**UN Special Rapporteur on the Right to Privacy**

*‘A Better Understanding of Privacy: Children’s Right to Privacy’*

Call for Contributions

**Introduction**

Facebook welcomes the opportunity to share insights and views as part of the UNSRP’s call for contributions on the privacy rights of children and issues relating to their autonomy. Protecting children is a critical goal and we fully support measures to uphold the privacy rights of children and young people in a way that is safe and protective for them.

The right to the protection of children’s privacy as well as their other rights, such as their right to association, play, access to information, right of education and freedom of expression are as important as measures aimed at protecting them. Careful balancing of these rights is needed in order to protect children and young people. Indeed, the best interests standard is an important lens through which to view and balance the right to privacy as well as other key rights under the UN Convention on the Rights of the Child (“UNCRC”), including the right to appropriate information (Article 17) and the right to education (Article 28).

Facebook appreciates the opportunity to share comments in this important proceeding. We are committed to providing services that reflect a broad view of the best interests of children and young people who use them, in coordination and consultation with young people, parents, regulators, policymakers, and civil society experts.

Recent events have demonstrated the importance of connecting children and young people through Internet services. During the Covid-19 pandemic, greater numbers of children and young people are using the internet for at-home schooling as well as to connect socially with their friends and family. On Facebook’s Messenger Kids product alone, daily active accounts on Messenger Kids have grown over 3.5x since the beginning of March. Facebook is conscious of its role in protecting privacy while supporting this increased child engagement, particularly as Messenger Kids has been touted as a useful tool for children to engage online with parental supervision.

For purposes of these comments, we have focused our response on questions that raise particular challenges to the privacy rights of children and young people as well as to their independence and autonomy in the context of their development through social media and using the online environment.

As discussed in further detail below, Facebook offers the following recommendations to the UN SRP to inform its report to the UN Human Rights Council:

1. To recognise that parental consent and age verification can be important tools in the right context, but they are not a cure-all for addressing privacy concerns and, in some cases, can undermine privacy and other rights;
2. To encourage and provide flexibility for companies to protect privacy through a range of tools that are appropriate and proportionate, based on the nature of their services and the populations using those services;
3. To encourage partnerships between governments, civil society, and industry to co-create tools that serve the best interests of children and young people to better enable age-appropriate online experiences.
4. **Recognise that parental consent and age verification can be important tools in the right context, but they are not a cure-all for addressing privacy concerns and, in some cases, can undermine privacy and other rights**

The UNCRC highlights the importance of children having their voices heard in decisions that impact their futures. In recent years, there has been increasing momentum in legislating specific requirements for children and young people, particularly with respect to age verification and parental consent.

Because all children and young people should have the opportunity to access age appropriate online services, measures which may restrict or prevent them from accessing the Internet must be approached carefully, taking account of their independent rights to privacy, expression, freedom of information, and participation in civic engagement and online education.

As children and young people develop, they increasingly turn to the online environment as a source to obtain news and information, to get educated, to connect with their friends and family as well as to play. Therefore, it is in the best interests of the 13-18 age demographic to empower them to engage in these activities with age-appropriate safeguards in place, rather than restricting access outright.

In the required balance between the right of children and young people to access online services and the need to ensure that they are adequately protected, prevailing narratives focusing only on restricting access for those under the digital age of consent rather than ensuring that people have age appropriate experiences online may threaten the privacy, autonomy and independence of a substantial number of children and young people around the world.

**Parental controls should be implemented in accordance with the child’s evolving capacities**

Those with parental authority play a pivotal role in supporting the development of children and young people and determining what is best for them. Article 5 of the UNCRC emphasises the need to respect the responsibilities, rights and duties of parents, extended family members or legal guardians to provide the appropriate direct and guidance in the exercise by the child of the rights recognised in the UNCRC. In many instances, the parent is best placed to support the development and best interest of the child, and it is important that parents feel empowered to guide their children’s online activity. In order to uphold the child’s right to privacy, parental controls must be proportionate and in accordance with the child’s evolving capacities.

