DAGITAL LEGAL
Privacy & Technology Law Firm

Dagital Legal, s.r.o.
Nové Záhrady I/9
821 05 Bratislava, Slovakia
www.dagital.eu
+421 911 195 133
jakub.berthoty@dagital.eu

Comments on the Guidelines 8/2020 on the targeting of social media users

From: Dagital Legal, s.r.o, Privacy & Technology Law Firm, Bratislava
Date: 19th October 2020

Endorsed by: Association of Cybersecurity, Comenius University in Bratislava, Cyber Security Competence and Certification Centre, Mitsubishi Chemical Advanced Materials Composites, Planeat, SuperScale and Sygic, mentioned in alphabetical order. See Annex No. 1 (**Endorsements**) for more detail.

Dear All,

We would like to take this opportunity to comment on the Board's Guidelines 8/2020 on the targeting of social media users (the "**Guidelines**"). We very much welcome the Guidelines.

However, we feel that the Guidelines supersede general guidelines on "cookie regulation" and social media platforms, that are yet missing at the EU level. Guidelines jump into deep waters of ePrivacy's practical application and complex multi-layer relationships with social media platforms and explain only one specific type of processing, albeit the most important one. However, consensus on the underlying and more general issues in this context is missing at the EU level, which can be seen on the way how ePrivacy regulation is being adopted as well as on the Guidelines.

Therefore, we suggest including in the Guidelines a comprehensive introduction to "cookies" regulation under Article 5 (3) of the ePrivacy directive and to the overall relationship that exists in the context of social media platforms' operations. Then a specific regulatory guidance for targeting via social media would make more sense.

1. Summary

Our comments can be summarized like this:

i. "**Cookie regulation**". The Guidelines deal very little with Article 5 (3) of the ePrivacy directive. This article, its interpretation and application on newer technologies like pixels, scripts, SDKs, APIs (?), forced link redirects (?) or other technologies[1] should be the centre-point of the Guidelines. These are the technologies that practically all social media targeting is based on and we need more clarity on whether they fall under the current regulation.

ii. "**Single cookie for everything**". We believe most of the targeting is ultimately based on cookie-like technologies. This is because of the questionable practice of social media providers who often use a single cookie for running the service as well as for the marketing profiling, analytics and targeting.

iii. "**Targeting categories**". We do not feel that the proposed 4 new categories of targeting are helpful. On the contrary, there is no legal relevance on making such distinction. We propose to either formulate a different categorization or abandon such attempts altogether. In any case, using references to

[1] It might be helpful to underline in the Guidelines that „cookie" regulation does not regulate cookies as such and that by some, cookies are already seen as an outdated technology. Article 5 (3) of the ePrivacy directive and future Article 8 of the ePrivacy regulation in fact regulate wide spectrum of technologies that intercept information exchange with end user devices, cookies being just one of them. Because there is no EU-wide guidance, examples of what technologies currently fall under the regulation are scarcely given by data protection authorities. We need to bring more light into this, and the Guidelines were a perfect opportunity.

existing services like “Lookalike Audience of Facebook” would be better than making new categories of unknown content.

iv. “**Legitimate interest**”. Currently, Article 5 (3) of the ePrivacy directive does not allow ad targeting based on cookie-like technologies as the Guidelines correctly confirm in respect to the observed and inferred data based targeting. However, it is very surprising the legitimate interest is mentioned among the legal bases in respect to the first two types of targeting. We do not see why Article 5 (3) of the ePrivacy directive would not apply here as well.

v. “**Processor and controller relationship**”. The Guidelines dwell too much on the joint controllers’ relationship and do not explain the broader picture of relationships as regards controller/processor standpoint. We believe social media providers simultaneously act as processors of their business users and independent controllers and the Guidelines should recognize this before explaining only one stream of processing operations. This would not be a problem if we would have a general guidelines on social media, but we don’t.

More detailed explanation of these comments can be found in section 2 below.

2. Detailed comments

2.1 Targeting categories

Guidelines try to distinguish between four categories of social media targeting. This categorization is used here for the first time and is not a “common knowledge” among privacy professionals. The categorization is made only to show how different the roles, relationships and legal bases might be in each category. But the main difference is basically that in case of the inferred data-based targeting, one would need to comply with Article 22 GDPR?

