Purposes in IAB Europe's TCF: which legal basis and how are they used by advertisers?

Célestin Matte, Cristiana Santos, Nataliia Bielova

Purposes in IAB Europe's TCF: which legal basis and how are they used by advertisers?

Célestin Matte[1*], Cristiana Santos[1,2*], and Nataliia Bielova[1]

[1] Inria, Université Côte d'Azur, France
{celestin.matte, nataliia.bielova}@inria.fr
[2] cristianasantos@protonmail.com

Abstract. The General Data Protection Regulation (GDPR), Data Protection Authorities (DPAs) and the European Data Protection Board (EDPB) discuss purposes for data processing and the legal bases upon which data controllers can rely on: either "consent" or "legitimate interests". We study the purposes defined in IAB Europe's Transparency and Consent Framework (TCF) and their usage by advertisers. We analyze the purposes with regard to the legal requirements for defining them lawfully, and suggest that several of them might not be specific or explicit enough to be compliant. Arguably, a large portion thereof requires consent, even though the TCF allows advertisers to declare them under the legitimate interests basis. Finally, we measure the declaration of purposes by all advertisers registered in the TCF versions 1.1. and 2.0 and show that hundreds of them do not operate under a legal basis that could be considered compliant under the GDPR.

1 Introduction

As a response to the General Data Protection Regulation (GDPR) [25] that came into force in May 2018, the *Internet Advertisement Bureau* (IAB) Europe introduced an open-source framework called the *Transparency and Consent Framework* (TCF) in April 2018 [28]. This framework introduces *Consent Management Providers* (CMPs), new actors collecting consent through the use of so-called "cookie banners", and transmitting this consent to advertisers by implementing an API defined in the framework. The TCF became popular and is actively used on 1,426 out of top 22,000 EU websites [38], and in 680 UK websites [39].

Any advertiser willing to be involved in the TCF and wishing to appear in CMP-based cookie banners must register therein. Thereupon, an advertiser must select one or more of the predefined purposes for data processing. These purposes are presented to website users in cookie banners when collecting their consent. For each purpose, advertisers must choose a legal basis for processing: consent or legitimate interest. The choice of the purposes and their legal basis hold strong legal compliance implications – both on the advertisers, but also on the publishers side, as the latter include third-party resources in their websites.

[*] Co-first authors listed in alphabetical order.

According to Article 8 of the Charter of Fundamental Rights of the European Union [23], personal data must be processed fairly for *specified purposes* and on the basis of a *lawful ground*. Article 5(1)(b) of the GDPR predicates the *"Purpose Limitation"* principle which mandates personal data to be collected for specified, explicit and legitimate purposes. Identifying the appropriate legal basis that corresponds to the purpose of the processing is of essential importance. Thereby, in this work, we make the following contributions:

- We identify the legal requirements for defining purposes based on the GDPR, the 29 Working Party (now EDPB endorsed) and Data Protection Authorities guidance that help us to answer the following questions: *"Does a purpose satisfy the requirements of the purpose specification principle?"* and *"Which is the legal basis for a specific purpose?"* (Section 2);
- We analyse the purposes defined in IAB Europe's TCF versions 1.1 and 2.0, discuss whether such purposes comply with the legal requirements and which purposes should rely on consent (Section 3);
- We collect data about all advertisers registered in both versions of the TCF in order to measure which purposes are selected by advertisers and which legal bases are declared. We show that hundreds of advertisers rely on legitimate interest for purposes that instead should rely on consent (Section 4).

Our work demonstrates the persistence of the advertising industry in non-compliant (with GDPR and ePrivacy Directive) methods for tracking and profiling, bundled in often complex and vague presentation of purposes. The importance of this is further underlined by the extended prior work, guidance, as well as enforcement actions and court decisions in the field.

2 Legal requirements for defining purposes

In this section, we discuss the legal requirements to describe purposes lawfully. Article 5 (1)(b) of GDPR and the 29WP [4] elaborate on the *"Purpose Limitation"* principle. This principle mandates personal data to be collected (1) for specified, explicit and legitimate purposes only and (2) not further processed in a way incompatible with those purposes. In this work, we focus on the first component of this principle named *purpose specification*. This principle focuses on the initial purpose of collection [45] and mandates that each purpose needs to comply with the three criteria of explicitness, specificity, and legitimacy [4]. We analyze each requirement and corresponding violations to better discern its application in the TCF.

Explicitness. The following conditions must be met for a purpose to be explicit:

- Unambiguous. A purpose must be sufficiently unambiguous as to their meaning or intent;
- Exposed. Purposes need to be clearly expressed, revealed or explained, (e.g. not hidden from the data subjects).

– Shared common understanding. The definition of the purposes must be understood in the same way by everybody involved. This ensures that everyone has the same unambiguous understanding of the purposes.

Violation: Hidden or defined with confusion, ambiguity as to their meaning or intent (i.e. purposes that leave doubt, difficulty in understanding).

Specificity. To fulfill the specificity requirement, purposes should be identified precisely, i.e. clearly defined. Their formulation must be detailed enough to determine what kind of processing is and is not included within them [4].
Violation: Vague, too general or overly legalistic purposes. The 29WP [4,10] give examples: "improving users' experience"; "marketing purposes", "IT-security purposes"; "we may use your personal data for research purposes"; etc.

Legitimacy. The purposes defined by the controller should conform to a legal basis for processing. Regarding the use of cookies and similar technologies, the eligible legal basis is informed consent (Article 5(3) of the ePD [19]).

Articles 4(11) and 7 of the GDPR establish the requirements for a valid consent: freely given, specific, informed, unambiguous, readable, accessible and revocable [44]. Whenever consent is exempted for concrete purposes, another legal basis might be applicable. Pursuant to the legitimate interest basis, the 29WP [6] recognizes the *usefulness* as a ground for lawful processing which in the right circumstances and subject to adequate safeguards, may help to prevent misuse of, and over-reliance on other legal grounds. The 29WP postulates this basis should not be used sparingly as a "catch-all" provision to fill in gaps for rare and unexpected situations as "a last resort" where other grounds for legitimate processing are not applicable. Nor should it be seen as a preferred option, or its use unduly extended on the basis of a perception that it is less constraining than the other grounds to legitimize all data processing activities.

In effect, it requires a three-tiered test [35] that allows a processing operation consisting of:

1. Legitimate interest test. Interests must be "lawful", "sufficiently clearly articulated" (transparent) and "represent a real and present interest" [6, p. 25,52];
2. Necessity test. Any data not directly linked to accomplishing the specific purpose are therefore considered "unlawful"; and
3. Balancing test of these interests and the interests of the data subject [20].

