

# The Impact of the Transparency Consent Framework on Current Programmatic Advertising Practices

Hubert Pawlata<sup>1</sup> and Gültekin Cakir<sup>2</sup><sup>a</sup>

<sup>1</sup>OMD Düsseldorf, Düsseldorf, Germany

<sup>2</sup>Innovation Value Institute, School of Business, Maynooth University, Maynooth, Ireland

**Keywords:** Transparency Consent Framework, GDPR, Programmatic Advertising, Online Advertising Campaigns, Demand Side Platforms.

**Abstract:** With General Data Protection Regulation (GDPR) introduced, many online advertising practices were affected as data-driven techniques were inhibited by missing user consents. Meanwhile, the IAB Europe introduced the Transparency and Consent Framework to adapt the GDPR requirements into the online advertising ecosystem and provide support in handling consent management for involved actors. In this paper, the impact of the new framework from a programmatic advertising campaign perspective is reflected from a practitioner point of view and implications of missing user consent in five typical techniques which are applied in programmatic campaigns (targeting, retargeting, frequency capping, frequency tracking and cross-device targeting) are addressed and also viewed from an e-commerce perspective. The discussion indicates potential losses in the effectiveness of the applied techniques as well as a potential shift in the market towards walled-garden DSPs such as Google or Facebook. It further provides awareness to raise the potential implications addressed and open future work in this regard.

## 1 INTRODUCTION


The introduction of the General Data Protection Regulation (GDPR) has affected a wide range of data-driven industries and influenced particularly digital marketing practices and the programmatic advertising (PA) industry. Data collection and tracking became more and more inhibited ever since. In order that advertisers are able to fulfil their advertising activities but ensure to comply with the GDPR, the “Transparency and Consent Framework” (TCF) was introduced by IAB Europe in March 2018.

The TCF provides technical specifications and infrastructure for requests and transmissions of user consents between publishers, advertisers, marketers and other technology providers who are involved in the data-driven advertising ecosystem (IAB Europe, 2020). With the help of “Consent Management Platform” (CMP) providers, users have the opportunity to decide which publisher to give consent or not upon visiting the page. CMPs are IAB certified platforms and function practically as gatekeepers. Since the introduction of TCF in version 1.1, a slight decline of data-driven measures was observed

(Aridor et al., 2020). In August 2020, TCF 1.1 was updated to version 2.0 and one of the improvements represented the introduction of the “GDPR Consent Strings”. The GDPR Consent String needs to be attached to the URL of the respective publisher (e.g. URL of the ad server, tracking URL of the data management platform or tracking URL of an audience verification provider). The string enables publishers to make sure that user consent is provided. In the case of missing consents at publishers, problems in the displaying of advertising can occur.

Of great significance is this limitation for e-commerce providers and their websites as data tracking is essential to measure general campaign success and especially conversion rates leading to sales.

In literature, there is a wide range of coverage of this matter from different points of view (e.g. Palos-Sanchez et al., 2019; Nouwens et al., 2020 or Santos et al., 2019). However, so far, there is a lack of discussion of the implications of the TCF on typical PA campaign activities in detail such as targeting, retargeting, frequency-capping, or cross-device targeting. This paper provides a reflection about the

 <https://orcid.org/0000-0001-9715-7167>

potential limitations caused by missing user consents and consequences to the effectiveness of those features from a practitioner point of view. The aim is to trigger discussion in this field and rise awareness for potential implications to the industry.

The reflection reveals major potential shortcomings in the effectiveness of techniques in the advertising ecosystem and the proposition that affected actors should not remain inactive but develop ideas and strategies to overcome the limitations.

The remainder of the paper is structured as follows. The next section provides an overview of PA campaign techniques and discussions on how they are likely impacted by the new regulation. Examples in the context of e-commerce are provided. The last section concludes the discussion and proposes several alternative suggestions.

## 2 OVERVIEW PROGRAMMATIC ADVERTISING TECHNIQUES ALONG CAMPAIGNS

Programmatic advertising campaigns incorporate several techniques in conjunction to provide successful implementation and delivering value to the user as well as to the clients. There are typical techniques applied and ideally, all of them are utilised to steer and optimise running campaigns. They cover mainly targeting, tracking as well as cross-device activities. For an overview, Busch (2016) or Stevens et al. (2016) are recommended.

