October 16th, 2020

Access Now's comments to the EDPB consultation on Guidelines 8/2020 on the targeting of social media users

Introduction

Thank you for the opportunity to provide comments to the EDPB draft Guidelines 8/2020 on the targeting of social media users.

Access Now is an international organisation that defends and extends the digital rights of users at risk around the world.[1] We work on data protection and privacy around the world and we maintain a presence in 13 locations around the world, including in the policy centers of Washington DC and Brussels.[2]

In our submission, we will provide comments and suggested edits in several sections of the draft guidelines. For ease of reading, we organise these comments following the structure of the draft guidelines, rather than organising them by issues. Our comments focus on a range of issues, including the processing of inferred data, the choice of legal basis and in particular the limitation of "legitimate interest" for the protection of users' rights, the application of data protection by design and by default principles, measures to enhance users' control and the responsibility of targeters.

Our comments

As expressed in the ICDPPC resolution on privacy as a fundamental human right and precondition for exercising other fundamental rights: privacy and data protection rights are the fundamental locus in enabling the enjoyment of other rights like human dignity, freedom of expression, freedom of association and freedom of thought and belief".[3] In the draft guidelines,

[1] Access Now, https://www.accessnow.org/
[2] Access Now - About Us, https://www.accessnow.org/about-us/
[3] ICDPPC, International Resolution on privacy as a fundamental human right and precondition for exercising other fundamental rights

the EDPB concretely explains the interactions between the rights to privacy and data protection with other fundamental rights, in particular within paragraphs 9 to 14 of the sections entitled “Risks to the rights and freedom of users posed by the processing of personal data”. This context is essential to understanding the importance of the draft guidelines, not only for the protection of the rights to data protection but also for compliance with human right laws, including obligation under the General Data Protection Regulation. We further support the language in this section detailing the different roles and responsibilities associated with the many actors involved in the processing of personal data when targeting social media users.

We further support the language of paragraph 16 highlighting the increasing relationship between data protection and competition law. We suggest the following modifications “in bold” to expand on the issue:

> *16. “The EDPB recognizes that the increase in concentration in the markets of social media and targeting may also increase risks to the rights and freedoms of individuals. For example, certain social media providers may be able to combine, either alone or in connection with other companies, a higher quantity and diversity of personal data. This ability, in turn,may increase the ability to offer more advanced targeting campaigns.* ***It shall be noted that numerous complaints filed with supervisory authorities raised questions as to whether the data processed for targeting of social media users have been obtained in a way that is compliant with the obligations set forth under the GDPR.*** *This aspect is relevant from both a data protection (more in-depth profiling of the persons concerned,* ***potential unlawful processing of data****) and competition law viewpoint (the unrivalled insight capabilities provided by the platform may make it an unavoidable trading partner for online marketers). The degree of market and informational power, in turn, as the EDPB has recognised, “has the potential to threaten the level of data protection and freedom enjoyed by consumers of digital services”.”*

Moving to the section on “actors and roles”, we suggest adding to paragraph 20 a reference to the obligation pursuant Article 25 of the GDPR for data processing entities to implement the principles of data protection by design and by default to provide greater control to users:

> *20. “Social media providers offer an online service that enables the development of networks and communities of users, among which information and content is shared. Social Media services are typically offered through web browsers or dedicated apps, often after having requested the user to provide a set of*

---

https://edps.europa.eu/sites/edp/files/publication/resolution-on-privacy-as-a-fundamental-human-right-2019-final_en.pdf

personal data to constitute the user's "account" or "profile". They also often offer users associated account "controls", to enable them to access and control the personal data processed in the context of the use of their account. ***It is worth noting that a low number of actors involved in targeting activities on social media, including social media platforms, fully implement the principles of data protection by design and by default as required by Article 25 GDPR in a way that it would limit the processing of personal data by default.****"*

We further recommend the EDPB to clarify in paragraph 21 that the use of targeting on social media is not, *per se*, necessary for the functionality of the service but is part of a conscious business decision or business model. This in turns means that actors involved in targeting activities on social media need to have a clear and separate legal basis for such activities and this legal basis should be clearly indicated:

21. "The social media provider determines the functionalities of the service. This in turn involves determination of which data are processed, for which purpose, under which terms, as well as how personal data shall be processed. This allows for the provision of the social media service but also likely the provision of services, such as targeting, that can benefit business partners operating on the social media platform or in conjunction with it. ***The use of targeting by social media and their partners is part of a business model and not linked with the functionality of social media to "to stay in touch with family and friends, to engage in professional networking or to connect around shared interests and ideas" which in turn means that any targeting activities will require a separate valid legal basis to be conducted."***