The general provision on legitimate interest is open-ended (with a broad and unspecific scope), meaning that it can be relied upon a wide range of purposes – as long as its requirements are satisfied. In this paper, we focus on point (1), since (2) and (3) require a casuistic analysis under a concrete context.
Violation: Purpose(s) without (or incorrect) legal basis for processing.

Discussion. In line with the above clarifications, the purpose specification principle does not allow for open or vaguely defined purposes to govern data-processing practices. These requirements contribute to transparency, legal certainty and foreseeability and aims to protect data subjects by setting limits on

how controllers are able to use collected data. This functional delimitation should prevent the use of personal data in a way (or for further purposes) that they might find unexpected, inappropriate or otherwise objectionable, assuring this way the data minimisation principle (Article 5, (1)(c)). However, the purpose specification principle only provides for abstract procedural norms for purposes definition. Since purpose specification is a *procedural* and not a substantive norm, it allows website owners considerable freedom to define their purposes in flexibly interpretable terms [37]. In this paper, we complement this prescriptive framework by analyzing the purposes deployed in the concrete context of the TCF.

3 IAB Europe's Transparency and Consent Framework

IAB Europe introduced two versions of the TCF: version 1.1 in April 2018, and version 2.0 in August 2019 [29]. Although version 1.1 is actively used by website publishers [38], IAB Europe announced version 1.1 will no longer be supported starting from June 30, 2020 [30]. Version 2.0 will plausibly become even more popular because Google will integrate it as well[3]. In this paper, we consider both versions 1.1 and 2.0.

Upon registration, advertisers must select one or more purposes for data processing from the TCF's pre-defined list of purposes. These purposes are presented to website users in cookie banners when collecting their consent. The list of purposes differ in each version and we will discuss them in detail in Sections 3.1 and 3.2. For each purpose, an advertiser must choose a legal basis for processing: consent or legitimate interest. Advertisers can also declare "features", which correspond to supplementary types of user's data – this usage relies on different purposes of the framework. We discuss potential risks of such features in Section 3.3.

Legal analysis and its limitations. Even though we ground our legal analysis in both authoritative and also expert generated legal sources (GDPR, ePD, 29WP and DPAs guidelines) to discern whether the declared IAB purposes are compliant with the purpose specification principle, as mentioned in Section 2, this analysis is yet limited if not sustained judicially, where a more specific fact finding of each practice could render a final appraisal. We therefore deliberately leave space to legal uncertainty on the assessment made on each purpose and its legal basis. Finally, there are some purposes analysed in v1.1 that are reused in a more granular way in v2.0 and therefore the reasoning given to some of the purposes is still applicable where appropriate, as identified in the text.

3.1 Analysis of purposes of the IAB Europe's TCF v1.1

In this section, we analyze the purposes defined in v1.1 that we show in Table 1.

[3] `https://support.google.com/admob/answer/9461778`, accessed on 2020.02.05

Table 1: Purposes defined in IAB Europe's Transparency and Consent Framework, TCF v1.1 [26, p. 13].

Purpose number	**Purpose name**	**Purpose description**
1	Information storage and access	The storage of information, or access to information that is already stored, on your device such as advertising identifiers, device identifiers, cookies, and similar technologies.
2	Personalisation	The collection and processing of information about your use of this service to subsequently personalise advertising and/or content for you in other contexts, such as on other websites or apps, over time. Typically, the content of the site or app is used to make inferences about your interests, which inform future selection of advertising and/or content.
3	Ad selection, delivery, reporting	The collection of information, and combination with previously collected information, to select and deliver advertisements for you, and to measure the delivery and effectiveness of such advertisements. This includes using previously collected information about your interests to select ads, processing data about what advertisements were shown, how often they were shown, when and where they were shown, and whether you took any action related to the advertisement, including for example clicking an ad or making a purchase. This does not include personalisation, which is the collection and processing of information about your use of this service to subsequently personalise advertising and/or content for you in other contexts, such as websites or apps, over time.
4	Content selection, delivery, reporting	The collection of information, and combination with previously collected information, to select and deliver content for you, and to measure the delivery and effectiveness of such content. This includes using previously collected information about your interests to select content, processing data about what content was shown, how often or how long it was shown, when and where it was shown, and whether the (sic) you took any action related to the content, including for example clicking on content. This does not include personalisation, which is the collection and processing of information about your use of this service to subsequently personalise content and/or advertising for you in other contexts, such as websites or apps, over time.
5	Measurement	The collection of information about your use of the content, and combination with previously collected information, used to measure, understand, and report on your usage of the service. This does not include personalisation, the collection of information about your use of this service to subsequently personalise content and/or advertising for you in other contexts, i.e. on other service, such as websites or apps, over time.

Purpose 1 *"Information storage and access"* is not specific, but could require consent. This purpose does not provide enough information. In fact, it only mentions the technical tools that collect data (such as advertising identifiers or cookies) without explaining at all for which purpose the data will be used. According to the "*specificity*" requirement denoted in Section 2, the GDPR requires a purpose to be sufficiently and clearly defined, i.e. it must be detailed enough to determine what kind of processing is and is not included. In effect, this purpose conveys the impression to be unspecified: it is too general and possibly violates the specificity requirement.

Nevertheless, we can argue that this purpose requires consent as a legal basis due to Article 5(3) of the ePD. However, due to its lack of specificity, it's still unclear whether the final usage of the stored or accessed data falls under any of the exceptions of the ePD. Moreover, this reasoning may differ within EU member States due to the implementation of this ePD in national law.

Purpose 2 *"Personalisation"* is not explicit, nor specific, and so we cannot derive its legal basis. Although its name is clear, its description is ambiguous and vaguely-worded: this purpose bundles a host of separate processing purposes under a single name – it implies both advertising *and/or* content personalization. We hereby decompose such purpose. Regarding personalization (also called customization or preferences), the 29WP [5] cautioned that cookies storing user's preferences of a service are explicitly enabled by the user (e.g. clicking a button or ticking a box to keep a language, display format, fonts, etc.). Only session (or short-term) cookies storing such information can be exempted. Regarding advertising, we cautiously conjecture that *"personalization for advertising"* conflates two different purposes. Taking the positioning (advocated by both 29WP and DPAs) that advertising requires consent, we further account the requirement for consent to be *specific* (Article 4(11) of the GDPR). It mandates granularity of the consent request in order to avoid a catch-all purpose acceptance, so that the user is able to give consent for an independent and specific purpose [7]. Moreover, Recital 43 clarifies the need for a separate consent for different processing operations. Recital 32 states consent should be given per purpose (or set of purposes). The 29WP [22] instructs further that *"a controller that seeks consent for various different purposes should provide a separate opt-in for each purpose, to allow users to give specific consent for specific purposes"*. Finally, Planet49 Judgment of the Court of Justice of the EU [18] determined that consent should be granular for each purpose. In the light of the above, we argue that this multi-purpose might be non-specific.

