Meta

EU Digital Services Act
Meta's views on European Commission's Call for Evidence on Article 28 Guidelines

1. Introduction

Meta Platforms Ireland Limited (thereafter "Meta") welcomes the opportunity to provide feedback to the European Commission's Call for Evidence on the future Guidelines on Article 28 of the Digital Services Act (DSA).

Meta shares the Digital Services Act's goal of creating a safer, more predictable and trusted online environment, as well as the important policy objective of protecting minors. Meta is committed to raising the standard for protecting minors and supporting families online. We believe that harmonized regulation in the European Union and a cross-industry, multi-stakeholder approach with parents, youth representatives and mental health experts are essential to build strong youth standards that protect young people's online participation.

Keeping young people safe online is a top priority for Meta. With more than 3 billion people from all over the world using Meta's family of apps and billions of pieces of content posted on our platforms every day, we take the issue of safety on our platform very seriously, especially the safety of children. It's one of our most important responsibilities. As such, we welcome the work of the European Commission aimed at achieving an effective level of protection across the industry which balances privacy, safety and security of minors online.

2. Meta's approach to protection of minors

At Meta, we have experience in tackling these issues, including through establishing policies, building tools and technologies, and producing guides and resources, all in partnership with experts both within and outside our company, to create a safer online environment for minors.

We have designed our services to be safe for all users, integrating a comprehensive suite of safeguards and controls; and have implemented further safeguards in the interests of young people, where possible, striking a balance between protecting them and facilitating their connection and development in the digital environment. To date, we've developed more than 50 tools and resources to support teens and their parents, including enforcing strict age limits, restricting adults from contacting teens, and using default privacy settings to protect teens.

Meta has designed its services to be safe by providing a suite of in-app safety tools and privacy and security features available to all users service-wide. They include specific measures to govern activities online through our Community Standards and Community Guidelines, default settings for accounts of minors, time-management tools, restrictions to unwanted interactions, as well tools around parental supervision. These protections are in addition to Meta's policies regarding minimum age, age assurance, and specific advertising policies for minors. We outline in the Annex more details on these policies and tools to address safety of minors online. We have also recently launched "Teen Accounts" in the US, Canada, Australia, and the UK - with plans to begin roll-out in the EU later in 2024.

Instagram Teen Accounts
As a part of our continued effort to ensure the safety of young people and help parents and guardians manage time online, we're introducing Instagram Teen Accounts - a new experience for teens, guided by parents. We have started to place teens into Teen Accounts in the US, UK, Canada and Australia, and plan to start placing them in Teen Accounts in the European Union later this year. Teens around the world will start to get Teen Accounts in January. We'll also bring Teen Accounts to other Meta platforms next year. These are big updates that will change the Instagram experience for millions of teens, and we need to make sure they work correctly.

Teen Accounts is rooted in research and consultation with families and experts across many countries (including Ireland, Germany, Spain, Italy, Belgium, Czech Republic, Sweden, the Netherlands) where we learned two key insights: 1. A key insight drawn from this engagement is that younger teens' needs on Instagram differ from those of older teens, with no two teens alike. 2. Parents play a critical role in supporting their teens' online experiences and are especially concerned about (i) what content their teen sees, (ii) the potential for suspicious or unwanted contact; and (iii) time management; how long their teens are spending online. With these insights in mind, we built Teen Accounts to reflect these top concerns and research.

Teen Accounts have built-in protections that limit who can contact them and the content they see, and also provide new ways for teens to explore their interests. We'll automatically place teens into Teen Accounts, and teens under 16 will need a parent's permission - through our Parental Supervision tools - to change any of these settings to be less strict. Teen Accounts will utilize our current if any of you want to take the floor to flag what we do, feel free to fication tools and we're also building technology to find accounts that belong to teens and automatically place them in protected, age-appropriate settings.