However, placing the responsibility *solely* on parents to manage their children’s online experience, particularly as children move towards young adulthood, may not be the best way of ensuring that the best interests of a child, when considered holistically, are met. Although parental controls can be an important component of protecting children’s privacy, their role should take on less importance for older youth. For those populations, organisations should provide the tools to guide and support parents, for example by providing information on indicative age-appropriate safeguards for certain age groups and educational resources for parents on how to have important conversations with their children in relation to online safety.

**Age verification is not a guaranteed solution, and instead should be implemented in a risk-based and proportionate manner**

Age verification is a complex and industry-wide challenge requiring thoughtful collaborative solutions that protect children’s privacy and safety, without unduly restricting their ability to access information, express themselves, play, receive an education and build community online. Solutions to verify age are still a developing area. It is critical to collectively figure out how to do this fairly, in a way that does not present a barrier for young people in accessing online services, for example by excluding large numbers of young users who may simply be unable to prove their age. Any solution which aims to protect young people online needs to be aware that millions of people, in particular, young people, often do not have a reliable and easy way to prove their age or identity off-line or on-line, in particular, when they are of young age.

In tandem with this, it is important that age verification solutions are proportionate in response to actual risks posed. Any evaluation of age verification solutions should be context-specific and take into consideration the risks involved with the use of the online service along with the age appropriate safeguards (from both a privacy and safety viewpoint) in place.

On the other hand, age verification solutions should avoid creating excessive collection of data which may potentially lead to subsequent security and privacy concerns. For example, requiring individuals to provide official identity documents in order to prove their age and identity would be providing far more detailed personal data than would otherwise be necessary to use certain services, in tension with key privacy principles such as data minimisation and proportionality.

These are also challenges that exist in relation to parental consent. A key challenge with regard to requirements regarding parental consent is how platforms and parents could evidence their parental/guardianship status and consent. This potentially requires the collection of even more sensitive information (e.g. birth certificates, adoption court rulings, custody court decisions, family official books). This problem is likely more pronounced in countries where age verification measures require some form of government ID, which may result in the exclusion of large parts of the population that do not not have government IDs. Furthermore, a related challenge here would be situations wherein a non-parent plays a guardianship role, but that relationship is not evidenced by a legal document. For instance, in situations where a family member such as a grandparent, aunt or uncle, or older sibling who through various reasons may have assumed the role of a parent/guardian but who do not have official documentation to evidence this.

Requiring young people to obtain the consent from a parent to access the Internet does not solve the need for age appropriate safeguards. In reality, such requirements may simply shift the burden for protecting young users to the parent rather than requiring companies to implement robust and innovative protections designed to address the potential risks present to young users.

For the reasons that we have outlined, we recommend that the UNSRP’s report accounts for the fact that parental controls and age verification measures alone do not suffice in meeting the best interests of the child. Instead the UNSRP should support organisations to leverage a range of tools to ensure age-appropriate experiences for children.

1. **Encourage and provide flexibility for companies to protect privacy through a range of tools that are appropriate and proportionate, based on the nature of their services and the populations using those services**

Measures to ensure that young people are above a certain age should not be seen as the ‘silver bullet’ in relation to protecting children online, and instead one of many measures that can be used in conjunction with other “tools” such as data education; age-appropriate content; privacy by design and by default; transparency and data minimisation to protect children online. These tools can be adapted accordingly to provide adequate safeguards whilst at the same time respecting the child’s privacy rights and autonomy.

The tools should be adapted according to the maturity of the child or young person, instead of a one-size-fits-all approach. For example, at Facebook we have differentiated the products that we offer, according to the age of the child or young person. We offer Messenger Kids for children aged 6-12, while Facebook, Instagram, Messenger and WhatsApp require everyone to be at least 13 years old before they can create an account.

At Facebook, we have a variety of measures in place to ensure that young people who use our services have age-appropriate experiences. Young people generally have a more limited experience on Facebook when it comes to the features they have access to, who they share and connect with, and the content they see (including ads).