This multipurpose seems ambiguous, leaving room for doubt and confusion as to its meaning and intent and may possibly violate the *explicitness* requirement. As such, it is complex to determine which is the applicable legal basis.

Purpose 3 *"Ad selection, delivery, reporting"* is not explicit, not specific, but should require consent. We argue that this purpose requires

consent because it describes collection of data with the purpose of selection and delivery of advertisement. Pursuant to this purpose, the 29WP stated that third-party advertising cookies are not exempted from consent [5][4]. The ICO (UK DPA) also contended that data collection for advertising is not "strictly necessary" from the point of view of a website user, and hence this purpose cannot rely on legitimate interest, requiring consent [36]. The same reasoning holds for the German [12] and Dutch DPAs [1].

Furthermore, the description afforded in this purpose induces to consider that we might be across multipurpose advertising with adjacent profiling that is not disclosed explicitly. While the documentation excludes "personalization", its description seems instead to accommodate profiling. It is perceivable that considering the user's interests and his reactions towards ads and the combination of the user's includes profiling. To ascertain this argument, we call forth the definition of profiling in Article 4 (4) (and Recital 30 of the GDPR): "*any form of automated processing of personal data consisting of using those data to evaluate certain personal aspects (...), in particular to analyse or predict aspects concerning that natural person's (...) personal preferences, interests, reliability, behaviour, location or movement.*" We deduct the personal data to be collected and combined with a previous user profile is meant to analyze or predict (i.e. some form of assessment) aspects concerning the user's interests and likely behavior towards ads. In the light of the above, this purpose seems not explicit and non-specific. Morevoer, users would need to be informed of the purpose of profiling (and the legal basis of consent), pursuant to Article 13 (1)(c), and (2)(f).

Purpose 4 *"Content selection, delivery, reporting"* might be exempted from consent (if session-only). This purpose's name suggests it might be exempted of consent because it only mentions personalization of content (and not of ads as in purpose 3) based on the previously collected information about user interests, clicks, etc. According to the 29WP [5], customization cookies storing user's preferences regarding a service that is explicitly enabled by the user are exempted of consent. However, we note that only session (or short-term) cookies storing such information are exempted. These purposes can instead rely on other legal bases (e.g. legitimate interests) if these pass both the necessity and the balancing tests.

Purpose 5 *"Measurement"* requires consent. It covers the collection of information and combination with previously collected information. We are aware that the entities who will collect information are advertisers– hence third-party content providers for a website publisher. The 29WP regarded that cookies used for "analytics" are not "strictly-necessary"to provide a functionality explicitly requested by the user, because the user can access all the functionalities provided by the website when such cookies are disabled, especially when they are used by third-party services [5]. Moreover, according to the CNIL [15], analytics cookies

[4] In our work, the denomination of "cookies" covers all tracking technologies.

require consent when collected data is combined or merged with other types of data. Both the ICO [36], and the German DPA [12] sustain the same position that third-party analytics cookies are not strictly necessary and require consent.

3.2 Analysis of purposes the IAB Europe's TCF v2.0

Version 2.0 introduces 12 purposes (as opposed to 5 purposes in v1.1) and a new category of *"special purposes"* that do not allow users to opt out therefrom. In v2.0, advertisers declare which purposes they use under which legal basis. For each purpose, advertisers can choose to be "flexible", i.e. to leave the choice of the legal basis to publishers who embed TCF banners in their websites. Table 2 lists all purposes and special purposes from v2.0. TCF v2.0 also proposes "special features" that require user opt-in (we analyse features separately later in Section 3.3).

Purpose 1 *"Store and/or access information on a device"* is not specific, but could require consent. We reproduce the same observations as for purpose 1 in TCF v1.1. Its description seems to be contradictory: it states this purpose requires consent but it confirms that "*Purpose 1 is not a data processing purpose, is technically treated the same way for signalling purposes*". Also, it mentions that "*any personal data stored and/or accessed via Purpose 1 still requires another Purpose to actually be processed*"; this statement renders it as a condition to other listed purposes. This suggests to be an unspecified purpose: we adduce it seems too general and it might violate the specificity requirement.

Interestingly, v2.0 introduces a special mechanism to prevent disclosing this purpose 1 depending on the publisher's country: when the publisher estimates that its country's jurisdiction does not require consent for this purpose, it will not be shown in cookie banners. As a result, purpose 1 is likely to require consent due to the national implementation of the ePD.

Purpose 2 "*Select basic ads*" is specific, explicit and requires consent. It relates to advertisement which requires consent (like purpose 3 of v1.1.)

Purpose 3 "*Create a personalized ads profile*" and 4 "*Select a personalized ads*" may require explicit consent. They may trigger significant effects to end users under the set of assumptions interpreted below, which also apply to Purposes 2 and 3 of version 1.1. The 29WP [3] identified occasions where targeted behavioural advertising (as it is the case conducted by the TCF), could be considered as having *"significant effects"* on users. Where significant and solely automated decisions are made about an individual, *explicit consent* is required (as per Article 22 (1) and (2) c)). This holds specially where vulnerable individuals are targeted with ads of services that may cause them detriment (such as gambling or certain financial products). The 29WP [3] further illustrates that in many typical cases, targeted ads based on profiling might have significant effects on users depending upon the particular characteristics of the case, suchlike:

Table 2: Purposes defined in IAB Europe's TCF v2.0 [27, p .25]

(a) Purposes

Purpose number	**Purpose name**	**User-friendly text**
1	Store and/or access information on a device	Cookies, device identifiers, or other information can be stored or accessed on your device for the purposes presented to you.
2	Select basic ads	Ads can be shown to you based on the content you're viewing, the app you're using, your approximate location, or your device type.
3	Create a personalised ads profile	A profile can be built about you and your interests to show you personalised ads that are relevant to you.
4	Select personalised ads	Personalised ads can be shown to you based on a profile about you.
5	Create a personalised content profile	A profile can be built about you and your interests to show you personalised content that is relevant to you.
6	Select personalised content	Personalised content can be shown to you based on a profile about you.
7	Measure ad performance	The performance and effectiveness of ads that you see or interact with can be measured.
8	Measure content performance	The performance and effectiveness of content that you see or interact with can be measured.
9	Apply market research to generate audience insights	Market research can be used to learn more about the audiences who visit sites/apps and view ads.
10	Develop and improve products	Your data can be used to improve existing systems and software, and to develop new products.