We recommend that the EDPB add the language suggested below regarding inferred data and the sometimes problematic natures of the 'insights' derived from it in paragraph 22. We also note in this regard that social media companies have started to take questionable initiatives about addressing the mental health of their users based on their activities on platforms including inferences described below.[4]. While such attempts have led to public criticism,[5] it is very likely that under the difficult conditions the COVID-19 pandemic is causing for mental health as well, such initiatives may resurface.[6]

22. "The social media provider has the opportunity to gather large amounts of personal data relating to users' and non-registered users behaviour and interactions, which enables it to ***~~obtain considerable insights~~ create***

[4] See for instance https://techcrunch.com/2017/11/27/facebook-ai-suicide-prevention/
[5] See https://www.nytimes.com/2018/12/31/technology/facebook-suicide-screening-algorithm.html
[6] For more information, please see: https://privacyinternational.org/campaigns/your-mental-health-sale

significant 'insights' *into the users' socio-demographic characteristics, interests and preferences. It is important to note that the 'insights' based on user activity often involve inferred or derived personal data* ***and are sometimes based on flawed and unscientific assumptions****. For example, where a user interacts with certain content (e.g.by "liking" a post on social media, or watching video content), this action can be recorded by the social media provider, and an inference might be made that the user in question enjoyed the content he or she interacted with* ***whereas in reality they may have interacted with the content for entirely different reasons, thus contributing to a flawed profile****.* ***Inferences may also be made about highly controversial attributes, such as inferring sexuality or contentious attributes such as 'criminality' or 'terrorist sympathy' from physiological characteristics taken from photos. Despite being inaccurate, such insights may nevertheless create serious risks for people and have significant impact.***

In section 5 of the guidelines on the "analysis of different targeting mechanisms", we suggest several modifications to clarify the role and responsibilities of all actors involved in the targeting, including the users. It shall be noted for instance that when using social media, users are not necessarily considering that they are providing personal information to be targeted with content, including advertisement, but to create a "profile" and interact with other users. The fact that a platform may be using targeting, including as part of a monetizing system, may or may not be known to users and even in cases where it is, platforms rarely offer an opportunity to opt-in or out of these activities. The mere fact that users fill in information to create a profile on a social media does not mean that they agree or know that this data may be used for targeting purposes.

37. "Individuals may ~~**actively**~~ disclose a great deal of information about themselves when making use of social media. The creation of a social media account (or "profile") involves disclosure of a number of attributes, which may include name, date of birth, gender, place of residence, language, etc. Depending on the nature of the social media platform, users may include additional information such as relationship status, interests or current employment. Personal data provided by social media users ~~**can be**~~ **is often** used by the social media provider to develop criteria, which enables the targeter to address specific messages at the users of the social media. **However, it is important to note that users are not providing this information for targeting purposes but for being able to use social media where targeting is often not necessary for the service to function to but is rather part of a business model."**

We agree with the reasoning of the EDPB in paragraph 39 to 42 which identifies both entities involved in the targeting (targeters) and social media are jointly responsible for determining the

purpose and means of processing data in the context of targeting social media users. It is particularly important in this context to reiterate that "Indeed, joint responsibility of several actors for the same processing does not require each of them to have access to the personal data concerned." and "that actual access to personal data is not a prerequisite for joint responsibility." We support the language of the draft guidelines.

In the following paragraphs (unnumbered, 43 and 44), we recommend the following modifications to reflect the limitation of the use of Article 6.1.f (legitimate interest) as a legal basis, in the context of targeting social media users. In fact, the draft guidelines rightfully describe the opacity of the targeting practices and the general lack of transparency towards the users. In this context, the use of "legitimate interest" as a legal basis for targeting risks further exacerbating the power imbalance between social media and the targeters on one side and the users on the other side. Given the large number of risks identified with the use of targeting mechanisms for the rights of users, going beyond data protection rights, and the de facto power imbalance held by social media actors in defining the activities on their platforms, we recommend the EDPB to not allow for the use of "legitimate interest" for targeting activities.