If the categories have to be used, then it would be very beneficial to make refences to existing targeting services and cookie terminology (analytical, marketing, necessary). We understand the need for technologically neutral Guidelines, but surely there is an elephant in the room if the Guidelines do not mention Facebook and its services. Other types of the targeted advertising via other social or professional networks such as Youtube, Tumblr, Instagram, TikTok and LinkedIn can be easily compared to Facebook’s audience targeting tools. It would make the Guidelines much clearer, if we could relate targeting categories to specific types of services offered by Facebook or possibly other social networks. For instance:

Categorization	Clarification
Targeting on the basis of data provided by the user to the social media provider	We assume this refers to the most basic and the least sophisticated means of broad targeting techniques such as Facebook’s Core Audience? From the perspective of relationship and legal bases, we do not see a difference between less effective “easy demographic” targeting like Core Audience and more precise “Custom Audience” type of targeting, because both are based on information the social media provider collects from data subjects. We see difference in risks and intrusions in users’ privacy, possibly different outcomes in terms of DPIAs and Article 22 GDPR. That difference is not category, but service and technology related.
Targeting on the basis of data provided by the user of the social media platform to the targeter	Social media platforms might be used for retargeting. However, we do not feel this category refers to services like Facebook’s “Lookalike Audience”, or does it? Does it refer to something like Facebook “Customer list” or something else? Again, we see difference in risks and intrusions in users’ privacy, possibly different outcomes in terms of DPIAs and Article 22 GDPR between these services. But again, that difference is not category, but service and technology related.
Targeting on the basis of observed data	All social media providers observe the behavior and activities of their users so it is difficult to image what targeting is not based of observed data. Since the observed data falls under the wider category of data “provided” to the social media provider, a question arises whether this third and the first categories are not the same. This is only supported by a very brief description of this category in paragraph 61 of the Guidelines. In addition, the discussion about the “observed data” in light of the data portability under Article 20 GDPR is not relevant here.

	This category only refers to using pixels and geo targeting. Isn't it too narrow to define a specific category targeting based on that? What specific or other services might be included here?
Targeting on the basis of inferred data	The reason for making a distinction between targeting based on observed and inferred data is not clear to us and from the legal perspective such distinction is not even relevant. Do example 7 and 8 refer to "Custom Audience" type of services? Or do they wish to point out the specifics of using technologies like SDKs, pixels or other tools outside the social media environment?

In addition, we do not see more sophisticated targeting techniques in the examples. For example, the targeter that implemented Facebook pixels and SDKs might create a number of audiences via Facebook using its own filtering requirements. Such datasets can be then downloaded and analyzed. The targeter then runs its own big data algorithms to identify patters, biases, rules and other information that potentially lead to identification of new targeting criteria, i.e. possibly learning that its best customers are the ones that do not spend most in the first week. This big data analysis happens outside Facebook servers but once the new targeting criteria is identified, Facebook targeting services are again used to target new customers. We do not know into which category this processing falls? Is Facebook jointly responsible for such big data analyses if it allows downloading datasets? Can this additional layer of processing be based on legitimate interest?

We are trying to suggest that it would be helpful if the Guidelines recognize particular types of targeting services (by their name) and described them rather than creating new and ambiguous categories. Exact examples of using the most common targeting services and tools need to be used. Supervisory authorities did not have any problem referring specifically to Google Analytics as regards cookies consents and everyone was on the same page. We do not necessarily know what services is the Board referring to under these categories including under some examples.

We need more clarity in questions like:

- What particular ad targeting service can be used without the end user's consent?
- What technologies currently fall under Article 5 (3) ePrivacy directive and what technologies do not?
- Is there practically any ad targeting service not falling under ePrivacy rules that could be run based on legitimate interest? If so, what – according to the Board – supports the conclusion that the legitimate interest would override in case of ad targeting?
- What particular ad targeting service falls under automated individual decision-making under Article 22 GDPR and what does not?
- What particular ad targeting service might fall under the obligation to carry out a data protection impact assessment under Article 35 GDPR?
- Can we even use third country social media platforms after Schrems II judgement?
- How does the Board contemplate social networks naming all companies acting as their joint controllers as foreseen in paragraph 69 of the Guidelines?
- How does the Board look at the big data analysis of data downloaded by the targeters from social media providers?

Unless the Guidelines at least try to answer these questions, their use in practice is questionable.

2.2 Single cookie for both necessary and ad targeting processing operations

It is common (mis)practice of social media providers to gather marketing profiling data from any tool they offer. The main issue here is that a single cookie is often used for both:

(i) operation of the service or function – which could be regarded as "strictly necessary" cookie that would not need a consent under ePrivacy rules; and
(ii) marketing related data tracking and profiling sold to anyone wishing to use "audience" tools of social media provider that would need a consent under ePrivacy rules.