We've invested in technology to restrict teens from misrepresenting their age to avoid the Teen Account experience, but we need app stores to help us. Parents are required to share birthday information when they purchase a new phone for their teen or hand over their old phone, and set up the phone for the teen, and app stores should use this information to help apps like ours place teens in age-appropriate experiences. That's why we support regulations requiring app stores to verify age and get parental approval before their teen downloads any app.

Meta's policies, tools, and privacy, safety and security measures on our platforms provide an industry-leading level of protection for minors. We constantly work to enhance the protections that it provides on its services in light of industry developments, including technological changes, and we continue to invest in tools and products to help minors have a safe experience on our services, in accordance with our Best Interests of the Child Framework, which is based on the UN Convention of the Rights of the Child.

Meta's Best Interests of the Child Framework

We developed a process to help us apply the UN's Convention on the Rights of the Child directly to the products and experiences we build at Meta. We have complemented our own internal research with input from global data protection regulators to create Meta's Best Interests of the Child Framework, which distills the "best interests of the child" standard into six key considerations that product teams can consult throughout the development process:

1. Recognize and engage global youth and families using our products
2. Create safe, age-appropriate environments for youth
3. Promote youth autonomy while considering the rights and duties of parents and guardian
4. Prioritize youth well-being and safety over business goals and interests
5. Support young people's privacy in product decisions
6. Empower youth, parents and guardians to understand and exercise their data rights

The framework is available as a resource for all employees at Meta and is intentionally applied at different points of the product development cycle. Each consideration has extensive guiding questions, resources and examples to help our teams and product builders make balanced decisions. Adopting an approach that is grounded in the global "best interests of the child" standard helps us build products for young people that support their well-being and rights while promoting consistency across different jurisdictions and product teams. We continue to evolve and improve the guiding questions and resources in Meta's Best Interests of the Child Framework as we learn more through expert consultation, user research and co-design. We're excited to see how the six considerations in the framework continue to improve youth experiences across Meta technologies. Information for teens about privacy settings, ad experiences and parental controls can be found at Meta's Privacy Center.

In developing our policies and products, we bring together, among others, experts, civil society, industry and regulators. For example, we work closely with our Safety Advisory Council, comprising leading online safety non-profits, as well as over 400 safety experts and NGOS from around the world, including specialists in the area of combating child sexual exploitation and aiding its victims. We are committed to educating people on how to stay safe online and work with NGOs, industry and other stakeholders to ensure people have the resources they need to stay safe. Our Youth Advisory Council helps shape our work by providing feedback on the development of new tools, features, and policies for young people. We expanded this group to add new experts in privacy, youth development, psychology, parenting and youth media, and will continue expanding to include a diverse range of global perspectives.

More broadly, we continue to consult with experts, teens and parents. TTC Labs (Trust, Transparency and Controls Labs), is a cross-industry effort bringing together teens, parents/guardians, academics, regulators and civil society to uncover product-relevant insights and considerations for age-appropriate digital design. Furthermore, we established the Meta EU Youth Privacy Forum, which the European Commission has been part, which convenes a broad range of experts from the privacy and safety communities, to explore key policy issues, like age assurance, age appropriate experiences and parental interventions, as they relate to young people online through a multidisciplinary and multi-faceted lens.

To inform users and, more generally, the public about our efforts, we have built a Meta Safety Center on our platform to help people learn about staying safe on our site and a Parents Portal to help parents familiarize themselves with our tools and talk to their children about online safety. Most recently, we brought together tools and resources to tackle sextortion and intimate image abuse across our family of apps in an updated Sextortion page. Lastly, through the Safety Center we make it easy to access localized help through our directory of crisis resources around the world, including across Europe.

3. DSA Guidelines on protection of minors: ensuring appropriate balance between privacy, safety and security for minors online

Meta is fully committed to make sure that its platforms provide a "high level of privacy, safety and security of minors". Thus, we appreciate the European Commission's work to provide further guidance on the interpretation and application of Article 28 of the DSA. Before going into further detail, we strongly believe that we can only protect minors online if everyone is working together towards his goal–including apps of all sizes, operating system platforms, device manufacturers, and parents. We are conscious that the Guidelines would only be able to partially meet expectations needed to address protection of minors at a systemic level; therefore, we believe that long-term this will require thoughtful legislation and standards for the industry, since narrowing responsibility only to a subset of providers risks is not working.