(b) Special purposes

1	Ensure security, prevent fraud, and debug	Your data can be used to monitor for and prevent fraudulent activity, and ensure systems and processes work properly and securely.
2	Technically deliver ads or content	Your device can receive and send information that allows you to see and interact with ads and content.

– the intrusiveness of the profiling process, including the tracking of individuals across different websites, devices and services;
– the expectations and wishes of the individuals concerned;
– the way the advert is delivered; or
– using knowledge of the vulnerabilities of the data subjects targeted" [3].

This cognition of the 29WP holds significant interest for profiling. It advises the following relevant elements to account when profiling: the level of detail of the profile (broad, or segmented, granular); its comprehensiveness (does it describe merely one aspect of the data subject, or a more comprehensive picture); the impact of the profiling (effects on the data subject); the safeguards aimed at ensuring fairness, non-discrimination and accuracy in the profiling process.

We argue that the amount and variety of personal information collected under the aegis of these two purposes (as described in the specification policies) across websites, devices and services, might have a significant effect on individuals (even larger when conjugating with features and special features).

The TCF specification allows the use of legitimate interest for personalized advertising. Against this reasoning, the 29WP [22] suggested that "*it would be difficult for controllers to justify using legitimate interests as a lawful basis for intrusive processing and tracking practices for marketing or advertising purposes, for example those that involve tracking individuals across multiple websites, locations, devices, services or data-brokering*".

Purposes 5 *"Create a personalized content profile"* and 6 *"Select personalized content"* might be exempted from consent. With reference to them (the "content" in purpose 6 is shown to the user based on a profile), the 29WP [3, p .14] acknowledged profiling (that is not solely done by automated means resulting in legal or significant effects) can be legitimized under a legitimate interest.

From both versions of the TCF, we presume that only Purposes 5 and 6 from v2.0 and Purpose 4 from v1.1 are exempted of consent and thus, are hypothetically capable of being legitimized under a necessity of a legitimate interest of the controller or a third-party.

However, according to Recital 47 of the GPDR, when using legitimate interest as a legal basis for processing, the controller (in the balance test) has to consider the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate expectations could exist, for example, where there is a relevant and appropriate relationship between the data subject and the controller, e.g. when the data subject is their client or in their service. This means that the data subject needs to have a "reasonable expectation" that their own personal data is being used by a company for a specific purpose. This expectation must exist at the time and in the context of the collection of her personal data. Meanwhile, the collection of data from unknown sources, by third-parties that users have never heard of and do not have a direct relationship with – to profile them and share these "insights" with other advertisers – is not plausibly within the individuals' reasonable expectations. Hence, we suppose that processing personal data of users that have no relationship with third-party advertisers,

which is the case in the TCF, will, in practice, make that balance weight towards the interest and rights of users. As posited by the Norwegian Consumer Council [24], "*although consumers may know that many "free" digital services are funded by advertising, this does not mean that most people will have a "reasonable expectation" of the amount of sharing and processing going on behind the scenes (...) Companies are virtually unknown to most consumers, so one can hardly consider this a relationship at all."* Thus, the potentially unique purpose (from the specification of the TCF) that would rely on legitimate interest could, in practice, fail the requirements of such a legal basis. Lastly, Purpose 6 named *"Select personalized content"* would require consent in case of non session-only cookies.

Purposes 7 *"Measure ad performance"*, 8 *"Measure content performance"* and 9 *"Apply market research to generate audience insights"* require consent. We argue that they fall into the broader category of measurement purposes. Hence, we reproduce the same reasoning of Purpose 5 in v1.1. Based on the argument of the 29WP [6, p .47], consent is always required for third-party analytics and tracking-based digital market research: *"opt-in consent would almost always be required [...] for tracking and profiling for purposes of direct marketing, behavioural advertisement, location-based advertising or tracking-based digital market research"*. We also claim that this latter purpose *"Apply market research to generate audience insights"* is not specific and is defined in a broad way and with ambiguity as to its intent.

Purpose 10 *"Develop and improve products"* is not specific, and so we cannot derive its legal basis. It seems vague and might be qualified unspecified, since it is not detailed enough to determine its kind of processing (to allow compliance with the law to be assessed). In fact, this purpose is a typical example of a violation of the specificity requirements, as indicated in [4,9]. Accordingly, deriving its legal basis is intricate. It follows therefrom that this purpose would facilitate non-specific, hypothetical processing of personal data under a broad designation of undefined purpose of product improvement or new product development. As an example, a recent EDPB guidance [21] only proposes legitimate interest or consent (depending on a concrete case and the legal requirements demanded) for the purpose of *"Service improvement"* under a motivation that online services often collect detailed information on how users engage with their service through a collection of organizational metrics that need to be justified contextually for a concrete service, also grounding the way to improve it.

Special Purpose 1 *"Ensure security, prevent fraud, and debug"* is not specific, but could be exempted from consent. It seems to cover a broad range of purposes which could be made autonomous in the TCF. These purposes could supposedly rely on legitimate interest since these have been the most consensual and prevalent interests sustained across industries [13], by the EDPB [21], other DPAs guidance [6,1,12] and proposed in GDPR Recitals. Recitals 47 and

49 mention fraud prevention, network and information security could "constitute" legitimate interest. These purposes would still need to pass the necessity and balancing tests for processing to be lawful under legitimate interest.

As a remark, the specification policies do not permit to exert the right to object to processing under legitimate interest via the TCF. Such right exists in the GDPR, unless the controller can demonstrate "compelling legitimate grounds" (Article 21(1)) that override the interests or rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims [3].

Special Purpose 2 *"Technically deliver ads or content"* is not specific and could require consent. It bundles separate data processing purposes under a single name: it implies both advertising *or* content delivery. We reproduce the same reasoning of Purpose 2 in version 1.1.

We summarize our analysis of all purposes of IAB Europe TCF v1.1 and v2.0 in Table 3.

3.3 Features and special features defined in versions 1.1 and 2.0

In this section, we briefly comment on the use of features and special features defined in the framework on both versions. We exclude a crossed analysis of the features with each purpose as it requires extensive work and is out of scope of this paper. Table 4 presents features for TCF v1.1 and v2.0.