For this paper, five basic techniques are chosen as they seem to be of most relevance in the context of user consent. The following tables provide description and outline of the techniques (Table 1) along with implications out of the TCF and examples

Table 1: PA techniques along campaigns.

Concept	Description
Data-targeting	Specific targeting of audiences for ads, based on interests, affinities, demographics with the help of cookies and device-IDs
Frequency Capping	A frequency cap is the maximum frequency value an ad is to be displayed in order to steer ad efficacy
Frequency Tracking	A value to measure the average ad displayed per user
Retargeting	Refers to the retargeting of previously identified and targeted user
Cross-Device Tracking	The aim is to identify a user on different devices in order to leverage

in an e-commerce context (Table 2). Thereafter, discussions in detail are given for each concept.

Table 2: TCF impact on PA techniques and e-commerce practice.

Concept	TCF impact	E-commerce example
Data-targeting	Expected major loss of data provision and thus decreased targeting potentials due to more infrequent user consent provision, leading to inefficient ad effectiveness in campaigns	Data-driven strategies can become difficult as the user who does not provide consent are not able to be targeted effectively anymore. Huge potentials would be lost, alternative strategies would be needed for consent-free targeting
Frequency Capping	A frequency cap can only be set if the user is trackable, thus provided user consent. A missing consent cannot enable effective frequency capping	Frequency capping is essential to ensure an ideal ad spend allocation per user. Coverage loss would be the consequence as well as unsuccessful conversion due to ineffective ad displaying
Frequency Tracking	A user needs to be identified in order to measure the frequency correctly. Without user consent, the amount of ad displayed per user is unknown	Frequency tracking allows determining the ideal frequency of ad displayed in each e-commerce campaign. In conjunction with conversion values, an optimal frequency can be determined. This also allows setting an ideal frequency cap
Retargeting	Required is a user consent on each site the user visits to allow retargeting. Without consent, no retargeting possible.	Important for e-commerce as visitors already visited the web-shop with potential purchase intentions. A returning user usually has a high conversion rate
Cross-Device Tracking	Without user consent, it is not possible to track the user across devices, leading to inefficient and redundant ad displaying	User switching devices while on a shopping journey would not be tracked and conversions would not be measured accurately any longer

## 2.1 Data-targeting

Data-targeting offers a variety of possibilities. Essentially, data is represented by cookies and device-IDs which share a common feature. Data enables one to reflect certain interests, affinities, purchase intentions, or general demographic features of users (Busch, 2016). There are 1st party, 2nd party, and 3rd party data types. 1st party data represents user-related data directly retrieved from the user. For instance, CRM-data or login-data gathered from the client's website are considered 1st party data, which can be used for retargeting. 2nd party data is provided by the direct partner. 3rd party data is data generated and provided by third-party companies (Stevens et al., 2016).

In the TCF context, it is not a question of the data type at first. However, identifying the user within the data requires user consent. If there is no consent, there is no data access.

Thinking about this condition, the question is: how many users will be willing to provide their consent and how many will not? It is a delicate situation as you can imagine when asked for consent. Do you want to be asked before consent "Do you want to be tracked on the internet?" or "Do you want to provide us your data?"; the majority of the users certainly would not consent because they would assume that they would be tracked as a "person". Interestingly, cookie data do not possess any personal data. In the moment of a visit, a text file (the cookie) is stored on the hard drive, containing several information types, e.g. file creation date, which subpages have been visited or which volume level was set on the web-radio. Therefore, all information is website-related and not user-related.

3rd party data providers also usually utilise the domain address the user visited. Cookie technology allows addressing all devices with a specific cookie. This represents an effective technology enabling addressing interest-related ads without relying on personal information.

However, the European Court of Justice (ECJ) has decided that storing cookies requires user consent although they do not provide direct user-related data (ECJ, 2019). The argument is that it contains pseudonymous data and therefore should be consent as well. The interesting aspect here though is the fact that the ECJ made clear that cookies do not contain personalised data. However, in practice, users may not realise this and still hesitate in providing their consent upon visiting a webpage.

It needs to be emphasised that missing consents would lead to fewer potentials out of data-targeting.