For the end user to see any ad – irrespective of what types of targeting services is used – he or she must run the social media application in the first place. The user has to agree to the processing under (ii) above in order to run the service, which is highly questionable practice and most likely results in collection of invalid consent under Article 7 and 8 of the GDPR. Therefore, even if the targeter does not place any cookie or

similar files to the end user equipment, any targeting is ultimately based on social media provider's cookie and data collected on its basis. We believe this is the case of at least Facebook.

This practice of social media providers is dangerous to both users but also to targeters who need to be sure that data used for targeting is collected lawfully. Therefore, it would be worth elaborating on practices like this. We need social media providers to distinguish between strictly necessary cookies and purely marketing and analytics cookies. If they merge such different purposes of processing into a single cookie, then unfortunately Article 5 (3) of the ePrivacy directive applies to all types of social media targeting and consent is needed. Subsequently, one has to wonder what use does it have to even mention legitimate interest in the Guidelines? What particular services allow targeting without cookie collection? Surely not Facebook's services. The Guidelines should clarify this in the greatest of details. Currently, this problem is not even recognized in the Guidelines.

We believe *Wirtschaftsakademie* and *Fashion ID* confirm that this problematic practice exists and so should Guidelines, that rely so heavily on this case-law.

2.3 Legitimate interest under "cookie" regulation

Article 5(3) of the ePrivacy directive does not allow for targeting or marketing related analytics without the end user's consent, at least not presently.[2] The Guidelines confirm this but only in relation to the targeting based on observed or inferred data. As mentioned above, due to the common practice of social media providers having a single cookie for everything, it is very surprising to find the legitimate interest in the Guidelines at all. Could Guidelines clarify why the ePrivacy rules are not triggered in the first two categories of targeting?

In addition, we cannot side-line the fact that the new iOS 14 operation system will likely have a built-in opt-in consent for any ad tracking, collection of advertising IDs or use of marketing analytics SDKs. It seems the legitimate interest will not be allowed on Apple devices without the end user consent anyway.

2.4 Social media providers as processors and independent controllers

The Guidelines refer to relevant CJEU judgments in *Wirtschaftsakademie, Fashion ID* and *Planet 49.* The Guidelines basically interpret the CJEU case-law as confirming that all processing operations related to ad tracking are done by joint controllers. But the CJEU never said that. In those cases, the CJEU did not primarily interpret ad tracking so the Guidelines should explain that analogy is being made here not a direct quotation.

In *Wirtschaftsakademie* the CJEU primarily replied to the question whether operator of a Facebook fan page is a controller. The CJEU replied that that it is. In doing so, the CJEU played with the idea of joint responsibility under that existed under the Directive 95/46/EC as a concept but only under the definition of a controller under Article 2 (d) that allowed determining the purposes and means of processing alone or jointly with others.[3] According to the CJEU:

"According to the documents before the Court, the data processing at issue in the main proceedings is essentially carried out by Facebook placing cookies on the computer or other device of persons visiting the fan page, whose purpose is to store information on the browsers, those cookies remaining active for two years if not deleted."

*"That processing of personal data is intended in particular to enable Facebook to improve its system of advertising transmitted via its network, **and** to enable the fan page administrator to obtain statistics produced by Facebook from the visits to the page, for the purposes of managing the promotion of its activity, making*

[2] We understand the ongoing debate about legitimate interest in Article 8 of the proposed ePrivacy regulation. However, it is not for the Board to introduce legitimate interest by the Guidelines under current ePrivacy rules. By not recognizing the practice of using a single cookie, the Board effectively does this.

[3] Article 2(d) of the directive 95/46/EC *"'controller' shall mean the natural or legal person, public authority, agency or any other body which **alone or jointly with others** determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;"*

it aware, for example, of the profile of the visitors who like its fan page or use its applications, so that it can offer them more relevant content and develop functionalities likely to be of more interest to them."

Therefore, the CJEU distinguishes between two different purposes of cookie use: advertisement purposes and anonymous statistics obtained by the fan page operator referred to as "**Page Insights**". The core message of the *Wirtschaftsakademie*'s judgement is that even though the fan page operator does not have access to the underlying personal data converted by Facebook to "Page Insights", the operator is jointly responsible with Facebook for creating it. As a result, Facebook published joint controller addendum, which only refers to "Page Insights". Page Insights are very small part of the processing that happens by virtue of operating fan page and has very little to do with ad targeting. Then on 31st August 2020 Facebook published joint controller addendum for Facebook business tools such as API, SDK, pixels and offline conversions and similar. The current understanding and Facebook's general data processing terms, however, regard anything else falling under the regime of operator/targeter as a controller and Facebook as a processor.