Feature 1 of v1.1 "Matching Data to Offline Sources"
i) Definition of "matching" is problematic. This feature allows to combine data from offline sources that were collected in other contexts, without explaining what data and which context are at stake. Additionally, matching implies offline but *also* online data (*"data from offline data sources can be combined with your online activity in support of one or more purposes")*. Finally, the purpose description in the specification does not suffice to render probable *consequences* of such a feature.
ii) Profiling. Disparate and seemingly innocuous data from online and offline sources can ultimately be combined to create a meaningful comprehensive profile of a person. On this feature, Johnny Ryan [43] formulated that *"these notices fail to disclose that hundreds, and perhaps thousands, of companies will be sent your personal data. Nor does it say that some of these companies will combine these with a profile they already have built about you. Nor are you told that this profile includes things like your income bracket, age and gender, habits, social media influence, ethnicity, sexual orientation, religion, political leaning, etc. Nor do you know whether or not some of these companies will sell their data about you to other companies, perhaps for online marketing, credit scoring, insurance companies, background checking services, and law enforcement".*

Feature 1 of v2.0 "Match and combine offline data sources" and Feature 2 of v1.1 and of v2.0 "Linking devices"

Table 3: Purposes defined in IAB Europe's TCF v1.1 and v2.0. The "Allowable Lawful Bases" column indicates the official documentation guidelines of IAB regarding the use of legal basis in v2.0 [27, p .25]. The "Requires Consent" column sums up our analysis. We indicate the default legal basis, and add parentheses if exceptions occur.

(a) Purposes (TCF v1.1)

Purpose number	**Purpose name**	**Allowable Lawful Bases**	**Requires Consent**
1	Information storage and access	-	(✓)
2	Personalisation	-	?
3	Ad selection, delivery, reporting	-	✓
4	Content selection, delivery, reporting	-	(✓)
5	Measurement	-	✓

(b) Purposes (TCF v2.0)

1	Store and/or access information on a device	Consent	(✓)
2	Select basic ads	Consent, LI	✓
3	Create a personalised ads profile	Consent, LI	✓
4	Select personalised ads	Consent, LI	✓
5	Create a personalised content profile	Consent, LI	(✓)
6	Select personalised content	Consent, LI	(✓)
7	Measure ad performance	Consent, LI	✓
8	Measure content performance	Consent, LI	✓
9	Apply market research to generate audience insights	Consent, LI	✓
10	Develop and improve products	Consent, LI	?

(c) Special purposes (TCF v2.0)

1	Ensure security, prevent fraud, and debug	LI	(✗)
2	Technically deliver ads or content	LI	?

Table 4: Features defined in IAB Europe's TCF v1.1 and v2.0.

(a) Features in TCF v1.1 [26, p. 13]

Feature number	**Feature name**	**User-friendly text**
1	Matching Data to Offline Sources	Combining data from offline sources that were initially collected in other contexts with data collected online in support of one or more purposes.
2	Linking Devices	Processing of a user's data to connect such user across multiple devices.
3	Precise Geographic Location Data	Processing of a user's precise geographic location data in support of a purpose for which that certain third party has consent.

(b) Features in TCF v2.0 [27, p .25]

1	Match and combine offline data sources	Data from offline data sources can be combined with your online activity in support of one or more purposes.
2	Link different devices	Different devices can be determined as belonging to you or your household in support of one or more of purposes.
3	Receive and use automatically-sent device characteristics for identification	Your device might be distinguished from other devices based on information it automatically sends, such as IP address or browser type.

(c) Special features in TCF v2.0 [27, p .25]

1	Use precise geolocation data	Your precise geolocation data can be used in support of one or more purposes. This means your location can be accurate to within several meters.
2	Actively scan device characteristics for identification	Your device can be identified based on a scan of your device's unique combination of characteristics.

i) Personal data. Both features configure technical means to process personal data (considering its broad definition predicated in Article 4(1) and Recital 26 of the GDPR [2]), as matching data to offline sources and linking devices are means that could reasonably enable identification of individuals.
ii) Profiling. An advertiser able to track and link people's interests and/or behavior across different devices (e.g. laptops, computers, phone, smart TV, etc.) is able to get a fine-grained view of an individual's activities throughout a day. To this scope, whenever companies process data using these technical means, is is plausible they are processing personal data and they need to be GDPR compliant, e.g. to the lawfulness and purpose limitation principles.

Feature 3 of v1.1 and Special Feature 1 of v2.0 "Precise Geographic Location Data"
i) Requires consent. Gaining access to information stored in the device of a user requires consent (under Article 5(3) of the ePD).
ii) Personal data. The GDPR also applies whenever the provider collects location data from the device and if it can be used to identify a person, which distinctively occurs with "precise geolocation data". The broad definition of "personal data" specifically includes location data as one of the elements that can identify a person. The 29WP [8] sets out that providers of geolocation based services gain *"an intimate overview of habits and patterns of the owner of such a device and build extensive profiles.*"
iii) Profiling. Using location data may involve "profiling" within the meaning of Article 4(4) and Recital 72 which specifically includes analyzing location data.
iv) Special categories of personal data. In particular contexts, location data could be linked to special categories of personal data, requiring explicit consent (Article 9 of the GDPR), e.g. location data may reveal visits to hospitals or places of worship or presence at political demonstrations.

Feature 3 of v2.0 "Receive and use automatically-sent device characteristics for identification" and Special Feature 2 of v2.0 "Actively scan device characteristics for identification" Consent is required. Due to browsers behavior, cookies are automatically sent to websites. These cookies can store user identifiers based on the device characteristics. Such features in principle require consent (under Article 5(3) of the ePD). This applies irrespective of whether or not the location data is personal data.

4 Evaluation of the Usage of Purposes of IAB Europe's Transparency and Consent Framework by Advertisers

In this section, we analyze the purposes declared by all the advertisers registered in IAB Europe's Transparency and Consent Framework. Our goal is to bring transparency to the use of purposes and features by advertisers, to raise concerns derived from the legal analysis in Section 3 and the practical usage measured herein. To do so, we take advantage of the fact that all data regarding different

advertisers of the TCF is made public, and notably the Global Vendor List (GVL, the list of all registered advertisers). This list includes data about advertisers, what purposes they use and under which legal basis they operate. In Appendix A we show the evolution of the number of advertisers registered in TCF.

In TCF v1.1, only advertisers can choose which legal basis to use for each purpose. In TCF v2.0 however, advertisers can decide to declare some purposes as "flexible" – in that case publishers can impose "restrictions" and require a specific legal basis for such purposes [33][5].

4.1 Purposes and legal basis of processing declared by advertisers

In this section, we measure the legal basis for purposes declared by advertisers in the Global Vendor List: in v1.1 (version 183) [31] and v2.0 (version 20) [32].