> *"As joint controllers, both parties (the social media provider and the targeter) must be able to demonstrate the existence of a legal basis (Article 6 GDPR) to justify the processing of personal data for which each of the joint controllers is responsible.The EDPB recalls* ***~~that no specific hierarchy is made between the different lawful basis of the GDPR:~~*** *the controller needs to ensure that the selected lawful basis matches the objective and context of the processing operation in question. The identification of the appropriate lawful basis is tied to principles of fairness and purpose limitation."*
>
> *43. "Generally speaking, there* ***~~are two~~ is one*** *legal base****~~s~~*** *which could theoretically justify the processing that supports the targeting of social media users: data subject's consent (Article 6(1)(a) GDPR)* ***~~or legitimate interests (Article 6(1)(f) GDPR)~~****. A controller must always consider what the appropriate legal basis is under the given circumstances.*
>
> *44. "For what concerns the legitimate interest lawful basis, the EDPB recalls that in Fashion ID, the CJEUreiterated that in order for a processing to rely on the legitimate interest, three cumulative conditions should be met, namely51(i) the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed, (ii) the need to process personal data for the purposes of the legitimate interests pursued, and (iii) the condition that the fundamental rights and freedoms of the data subject whose data require protection do not take precedence. The CJEU also specified that in a situation of joint*

> *controllership "it is necessary that each of those controllers should pursue a legitimate interest [...] through those processing operations in order for those operations to be justified in respect of each of them".* ***In the context of targeting of social media users, the risks for their fundamental rights and freedom, including the rights to data protection, privacy, and freedom of expression is such that the use of legitimate interests as a valid basis is highly questionable.****"*

In sections 5.3 and 5.4 of the guidelines, we proposed language to clarify the activities of social media platforms and the importance of providing clear protections around the use of observed and inferred data.

> *61. "There are several ways in which social media providers may be able to observe the behaviour of* ***people, including users and non- registered users****. For example, observation is possible through the social media service itself or may also be possible on external websites by virtue of social plug-ins or pixels.* ***While widely used, these practices raise questions as to whether the data processed for targeting of social media users have been obtained in a way that is compliant with the obligations set forth under the GDPR."***
>
> *73. "Inferred data refers to data which is created by the controller on the basis of the data provided by the data subject (regardless of whether these data were observed or actively provided by the data subject,or a combination thereof). Inferences about data subjects can be made both by the social media provider and the targeter. People should have the possibility to see what inferences have been made about them, through their right to access, and to contest those inferences, including through their rights to object, to correct, and to erasure. Data controllers should ensure that any inferences made about people are based on sound, verifiable, and reasonable grounds, and do not put people at risk, including by impacting their ability to access services(e.g. inferring that a person is susceptible to gambling addiction, or misgendering trans people by inferring gender from physiological characteristics). Inferred and observed data shall never be used for law enforcement purposes and judicial proceedings, as well as to determine whether a data subject is eligible to access public services, to receive financial support or compensation - either when provided by public or private entities, or to access to public or private education."*

We would like to express support to the language in paragraph 67 which provided much-needed clarity on the use of cookies and on how to fulfil the conditions laid out in Article

7 GDPR. We further support the language on the application of data protection rights and transparency included in paragraphs 82 to 84.

In section 8.2 of the draft guidelines on the use of Article 9(2) exception of special categories of data made manifestly public, we suggest modifications to reiterate that even if information has been "made public" by the user, it does not mean that the user is agreeing for this information to be used for targeting. This is particularly true in a context where social media and targeters are not fully implementing the principle of data protection by default and users may not be aware of what information is necessary to provide or not.

> *120. "Article 9(2)(e) of the GDPR allows processing of special category of data in cases where the data have been manifestly made public by the data subject. The word "manifestly" implies that there must be a high threshold for relying on this exemption.* ***This Article cannot therefore be used as a legal basis in a systematic manner.*** *The EDPB notes that the presence of a single element may not always be sufficient to establish that the data have been "manifestly" made public by the data subject. In practice, a combination of the following or other elements may need to be considered for controllers to demonstrate that the data subject has clearly manifested the intention to make the data public, and a case-by-case assessment is needed.* ***Controllers who do not implement requirements of data protection by design and by default laid down under Article 25 shall not be authorised to use this exception.****"*

Conclusion

We appreciate the opportunity to submit comments to the Guidelines 8/2020 on the targeting of social media users and the continued effort of the EDPB to engage with stakeholders.

We remain available for any questions you may have.

For more information, please contact
Estelle Massé, Global Data Protection Lead (estelle@accessnow.org)
Daniel Leufer, Europe Policy Analyst (daniel.leufer@accessnow.org)