5) Have you changed your configurations since you joined the GVL?
6) Do you evaluate your configuration? If so, regularly or under specific circumstances?
7) Do you assess the GDPR compliance of CMPs or publishers you cooperate with?
8) Do you monitor how publishers design their consent dialogues? Could / would you like to stop working with those who use a consent dialogue you do not consider compliant?
9) How can users revoke consent? Do some users revoke consent?