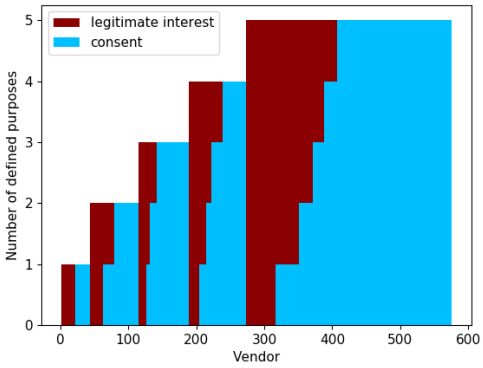


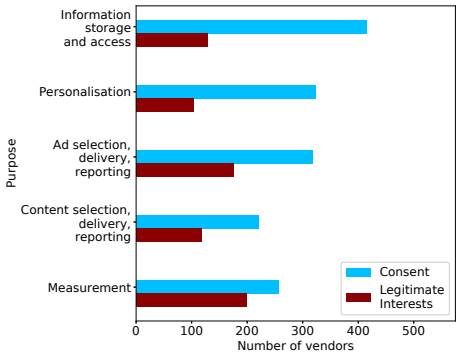
Fig. 1: Number of defined purposes and their legal basis per advertiser in the Global Vendor List for v1.1 (version 183) [31], January 2020.

Figure 1 shows the legal basis of processing for all advertisers: 46% (267) of them operate on legitimate interest for at least one purpose, and 19% (111) of advertisers rely on legitimate interest for all the purposes they declare (i.e., they do not operate on the basis of consent for any purpose). Overall, 54% (308 advertisers) operate on consent only and 27% (156) base their processing on both consent and legitimate interest. We present the list of all 267 third-party advertisers that rely on legitimate interests for at least one purpose in attachment [11].

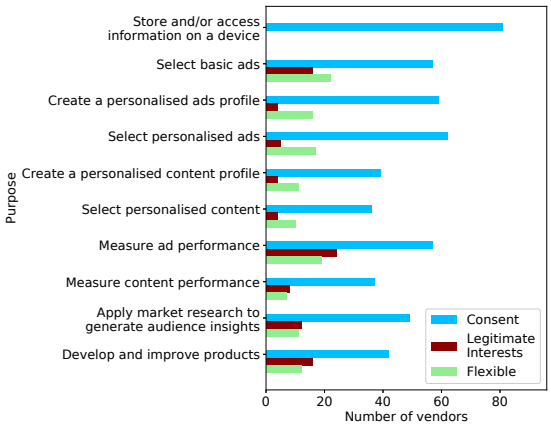
Next, we measure the purposes self-declared by advertisers in the TCF's GVL in Figure 2. Figure 2a details the results presented above for each individual purpose in v1.1 [31]. We observe a difference in the use of the different legal

[5] We do not study the legal bases of purposes declared by publishers in this paper.

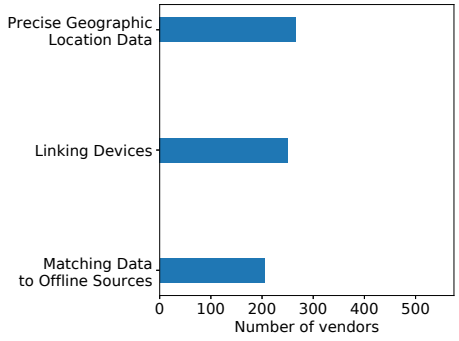
Fig. 2: Purposes, features and legal basis of processing declared by the registered advertisers in IAB Europe's Transparency and Consent Framework v1.1 and v2.0, January 2020.



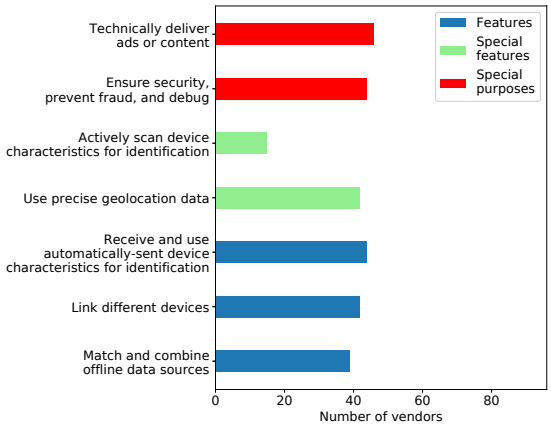
(a) Purposes, TCF v1.1 (version 183) [31]



(b) Purposes, TCF v2.0 (version 20) [32]



(c) Features, TCF v1.1 (version 183) [31]



(d) Features, special features and special purposes, TCF v2.0 (version 20) [32]

bases among purposes: while 72% of advertisers rely on consent for purpose 1 ("Information storage and access"), 38% do so for purpose 4 ("Content selection, delivery, reporting"). Interestingly, 22% of advertisers rely on legitimate interest for purpose 1 and 35% do so for purpose 5 ("Measurement"). We identified in Section 3 that purposes 3 and 5 of TCF v1.1 ("Ad selection, delivery, reporting" and "Measurement") require consent. However, we detect a particularly worrisome number of advertisers: 175 and 199 advertisers respectively rely on legitimate interests for purposes 3 and 5.

Figure 2b renders an analysis of purposes for the Global Vendor List of v2.0 [32]. The number of advertisers registered in this version is smaller, but we still see that a significant portion of advertisers use legitimate interest for purposes that require consent. For example, 17% advertisers rely on legitimate interest for purpose 2 ("Select basic ads"), and 25% advertisers do it for purpose 7 ("Measure ad performance"), while our legal analysis in Section 3 demonstrated that purposes 2 and 7 require consent. It is also notable that 32% of advertisers use "flexible purposes" for at least one purpose thus allowing publishers to change the legal basis for such purposes [33].

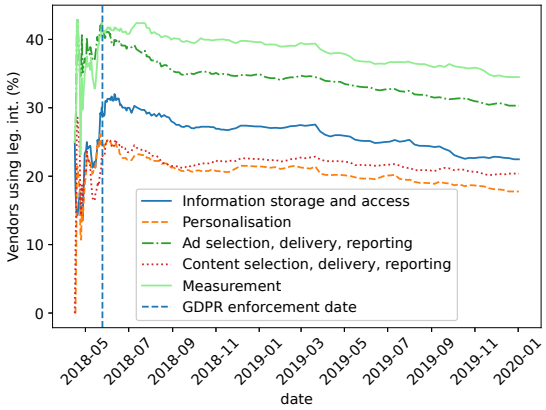


Fig. 3: Evolution of the proportion of advertisers of IAB Europe's TCF v1.1 that rely on legitimate interest as a lawful basis for data processing, between April 2018 and January 2020.