These safeguards and measures are aimed specifically at protecting children and young people by ensuring that they have an age-appropriate experience. The most effective way to create a safe digital experience for children and young people which has regard for their autonomy, is to place the responsibility on the shoulders of organisations. Rather than sole reliance on parental controls and age verification solutions, organisations should be required to ensure age-appropriate experiences for children and young people by implementing a range of robust safeguards and measures in an accumulative way, which are proportionate to risks posed by their services. Furthermore, the UNSRP should further recognise that the right approach depends on the context of the service, and should equally promote the suite of rights applicable to children and young people, including the right to expression and protection of privacy.

1. **Encourage partnerships between governments, civil society, and industry to co-create tools that serve the best interests of children and young people to better enable age-appropriate online experiences.**

Given the fact that the internet and the majority of online services have been designed by adults and for adults, tools to ensure age-appropriate experiences is an under-developed space. In line with this, we would encourage the UNSRP to explore partnerships between governments, civil society, and industry to co-create tools that serve the best interests of children and young people and enable them to have safer online experiences. This will encourage a wider selection and availability of tools to help foster age-appropriate experience, which in turn would help to encourage wider adoption by online services.

Design can play a crucial role in upholding the child’s right to privacy whilst balancing measures to protect the child, in a way which respects the increasing autonomy of the child. This has been highlighted through the work of the Trust, Transparency and Control Labs (‘TTC Labs’). TTC Labs is a co-creation lab initiated and supported by Facebook that drives collaboration between policy experts, privacy experts and technologists to advance user experience around data. Following a series of collaborative workshops known as “Design Jams” focusing on the privacy and safety needs of young people across digital services, TTC Labs have produced a draft guide [How to Design with Trust, Transparency and Control for Young People](https://downloads.ctfassets.net/94xygyiuusop/6TXRtYG6oDxNfdsuZtbNMg/9201a816fc8d0b8e9a561e7592526617/How_to_design_with_trust__transparency_and_control_for_young_people.pdf)[[1]](#footnote-1). The guide has generated three key design principles when designing online services for young people:

1. Design for different levels of maturity
2. Empower with meaningful transparency and control
3. Provide data education over time

The key principle is that digital services should design for increasing agency as young people evolve and explore their own distinctive identity, while respecting that there are differences between physical age, emotional maturity, digital literacy, and cognitive ability. This approach is in line with other industry guidance such as the Unicef Industry Toolkit on Children’s Online Privacy and Freedom of Expression[[2]](#footnote-2). Differences within and across age groups can be substantial and age is not always a consistent marker of privacy and safety knowledge. In order to provide appropriate experience for young people, services must provide tools that account for these differences and evolve with people so that they can apply appropriate safeguards accordingly.

In addition to this, the TTC Labs guide details a number of practical considerations relevant to designing online services for young people in way that respects their increasing and evolving autonomy and independence:

* Does data privacy and safety education evolve as a young person matures?
* Is there a way for young people to adjust their experience and settings as they mature over time?
* Do you provide guidance for any user-generated content created by young people? Does that guidance change over time?
* Can young people revisit their privacy and safety decisions over time?
* How do parental controls evolve as the young person matures?

In line with the work that has been undertaken by the TTC Labs, we believe that there is much more scope to work in partnership across governments, civil society,and industry to co-build solutions that can serve as prototypes for designing age-appropriate services.

**Conclusion**

We fundamentally believe in the crucial importance of providing special protections for young people, and have long had a variety of measures in place to ensure they have age-appropriate experiences on our services. We have designed our products to give children and young people a voice, and the ability to express themselves, access information, and build community online within a safer, age-appropriate environment designed specifically for them. Children and young people have a right to be heard, and our products give them a voice and the tools to explore their identity and access information while enjoying special privacy and safety protections. Access to these tools also enables them to build digital skills, awareness of online risks, and resilience in a more protected environment as they continue their journey toward adulthood.

1. The Youth Design Guide is currently in draft format, whereby this will be finalised following consultation with global experts and youth ambassadors [↑](#footnote-ref-1)
2. https://www.unicef.org/csr/files/UNICEF\_Childrens\_Online\_Privacy\_and\_Freedom\_of\_Expression(1).pdf [↑](#footnote-ref-2)