It is likely that TCF in version 2.0 will strengthen certain 2nd party data providers and weaken many 3rd party ones. Vendors such as Google, Amazon, and Facebook possess their own login "realms". If a user is registered among these vendors, he/she will be more likely to provide consent for data usage as compared to a sporadic visit of a random webpage. Moreover, users would be more interested in benefiting from various functionalities the platforms of the vendors offer.

Google, Amazon, and Facebook also possess their own Demand Side Platforms (DSP). Each vendor provides its own data within their DSPs (access to the data is therefore only possible through the use of the DSP). It is not possible to "push" data from one DSP to another – this is why these kinds of DSPs are labelled as "Walled Gardens". It is possible to feed in external 3rd party data though; however, the opposite is not possible. 3rd party data is useful in specific cases as some providers made more accurate targeting data available compared to Google, Amazon or Facebook. Unfortunately, the amount of data 3rd party vendors can provide would eventually drop. There are also DSPs that fully rely on 3rd party data only – the developments would have an effect on their market performances as well. Currently, there are various DSPs in the market with different solutions, addressing different niches. However, the threatening disappearance of DSPs would eventually strengthen the Walled Garden DSPs. Looking at Facebook, Amazon and Google, it can be said that Facebook is unique as it positions within the social media domain. Google and Amazon thus represent currently the biggest PA players in the industry, raising questions in regard to their influence in the whole market.

## 2.2 Frequency Capping

One of the advantages in PA is the ability to set a Frequency Cap (FC). A FC is the maximum frequency of the ad to be displayed per user (e.g. Buchbinder et al., 2014).

Before PA was introduced, agencies booked ad placements per publisher manually. For instance, ad placements on 20 different publishers resulted in different FC on each publisher set by the marketers. This represents a problem as ads would be displayed too frequently to users and lose potentially their optimal impact. With the introduction of PA, it was possible to set a FC on all marketers. With that, it is feasible to set a common FC of, for instance, 2 per week for over 3,000 different webpages. If the FC is set too low, the advertising impact would not be effective enough. However, this is important to

consider as ad spend with no impact would be spent. The contrary case happens when an ad is displayed too frequently to the users. This might have a negative impact on brand perception (Noller & Magalon, 2016). That is why it is important to have a balanced FC “in the middle” not to waste ad spend but also not to “bother” the user.

Users who did not provide consent, a FC cannot be set. The FC works only if there is a point of reference. Again, the point of reference could be represented by a cookie or device-ID. Walled garden DSPs would have an advantage here as they already possess relevant consents and a FC would be set accordingly.

Although non-walled gardens DSPs do apply different techniques to work around missing reference points via cookies or device-IDs (e.g. “cumulated alternative reference points”), the effectiveness and accuracy would not be of the same quality.

## 2.3 Tracking

Measuring campaign success is another crucial aspect in PA (Marotta et al., 2019). Tracking allows the campaign manager to retrieve every important information of the campaign and allow ongoing optimization through measures. The good news here is the fact that any user-independent values can still be measured. KPIs such as impressions, clicks, view-through-rates, listen-through-rates, viewability, etc. can still be measured as they are media-related.

However, there are several tracking types that do would not work as they are user-related and require consent.

### 2.3.1 Frequency Tracking

Frequency is a value that informs about the average ad displayed per user (Stevens et al., 2016). For example, a value of 3.5 indicates that a user has seen the ad 3.5 times on average. Similar to the concept of FC, frequency tracking also requires user-related consent.

### 2.3.2 Audience Verification Tracking

Audience verification tracking is useful to measure the targeting effectiveness. After a campaign is completed, the “Target Group Match” (also called “On Target Percentage”) is measured, informing about the degree of successfully addressing the intended target group in percentage.

The audience verification tracking consists of an URL additionally opened in the background next to the ad. With the introduction of the TCF, this URL also requires the GDPR Consent String. Without user consent, no results verifying a target-match could be generated. Inefficient audience targeting would be the result.

### 2.3.3 Brand Safety Tracking

Brand safety is a technique to measure the fit between the ad content and the surrounding ad placement area (rest of the webpage) in a way that it allows to set certain rules in order to avoid placements within certain themes (Noller & Magalon, 2016; Heine, 2017). For instance, a client can decide to exclude violence- or religion-related content.

As brand safety tracking is more related to content instead of the user, the TCF would not have a direct impact on this concept.