There are millions of valid data processing agreements under Article 28 GDPR between European business users and Facebook that impliedly cover ad targeting or operating of Facebook fan page which are not recognized and which are "squashed" by the Guidelines. This detail is not explained in the Guidelines at all and has great implications on European business users. Is the Board saying that millions of Europeans business users using Facebook have breached the Article 26 GDPR for not having joint controllers' agreement in place from May 2018? Other social media may currently have different contracts and relationships in place. We suggest that maybe a more balanced approach of having a basic rule and then exceptions from it might be more suitable.

Only paragraph 37 of the judgement can be used to support the interpretation that ad targeting is done by joint controllers:

"In particular, the administrator of the fan page can ask for — and thereby request the processing of — demographic data relating to its target audience, including trends in terms of age, sex, relationship and occupation, information on the lifestyles and centres of interest of the target audience and ***information on the purchases and online purchasing habits of visitors to its page****, the categories of goods and services that appeal the most, and geographical data which tell the fan page administrator* ***where to make special offers and where to organise events****, and more generally* ***enable it to target best the information it offers****."*

But even the above paragraph does not make a direct reference to the ad targeting and can be understood more broadly, especially if all previous and following passages are about Page Insights.

In *Fashion ID*, the CJEU replied in similar fashion that the operator of a website that uses Facebook's "**like button**" plugin is – not surprisingly – a controller. In addition, the CJEU said that such operator is a joint controller with Facebook. But even then, the joint controllers' relationship does not relate to everything Facebooks does with the collected data:

"By contrast, in the light of that information, it seems, at the outset, impossible that Fashion ID determines the purposes and means of subsequent operations involving the processing of personal data carried out by Facebook Ireland after their transmission to the latter, meaning that Fashion ID cannot be considered to be a controller in respect of those operations within the meaning of Article 2(d)."

We do not object that ad targeting on social media is to be understood as determined by joint controllers. But then the Guidelines should explain where this relationship ends and where Facebook acts as an independent controller. Again, we do not have general guidelines on this.

In addition, it is difficult to see why Facebook cannot act in some instances as a processor of its business users. The normal operation of the fan page like commenting, sharing and writing messages with fan base are not too much different from website hosting services. Millions of European companies only have a Facebook profile and do not use any targeting services. To say they are jointly responsible with Facebook in general, would be contrary to conclusions in *Fashion ID*. What the social media provider acting here as a processor does with the data is also subject to the Article 28 (10) GDPR, according to which:

"Without prejudice to Articles 82, 83 and 84, if a processor infringes this Regulation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing."

Surely, no operator of social media fan page automatically tells the provider to do any marketing related operations by simple use of its profile. The fact that the system is "corrupted" by use of a single cookie for everything should not lead us to changing logic of already established interpretation. If we do not recognise social media providers also act as processors in some instances, we will have trouble to define what exactly the processor is and what he does in the future. Imagine SaaS providers to read the Guidelines asking – aren't we also joint controllers? Who isn't?

After all, even in Guidelines 07/2020 (as defined below) the Board mentions:

"If the entity involved in the processing does not pursue any purpose(s) of its own in relation to the processing activity, ***but is merely being paid for services rendered, it is acting as a processor rather than as a joint controller.****"*

The question is, what does this relate to in case of social media providers?

We therefore recommend a broad explanation of all different possible relationships between the targeters, social media providers and users. All three streams of relationships are present in our opinion and should be explained in the Guidelines.

2.5 Joint controllers' relationship

It is clear the Guidelines are also related to draft guidelines 07/2020 on the concepts of controller and processor in the GDPR (the "**Guidelines 07/2020**") especially in respect to understanding the concept of joint controllers. According to the Guidelines 07/2020:

"In addition, when the entities do not have the same purpose for the processing, joint controllership may also, in light of the CJEU case law, be established when the entities involved pursue ***purposes which are closely linked or complementary****."*

We would like to clarify what CJEU's case-law says that joint controllers can have slightly different joint purposes, because *Wirtschaftsakademie* and *Fashion ID* clearly say exactly the opposite.