As the European Commission considers options on how to provide further guidance on the interpretation and application of Article 28 of the DSA, we recommend a number of considerations on how the Guideline's objectives can ensure appropriate balance between privacy, safety and security for minors online.

a. *Provide clarity on the full harmonization of rules on protection of minors*

Meta considers that the Guidelines should aim to harmonize the rules at EU level and provide guidance on a framework that is the same across the EU and that it applies across all online platforms. The DSA's key objective is fully aligned with this principle and we believe that the Guidelines should equally reiterate it.

There remains a lack of clarity for online service providers on how to navigate different EU regulatory frameworks that partially address similar concerns. Thus, the Guidelines should clarify the relationship between these frameworks, as well as the expectations for online platforms given the numerous overlaps. Among those, they should provide clarity on the interlinks and overlaps between the DSA and the Audiovisual Media Services Directive (AVMSD) in the area of age verification and parental controls; between the DSA and the General Data Protection Regulation

(GDPR) and other privacy and data protection frameworks when it comes to defining rules on age assurance and age verification; and finally, how initiatives such as the European Digital Identity Regulation would fit into the debate on minors protection.

It should also seek to provide clarity on the primacy of EU law over national initiatives targeting minors protection online that would undermine the consistency of the DSA, as well as its main objectives. Recently, a number of national initiatives have sought to disrupt the consistent application of harmonized rules established by the DSA, including on protection of minors online. As an economic operator, the absence of a common EU approach would worryingly increase concerns both from a technical and resourcing perspective, and it would create 27 potentially different experiences for our users and children across the EU, leading to the inevitable fragmentation of the EU single market. In this regard, Meta welcomes the action taken by the European Commission in multiple stances to push back on those national initiatives.

b. Establish a level-playing field for the protection of minors online

To be effective, any measures foreseen by the Guidelines should incorporate EU and industry-wide solutions whereby all platforms are held to the same consistent standard. Hence, when it comes to protection of minors, we believe that a key objective for the Guidelines should be to establish a level-playing field across the ecosystem. In the same way as the EU single market risks being fragmented should different solutions or frameworks be put in place, we believe that inconsistent approaches would compromise on the safety of more vulnerable users such as minors. Harmonized, consistent solutions applicable to the whole ecosystem provide the cohesion needed to protect young people most effectively. As such, if the whole industry is held to the same standards and works together to provide safe, age-appropriate experiences, this would help young people avoid platforms that are not as safe as those that have invested in age-appropriate protections and experiences. We consider the DSA to be clear about this and we expect the Guidelines to reflect this accordingly.

It is important to acknowledge that there are differences between providers of online platforms and what works well for one service may not be the best solution for another one due to differences in purpose, technical set up, integrity structures and audience. Thus, the guidelines should guarantee a level of flexibility and proportionality to allow room for differences between services. However, this does not equal compromising the level of protection for minors, which should be independent from size or resource constraints. Similarly, it is key that providers of online platforms are not carved out from putting measures in place to contribute to minors' protection only because they do not implement age assurance and therefore "are not aware" of minors using the service. As such, in line with the explanatory statements of the Call for Evidence, we believe the Guidelines should cover providers of online platforms who are aware or otherwise should be reasonably aware that some of their users are minors. In addition, we believe that the guidelines should capture all those platforms that either permit - or do not exclude - minors to use the service as part of their terms and conditions or where their service is otherwise directed or predominantly used by minors. This should include cases where the provider is otherwise aware that some of the recipients of its service are minors, for example because it already processes personal data of the recipients of its service revealing their age for other purposes.

c. *Ensure proportionality and flexibility in the applicable solutions*

It is essential that the solutions envisaged in the Guidelines remain proportional and flexible. In this regard, the Guidelines should seek to clarify how online platforms are expected to balance the need to meet privacy, safety and security for minors online, without undermining any of these principles. At Meta, we have spent several years investing in policies and tools that take into account privacy, fairness, effectiveness, and proportionality. Getting this balance right is not easy and achieving this through a one-size-fits-all approach is equally complicated. As such, while we acknowledge that ensuring youth safety may come with trade-offs in privacy, access, and free expression for teens, this is not a zero-sum exercise and we are actively working with stakeholders to support access, privacy and free expression while giving parents the tools and assurances they are seeking.