### 2.3.4 Conversion Tracking

A crucial technique, especially for e-commerce clients, is the tracking of conversions (Stevens et al., 2016). Depending on how to define a successful conversion, a conversion can represent a soft conversion (e.g. visit on the landing page) or a hard conversion (e.g. successful purchase).

For e-commerce clients, conversion tracking is of major importance as it helps to measure campaign success related to sales generation. On top of that, conversion information reveals insights about customer data such as target group characteristics, popular and most successful pages, devices, etc. so the client can steer the campaign towards best-performing settings and optimise ad spend.

To track conversions on the website, a CMP is now required to be implemented. Additionally, the provider of the conversion tracking itself would need to have attached the GDPR Consent String in the tracking. Finally, the user would need to accept and provide consent via the cookie banner upon visiting the site. Only then conversion tracking is ensured. Missing conversion tracking due to missing user consent would lead to distortion of results and could thus lead to difficulties in campaign optimizations.

## 2.4 Retargeting

Retargeting is the technique of readdressing of encountered users who were identified earlier through targeting activities (Lambrecht & Tucker, 2013). For example, the view targeting makes use of the

retargeting concept. View targeting is used for storytelling (e.g. Stevens et al., 2016) where a series of e.g. five different videos following a distinctive sequence is displayed. A user can be tagged with a so-called retargeting-pixel, allowing to consider her/him (cookie, device-ID) in the retargeting audience to address again in case the user did not finish the sequence. This process can be repeated until the user finished the sequence and the story got across. This feature works as long as the user has given consent on the relevant webpage the ad is displayed.

Similar to conversion tracking, it is possible to tag and retarget users who visited a certain landing page. The tag only works under the condition of user consent. The retargeting audiences feature is especially for e-commerce essential, as they generate high conversion rates. Within sales-heavy performance campaigns, usually, two typical steps are followed (simplified): 1. Prospecting to lead users towards the website and 2. Retarget those users who already visited the page once. Usually retargeting is prioritised as it shows higher conversion rates towards sales generation.

## 2.5 Cross-Device-Targeting

The aim of cross-device-targeting and tracking is to identify the user on different devices (Neufeld, 2017). This makes sense as this enables the frequency cap across all devices the user utilises. Without cross-device targeting, there would be separate cookies on all devices and the ad would be displayed equally as there were different users. Knowing all relevant devices belong to the same user allows considering this while placing ads (Brookman et al., 2017).

Moreover, cross-device tracking is useful for measuring conversions along with the devices. For example, users usually inform themselves about products via smartphone first before they switch to the desktop PC or laptop to purchase the product of interest (omnichannel customer journey, e.g. Verhoef et al., 2015). Without cross-device tracking, an ad displayed on the smartphone leading to a conversion on a PC or laptop would not be recognised. Cross-device tracking, therefore, is substantial to track the user in order to measure campaign success along with different devices.

There are different approaches to cross-device targeting. A deterministic and probabilistic approach. The deterministic approach is based on login-data and the user is identified without relying on tracking data (Brookman et al., 2017). Again, here it is evident that Google, Amazon, and Facebook would show an

advantage as users are required to login to their accounts along with the device information.

The probabilistic approach (Zimmeck et al., 2017; Brookman et al., 2017) however relies on different data points which can indicate to which user the devices belong through probability calculations. Examples for those datapoints are the IP address of the router, the “idle time” of the smartphone, surfing behaviour, etc. However, the deterministic approach is more accurate.

With the effect of the TCF, non-walled garden DSPs would now heavily rely on probabilistic approaches. With fewer and fewer datapoints resulted from missing user consent, the probabilistic approach would become more and more inaccurate as a consequence.

## 3 CONCLUSIONS

The discussion aimed at reflecting the impact of IAB’s TCF introduction on PA practices, particularly in the conduction of data-targeting, frequency capping, tracking, retargeting and cross-device-targeting as crucial activities within a PA campaign. The reflection revealed that it may be getting more and more difficult to use data-driven ad placements. Walled garden DSPs would merely be affected due to their login-advantage and could strengthen their role in the market. However, on the other side, non-walled garden DSPs and 3rd party data providers would be more and more limited in their opportunities and would run into the danger to lose relevance in the market. As a result, new approaches and strategies would need to be developed and deployed in order to adapt to the effects of the TCF.