As DPAs criticized the use of legitimate interest as a lawful basis for online advertising [34], it is interesting to see the evolution of this use over time. In Figure 3, we show that the proportion of advertisers registered in the TCF that rely on legitimate interest for each purpose slowly decreases over time.

4.2 Additional "features" of processing

Figure 2c shows the prevalence of features used by registered advertisers in TCF v1.1. Our analysis shows that 66% (377) of advertisers declare at least one of

these features in v1.1 [31]. We present a list of 118 advertisers that use all three features of v1.1 in a public repository [11]. Such advertisers might require a deeper inspection by the DPAs, since consent is not requested for using these features in the TCF. We also present the list of all 377 advertisers that use at least one feature in v1.1 [11].

Figure 2d shows prevalence of features, special features and special purposes used by registered advertisers in TCF v2.0: 45% of advertisers use at least one special feature, and 52% of advertisers use at least one special purpose.

5 Related Work

Matte et al. found several plausible violations of both the GDPR and the ePD in the implementations of cookie banners by actors using this framework [38]. Nouwens et al. [39] studied dark patterns in 5 popular CMPs of the TCF and estimated that only 11.8% of banners met minimum legal requirements. Other works on cookie banners briefly mentioned the framework [17,44].

On the legal side in 2018 several complaints were lodged in Europe by NGOs against the Real-Time Bidding (RTB) scheme supported by IAB. These complaints alleged that IAB is in breach of the GDPR, as broadcasting of personal data takes place every time an RTB-driven ad is shown [42]. The French and UK DPAs both criticized the framework. In 2018, the CNIL pronounced a relevant decision determining that Vectaury, acting as a TCF CMP, failed to demonstrate that valid consent had been obtained for the processing of data used for targeted advertising, and had not complied with the principle of transparency with respect to the purposes of processing [14,41]. The ICO studied the TCF, most notably criticizing the use of legitimate interest as a lawful basis for data processing for online advertising [34]. The Panoptykon Foundation filed complaints against Google and IAB Europe [40] to the Polish DPA related to the online behavioural advertising (OBA) ecosystem. These complaints focus on the role of IAB as an organization that sets standards for other actors involved in the OBA market, insisting they should be treated as data controllers responsible for GDPR infringements. The network of data protection expertise lodged a complaint to the German DPA about data processing in the context of personalized online advertising, adducing that providers who are members of IAB Europe incur into possible violations of the GDPR. [16]

6 Conclusions

In this paper, we assessed the scope of the principle of purpose specification in the predefined purposes of IAB Europe's TCF v1.1 and v2.0. Our analysis shows that some purposes, e.g. "Personalisation" are not specific and explicit enough to be used as legally-compliant ones and might not be exempted of consent. Nonetheless, we measured that 175 advertisers out of 575 registered in the TCF v1.1 declare the legitimate interest basis for this purpose.

All the actors using such frameworks need to be aware of the legal implications of the usage of predefined purposes and choices they make regarding the legal basis of processing personal data.

We hope these findings may be useful for policy-makers to design better guidelines regarding (i) the specification of purposes in the TCF and similar frameworks, and (ii) the legal basis to be used per purpose.

Acknowledgements: We thank Johnny Ryan for his comments on the analysis of the purposes. We thank anonymous reviewers of APF 2020 for their useful feedback. This work has been partially supported by ANR JCJC project PrivaWeb (ANR-18-CE39-0008), ANSWER project PIA FSN2 No. P159564-2661789/DOS0060094 between Inria and Qwant, and by the Inria DATA4US Exploratory Action project.

References

1. AP (Dutch DPA), "Standard explanation of the basis of the legitimate interest."
2. Article 29 Working Party, "EDPB opinion 4/2007 on the concept of personal data (WP136), adopted on 20.06.2007."
3. ——, "Guidelines on automated individual decision-making and profiling for the purposes of regulation 2016/679 (WP251 rev.01)."
4. ——, "Opinion 03/2013 on purpose limitation (WP203)."
5. ——, "Opinion 04/2012 on cookie consent exemption (WP 194), adopted on 7 june 2012."
6. ——, "Opinion 06/2014 on the notion of legitimate interests of the data controller under article 7 of directive 95/46/EC (WP217)."
7. ——, "Working document 02/2013 providing guidance on obtaining consent for cookies."
8. ——, "Opinion 13/2011 on Geolocation services on smart mobile devices (WP 185),Adopted on 16 May 2011," 2011.
9. ——, "Guidelines on Consent under Regulation 2016/679 (wp259rev.01)," 2016.
10. ——, " Guidelines on transparency under Regulation 2016/679 (WP260 rev.01), Adopted on 11 April 2018," 2018.
11. "Attachments to the paper (dropbox repository)," https://www.dropbox.com/sh/0g1qlsaatc8yplz/AACAaFLJNrwRH3eWRmGm_zqsa?dl=0.
12. BfDI (German DPA), "Guidance from german authorities for telemedia providers."
13. Centre for Information Policy Leadership, "CIPL examples of legitimate interest grounds for processing of personal data."
14. CNIL, "Décision n MED 2018-042 du 30 octobre 2018 mettant en demeure la société VECTAURY," 2018.
15. ——, "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.
16. "Decision of the Conference of Independent Data Protection Supervisors of the Federal and state governments - 07.11.20191," Datenshutzkonferenz.
17. M. Degeling, C. Utz, C. Lentzsch, H. Hosseini, F. Schaub, and T. Holz, "We value your privacy... now take some cookies: Measuring the GDPR's impact on web privacy," *Network and Distributed System Security Symposium (NDSS)*, 2019.