In paragraph 74 in *Fashion ID*, the CJEU says:

"Accordingly, as the Advocate General noted, in essence, in point 101 of his Opinion, it appears that a natural or legal person may be a controller, within the meaning of Article 2(d) of Directive 95/46, jointly with others ***only in respect of operations involving the processing of personal data for which it determines jointly the purposes and means****.* ***By contrast****, and without prejudice to any civil liability provided for in national law in this respect, that natural or legal person* ***cannot be considered to be a controller****, within the meaning of that provision,* ***in the context of operations that precede or are subsequent in the overall chain of processing for which that person does not determine either the purposes or the means****."*

In paragraph 76 in *Fashion ID*, the CJEU says:

"By contrast, in the light of that information, it seems, at the outset, ***impossible that Fashion ID determines the purposes and means of subsequent operations involving the processing of personal data carried out by Facebook Ireland after their transmission to the latter****, meaning that Fashion ID cannot be considered to be a controller in respect of those operations within the meaning of Article 2(d)."*

Therefore, anything other than the envisioned function of the plugin is outside the jointly determined purposes and means as is confirmed in section 4.5 of the Guidelines. The joint processing operation here was the same. It is true that in *Fashion ID* the CJEU mentions that joint controllers can have their own economic interests:

"those processing operations are performed in ***the economic interests of both Fashion ID and Facebook Ireland****, for whom the fact that it can use those data for its own commercial purposes is the consideration for the benefit to Fashion ID."*

It is also true that these economic interests can be different. But this does not automatically mean there are slightly different purposes of processing. The CJEU confirms this in paragraph 38 of *Wirtschaftsakademie* judgement where it mentions same processing to describe joint controllers:

"In any event, Directive 95/46 does not, ***where several operators are jointly responsible for the same processing****, require each of them to have access to the personal data concerned."*

Also, the Guidelines 07/2020 mention:

"Likewise, as noted by the CJEU in Wirtschaftsakademie, the processing of personal data through statistics of visitors to a fan page ***is intended to enable Facebook to improve its system of advertising transmitted via its network and to enable the administrator of the fan page to obtain statistics to manage the promotion of its activity****.22 Each entity in this case pursues its own interest but both parties participate in the determination of the purposes (and means) of the processing of personal data as regards the visitors to the fan page.23"*

This is not what the CJEU said in *Wirtschaftsakademie.* CJEU was explaining here that one cookie is used for both advertising and statistics. Statistics were the joint processing operation. In this respect, the Guidelines misinterpret the existing CJEU's case-law. The relevant paragraph reads:

"That processing of personal data is intended in particular to enable Facebook to improve its system of advertising transmitted via its network, and to enable the fan page administrator to obtain statistics produced by Facebook from the visits to the page, for the purposes of managing the promotion of its activity, making it aware, for example, of the profile of the visitors who like its fan page or use its applications, so that it can offer them more relevant content and develop functionalities likely to be of more interest to them."

It is a very dangerous concept that joint controllers could be jointly responsible for slightly different purposes because most of the basic data protection principles in Article 5 GDPR are linked to the purpose, and therefore different measures need to be put in place by each joint controller to ensure compliance with them leaving nothing joint. Joint controllers determine joint purposes as the word 'joint' suggest which means the same purposes and that is confirmed by the CJEU's case-law. The Board should not develop new concepts to describe old problems.

We hope our comments will be useful for the Board when adopting the Guidelines. I/we hereby consent to the publication of personal data contained in this document.

Kind regards,

On behalf of **Dagital Legal, s.r.o.**
and our clients
Jakub Berthoty
attorney and director

Annex No. 1
Endorsements

These comments have been drafted with the help and endorsements of the following organisations, listed in alphabetical order:

Association of Cybersecurity represents the Slovak community of information and cyber security professionals. www.akb.sk

Comenius University in Bratislava is a modern European university which in 2019 is celebrating its 100th anniversary. With thirteen faculties, it offers the widest selection of study programmes (over 800) at three levels, and several of these study programmes are the only ones of their kind offered in Slovakia. www.uniba.sk

Cyber Security Competence and Certification Centre is a non-profit organization supporting the National Security Authority in educational, awareness-raising and accreditation matters. www.cybercompetence.sk

Mitsubishi Chemical Advanced Materials is a leading global manufacturer of high-performance thermoplastic materials in the form of semi-finished products and finished parts. The company has locations in 20 countries and more than 2 800 employees. www.mcam.com

Planeat is a market-leading nutrition application for both commercial and personal use. www.planeat.sk

SuperScale are market leading game business analysts, who help game developers to commercially grow their games. SuperScale are experts on game and ad monetization, user acquisitions, business intelligence and data analytics. www.superscale.com

Sygic is a leading Slovak mobile application developer. Sygic's GPS navigation app is used by more than 200 million drivers around the globe. Sygic also provides enterprise solutions for the automotive, mobility and travel industries. www.sygic.com