Given the fact that there are still some opportunities left for data-driven ad placements, one can consider following a “hybrid approach”. This would imply splitting a campaign into two components. The first part would be run as usual and utilise remaining datapoint potentials. This would allow addressing trackable users. For those users who would not provide consent, the second part would be initiated. In this part, alternative strategies with no data usage would be rolled out to target those users who are not addressed with step 1 (tagging those who have provided consent can be easily excluded). An alternative targeting strategy would be e.g. “Contextual Targeting” relying on certain themes and keywords based on URL. A corresponding alternative approach to measure conversion could be achieved via a “discount code” shown directly on the ad or while landing on the website. The code would serve

as a successful conversion once redeemed (it needs to be noted that the code should be redeemed only once and changed immediately on the ad).

Currently, it can be observed that several marketers join together to form groups and bundle resources to retrieve consents. This increases the probability to retrieve consents which then can benefit the group.

Another approach to improve consent generation would be a more user-friendly design of the cookie banner / consent window.

A further thought is an idea of maintaining a loyalty points platform concept to incentivise users to provide consent.

This work represents a short discussion paper and therefore is subject of the following limitations which most of them could be considered as future work. As the purpose is to trigger discussion and increase awareness of the problem space, no empirical perspectives are applied. It would be interesting to reflect further the topics discussed on specific cases. Furthermore, developments are fast and dynamic, and it is likely that e.g. TCF 3.0 is introduced soon with new constraints for the whole industry to consider.

## REFERENCES

- Aridor, G., Che, Y. K., & Salz, T. (2020). The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR (No. w26900). *National Bureau of Economic Research*.
- Buchbinder, N., Feldman, M., Ghosh, A., & Naor, J. (2014). Frequency capping in online advertising. *Journal of Scheduling*, 17(4), 385-398.
- Busch, O. (2016). Programmatic advertising. *New York: Springer*, 10, 978-3.
- Brookman, J., Rouge, P., Alva, A., & Yeung, C. (2017). Cross-device tracking: Measurement and disclosures. *Proceedings on Privacy Enhancing Technologies*, 2017(2), 133-148.
- European Court of Justice (2019). Storing cookies requires internet users' active consent. *Court of Justice of the European Union PRESS RELEASE* No125/19. Retrieved from <https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-10/cp190125en.pdf>.
- Heine, C. (2017). With brand safety in focus, digital advertisers are quickly shifting toward direct programmatic.
- IAB Europe (2020). TCF - Transparency & Consent Framework v.2.0. Retrieved <https://iab europe.eu/tcf-2-0/>.
- Lambrecht, A., & Tucker, C. (2013). When does retargeting work? Information specificity in online advertising. *Journal of Marketing research*, 50(5), 561-576.
- Marotta, V., Abhishek, V., & Acquisti, A. (2019). Online tracking and publishers' revenues: An empirical analysis. In *Workshop on the Economics of Information Security*.
- Neufeld, E. (2017). Cross-device and cross-channel identity measurement issues and guidelines: How advertisers can maximize the impact of an identity-based brand campaign. *Journal of Advertising Research*, 57(1), 109-117.
- Noller, S., & Magalon, F. (2016). Programmatic brand advertising. In *Programmatic Advertising* (pp. 111-122). Springer, Cham.
- Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020, April). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1-13).
- Palos-Sanchez, P., Saura, J. R., & Martin-Velicia, F. (2019). A study of the effects of programmatic advertising on users' concerns about privacy overtime. *Journal of Business Research*, 96, 61-72.
- Santos, C., Bielova, N., & Matte, C. (2019). Are cookie banners indeed compliant with the law? deciphering eu legal requirements on consent and technical means to verify compliance of cookie banners. *arXiv preprint arXiv:1912.07144*.
- Stevens, A., Rau, A., & McIntyre, M. (2016). Integrated campaign planning in a programmatic world. In *Programmatic Advertising* (pp. 193-210). Springer, Cham.
- Verhoef, P. C., Kannan, P. K., & Inman, J. J. (2015). From multi-channel retailing to omni-channel retailing: introduction to the special issue on multi-channel retailing. *Journal of retailing*, 91(2), 174-181.
- Zimmeck, S., Li, J. S., Kim, H., Bellovin, S. M., & Jebara, T. (2017). A privacy analysis of cross-device tracking. In *26th {USENIX} Security Symposium ({USENIX} Security 17)* (pp. 1391-1408).