18. "Judgement of the court of justice of the EU, Case c-673/17."
19. "Directive 2009/136/ec of the european parliament and of the council of 25 november 2009 amending directive 2002/22/ec on universal service and users' rights relating to electronic communications networks and services."
20. "Judgment of the court (second chamber) of 4 may 2017," Case C-13/16.
21. European Data Protection Board (EDPB), "Guidelines 2/2019 on the processing of personal data under article 6(1)(b) gdpr in the context of the provision of online services to data subjects."
22. ——, "Guidelines on consent under regulation 2016/679" (wp259 rev.01), adopted on 10 april 2018."
23. European Parliament, the Council and the Commission, "Charter of Fundamental Rights of the European Union, Official Journal of the European Communities, 18 December 2000 (2000/C 364/01)."
24. Forbrukerrådet, "Out of control - how consumers are exploited by the online advertising industry," 2020.
25. "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," 2016.
26. IAB Europe, "IAB europe transparency & consent framework policies," https://iabeurope.eu/wp-content/uploads/2019/08/IABEurope_TransparencyConsentFramework_v1-1_policy_FINAL.pdf, accessed on 2019.11.20.
27. ——, "IAB europe transparency & consent framework policies," https://iabeurope.eu/wp-content/uploads/2019/08/TransparencyConsentFramework_PoliciesVersion_TCFv2-0_2019-08-21.3_FINAL-1-1.pdf, accessed on 2020.01.21.
28. ——, "Transparency and consent framework," https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework, 2018.
29. ——, "Transparency and consent framework (v2)," https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/tree/master/TCFv2, 08 2019.
30. ——, "Dates you need to know for the TCF V2.0 switchover," https://iabeurope.eu/tcf-2/dates-you-need-to-know-for-the-tcf-v2-0-switchover/, 2020.
31. IAB Europe and IAB Tech Lab, "Global vendor list (GVL, v1.1, version 183)," https://vendorlist.consensu.org/v-183/vendorlist.json, 01 2020.
32. ——, "Global vendor list (GVL, v2.0, version 20)," https://vendorlist.consensu.org/v2/archives/vendor-list-v20.json, 01 2020.
33. IAB Tech Lab and IAB Europe, "Transparency and consent string with global vendor & CMP list formats," https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/TCFv2/IAB%20Tech%20Lab%20-%20Consent%20string%20and%20vendor%20list%20formats%20v2.md#the-core-string, 12 2019.
34. ICO, "ICO report into adtech and real time bidding, adopted in 20 june 2019."
35. ——, "Lawful basis for processing legitimate interests," 2018.
36. ——, "Guidance on the use of cookies and similar technologies," 07 2019.
37. B.-J. Koops, "The (in) flexibility of techno-regulation and the case of purpose-binding," *Legisprudence*, vol. 5, no. 2, pp. 171–194, 2011.
38. C. Matte, N. Bielova, and C. Santos, "Do cookie banners respect my choice? measuring legal compliance of banners from IAB Europe's transparency and consent framework," in *IEEE Symposium on Security and Privacy (IEEE S&P'20))*, 2020.

39. 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 *Conference on Human Factors in Computing Systems (CHI'20)*, 2020.
40. Panoptykon Foundation, "Panoptykon files complaints against Google and IAB Europe," https://en.panoptykon.org/complaints-Google-IAB, 2019.
41. J. Ryan, "French regulator shows deep flaws in IAB's consent framework and RTB," https://brave.com/cnil-consent-rtb/, accessed on 2019.03.28, 2018.
42. ——, "Regulatory complaint concerning massive, web-wide data breach by google and other "ad tech" companies under europe's gdpr," https://brave.com/adtech-data-breach-complaint/, accessed on 2020.02.05, 2018.
43. ——, "Brave answers us senators questions on privacy and antitrust," https://brave.com/senate-qrfs-june2019/, accessed on 2020.02.05, 2019.
44. C. Santos, N. Bielova, and C. Matte, "Are cookie banners indeed compliant with the law? deciphering eu legal requirements on consent and technical means to verify compliance of cookie banners," *ArXiv*, vol. abs/1912.07144, 2019.
45. M. von Grafenstein, *The Principle of Purpose Limitation in Data Protection Laws: The Risk-based Approach, Principles, and Private Standards as Elements for Regulating Innovation*, 1st ed. Nomos Verlagsgesellschaft mbH, 2018.

A Evolution of the number of advertisers

We leverage the fact that all versions of the Global Vendor List of the TCF are public and dated – we can therefore display the evolution of the number of registered advertisers (vendors) in Figure 4. We observe a fast increase in the first three months following the release of IAB Europe's TCF in April 2018 (one month before GDPR came in force in the EU), followed by a slow increase until March 2020. Version 2.0 was announced in August 2019 and is supposed to operate alongside version 1.1 until the end of March 2020. The increase in registered advertisers is far from being as fast as for the release of version 1.1, and as of January 16$^{\text{th}}$ 2020, only 92 advertisers are registered, compared to 574 for version 1.1. This is surprising if we consider that advertisers do not have to pay the registration fee a second time to register for version 2.0.

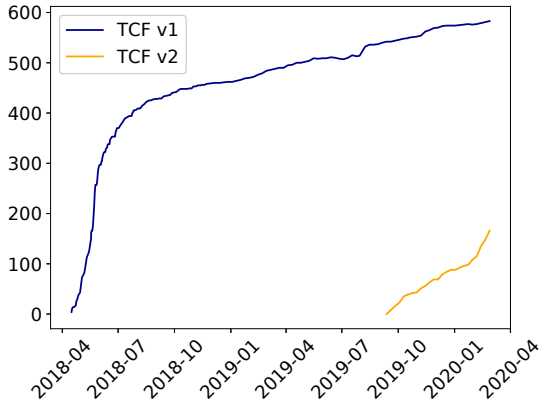


Fig. 4: Evolution of the number of registered advertisers in the IAB Europe's Global Vendor List between May 2018 and March 2020.

B Attachments

We report several lists of advertisers collected in this work in a publicly available repository [11]:

- the list of 377 advertisers declaring that they use features,
- the list of 118 advertisers declaring that they use all features,
- the list of 267 advertisers declaring that they use legitimate interests,
- the list of 111 advertisers using only legitimate interests,
- the list of 308 advertisers using consent only.

This analysis has been done for the Global Vendor List for TCF v1.1 (version 183) [31].

C Purposes, features, special purposes and special features of TCF v2

We present definitions of the following notions as quotations from the TCF v2's policy [27]:

- "Purpose means one of the defined purposes for processing of data, including users' personal data, by participants in the Framework that are defined in the Policies or the Specifications for which Vendors declare a Legal Basis in the GVL and for which the user is given choice, i.e. to consent or to object depending on the Legal Basis for the processing, by a CMP"
- "Special Purpose means one of the defined purposes for processing of data, including users' personal data, by participants in the Framework that are defined in the Policies or the Specifications for which Vendors declare a Legal Basis in the GVL and for which the user is not given choice by a CMP."
- "Feature means one of the features of processing personal data used by participants in the Framework that are defined in the Policies or the Specifications used in pursuit of one or several Purposes for which the user is not given choice separately to the choice afforded regarding the Purposes for which they are used"
- "Special Feature means one of the features of processing personal data used by participants in the Framework that are defined in the Policies or the Specifications used in pursuit of one or several Purposes for which the user is given the choice to opt-in separately from the choice afforded regarding the Purposes which they support."