Comments on Fundamentals for a Child-Oriented Approach to Data Processing - Draft Version for Consultation

Twitter, Inc. and Twitter International Company (collectively "Twitter") welcome the opportunity to respond to the DPC's request for comments on the draft Fundamentals for a Child-Oriented Approach to Data Processing" (the "Fundamentals").

Twitter supports the ambition of better protecting children's personal data online, and wants to work with policymakers and regulators to achieve this aim while also enabling the internet to continue providing benefits to the economy, consumers (including children) and society. In this context, Twitter has the following comments with respect to the draft Fundamentals:

I. Scope:

- Twitter is concerned that the scope of the draft Fundamentals are too broad and disproportionate to the policy issue that they are seeking to address – safeguarding children's rights and personal data. The requirement to apply the draft Fundamentals's obligations to services that are "***likely*** *to be accessed by children*" will capture an extremely wide set of internet services. In effect, this will mean the draft Fundamentals will cover services that are "***able*** *to be accessed by children*", which is far beyond the intended scope, and will potentially cover services such as Twitter that are intended for use by adults, and are, in fact, used predominantly by adults.

- "Likely to be accessed" is an unclear legal concept which creates uncertainty for business. What is to be considered "likely" will be clear in some cases and subjective in others.

II. Data Minimization

- Twitter is concerned that the draft Fundamentals will result in a significant increase in the amount of data collected by companies, and in particular a substantial increase in the amount of children's data collected. The broad application of the draft Fundamentals to services that are "likely to be accessed" by children – but which in practice may have very few child users – will mean that a wide range of online services could be compelled to collect unnecessary personal information, including 'hard identifiers' such as photo ID, which is inconsistent with data minimisation principles. Similarly, Fundamental 4 and Section 3.1 of the Fundamentals (Know Your Audience), state that:

"*...it is* ***vital that organisations know who their audiences are*** *(i.e. their customers, users, readers, or visitors to their website or app, or users of their internet of things device, whose personal data they are collecting and using)* ***so that they can tailor their transparency information for optimum accessibility and understandability****."*

It is impossible to do this without collecting additional identification data which runs counter to the principle of data minimization. For example, services like Twitter would have to collect photo IDs where they normally would not, which means they would collect, store and process data they do not otherwise need to have. Alternatively, they would have to use vendors to do these things that do not have the levels of security of established tech companies. It also makes the companies collecting this data an even larger target for attacks--if someone knows that Twitter or others have repositories of IDs, they are more likely to to be a target for security incidents.

III. Disproportionate Impact

- The draft Fundamentals's requirement to apply its standards to all account holders, unless age-verification is used, also means that it will have a disproportionate impact. Per Section 1.4 of the Fundamentals:

  "*In essence, organisations have two choices. Either they can* ***apply the requirements of the Fundamentals to the services they offer holistically, so that all users (irrespective of whether they are under 18 or not) benefit from a high and standardised level of data protection sufficient to protect the rights of any child users.*** *Alternatively, if organisations choose not to apply a "floor of protection" for all their users which complies with these Fundamentals, then they should take a risk-based approach to verifying the age of their users so that they can ensure that they apply the requirements of these Fundamentals to the processing of their child users' personal data.*"

- While the draft Fundamentals states that age-verification is part of the solution, recent experience in the EU and elsewhere shows that age-verification is a complicated policy issue. For example:
  - Any system that relies on online verification of information has potential for inaccuracies. It is never certain that the person attempting to verify an identity is using their own actual identity or someone else's. Currently, all age verification systems require proof of identity to establish adult status.
  - Any system that relies on public records has a better likelihood of accurately verifying an adult than a minor due to higher probability of public records being available.
  - Instituting a mandatory age-verification step during sign-up greatly increases friction for both online services and consumers.

- It is a challenge to try to find some genuine form of authentication that is also secure in privacy terms, great in security terms and reasonably achievable to the average person who simply wants to use an online service.
- Mandatory age verification will create a false sense of security for parents and children alike. It will lead them to believe they are entering "safe spaces" simply because someone has said account holders are "verified."
- There are data minimization concerns as explained above.

Thus, at this point in time, for a range of technical, operational and legal reasons, it is not feasible or desirable to put in place the required age-verification mechanisms to distinguish adults from children across a wide range of online services.

IV. Uncertainty for Online Businesses

- We welcome the DPC's endorsement of the FTC's established mechanisms for obtaining parental consent in Section 5.1 of the Fundamentals. However, by automatically presuming that good-faith efforts to enforce age limits through Terms of Service or other policies are ineffective, the Fundamentals cast doubt and create uncertainty with respect to business practices widely adopted by many online services. For example, Twitter has created mechanisms to:
  - Request consent from a parent or guardian prior to activation of an account when it is detected that a person is under age based on information provided in the sign-up flow (i.e. the person's age and their country of residence); and
  - To suspend account access where it becomes aware that an underage person is using the service. These accounts can be re-enabled once verifiable parental consent is obtained.

  The Fundamentals, as drafted cast doubt on: (i) whether such mechanisms are adequate measures to comply with the Fundamentals; and (ii) where Twitter stands with respect to Section 5.4 of the Fundamentals which states that: "...*compliance with the requirements of these Fundamentals, in no way justify the "locking out" of children from a rich user experience simply on the basis of purported data protection compliance.*"

- Depending on how the requirements in the Fundamentals are interpreted, they could lead to a requirement to reinvent portions of the service on the assumption that children may be able to access and use it.

- Section 7.3 of the Fundamentals suggests that where communications could be shared by children, the audience for such communications should be limited by default. Twitter's services are not intended for use by children, and Twitter repeatedly

emphasizes to all account holders that Twitter is public by default (see the top line messaging in our Privacy Policy for example). It places a considerable burden on online services to first pro-actively collect additional data to identify children on their services, and then apply customized audience settings to the identified account holders.

V. Bright Line Rules would Help Mitigate Uncertainty and Subjective Interpretation

- For the purposes of children exercising data protection rights, the Fundamentals consciously choose not to provide a bright line demarcation that services could practically implement. Instead, the burden is placed on online services by stating in Section 4.1 that:

  > "*Children of different ages have different levels of understanding and needs, and there is no "magic age" at which a new level of understanding is reached.... Accordingly, the DPC does not consider that it is appropriate to set a general age threshold as the point at which children should be able to exercise their rights on their own behalf.*"

  This will lead to further confusion among online services, and will prove a barrier to compliance.

- Similarly, in Section 4.2, the Fundamentals suggest separate tests with respect to when to provide data to children as opposed to their guardians, and when to prefer children over guardians. For example, it is suggested that the closer the child is to 18, the more likely it is that the online service should deal with them directly, rather than with their parent/guardian. This will mandate the creation of new workflows, will discourage compliance, drive up costs, and create the risk of human error due to subjective interpretations, and the lack of a bright line test.

- On the other hand, we welcome the DPC's position in Section 2.4 of the Fundamentals that child protection/welfare measures should always take precedence over data protection considerations and that the GDPR and that data protection in general, should not be used as an excuse, blocker or obstacle to sharing information where doing so is necessary to protect the vital interests of a child or children. This provides helpful and clear guidance.

We thank you again for engaging in this public consultation process, and for allowing us the opportunity to comment on the draft Fundamentals.