In addition, we refer to the suggestion by the European Commission to “regularly conduct a child specific impact assessment”. While not disputing the value and objectives the European Commission is trying to achieve with such assessment, we recommend that the Guidelines clarify the expectations around it since it would depart from the requirements established under Article 28 of the DSA. Providers of Very Large Online Platforms such as Facebook and Instagram are already expected to carry out a risk assessment - including on the protection of minors - under Article 34 and 35 of the DSA, it would be disproportionate to carry out a separate risk assessment. Therefore, we recommend that the Guidelines clarify what the expectations would be and provide guidance on potential overlaps, including how the measures required under Art. 28 could inform the periodical risk assessment carried out under the DSA.

4. Providing a solution to age assurance

At Meta, we want teens to have safe, age-appropriate experiences online, and we have over 50 tools and resources to support them and their parents. We’ve spent a decade working on these issues and hiring people who have dedicated their careers to keeping young people safe and supported online. We also want to make it simple for parents to shape their teens’ online experiences. We provide tools and resources to help them set boundaries with their teens, and we have protections to keep teens safe and away from harmful content and unwanted contact.

However, teens move interchangeably between many apps, which is why we need industry standards to ensure teens have consistent, age-appropriate experiences across all the apps and websites they use.

As the EU looks at ways to address protection of minors, age assurance remains a key issue underpinning all the work online services put in place to protect minors online. As such, information about age allows us to create new safety features for young people, and helps ensure we provide the right experiences to the right age group. However, understanding user age is a complex, industry-wide challenge that requires thoughtful solutions to appropriately balance privacy, effectiveness, and fairness: first, people may misrepresent their age. Second, in asking users to verify their age it is important to offer privacy-preserving tools and more options than just ID verification, as not everyone has access to formal documentation or feels comfortable sharing these documents online.

In looking for options to design age assurance methods, there are 4 key considerations to take into account that are rooted in the best interests of the child:

1. Privacy: Any solution should minimize the additional data being collected to verify age, unless it is proportionate to the risk.
2. Effectiveness: It is key to ensure that any method that is implemented has sufficiently reliable results and that it closes any gaps for circumvention.
3. Fairness: Any effective solution should provide meaningful user transparency and offer appeals tools that are accessible by diverse audiences.
4. Proportionality: For any age assurance measure implemented, it is important to ensure it is proportionate to the risk of getting it wrong, considering potential impact to both undetected minors and miscategorized adults.

It is also important to underline the responsibility of parents and guardians towards minors and the dialogue that needs to happen between minors and caregivers about their use of online platforms. We want people, especially young people, to foster their online relationships in an environment where they feel safe, and where they leave our apps feeling good about the time they spend on them. However, platforms cannot be the sole guardian and decider of what content young people consume. Generally speaking, parents and guardians know what's best for their teens, which is why we've worked hard to make it easier for them to be involved in their teens' experiences by providing them with more supervision tools and expert-backed resources, and also why we developed Teen Accounts.

Nonetheless, parents do not have unlimited bandwidth to chase down and monitor every app their children access. The industry has an important role to play in creating safe environments that give parents peace of mind and in creating a scalable way for parents to participate in monitoring the safety of their children online across the app ecosystem.

With these considerations, we believe that the most effective, secure and privacy-oriented approach is for app stores or operating systems to provide service providers with users' ages, allowing minors to be placed in age-appropriate experiences across all the services they use. This is the case for two reasons:

- First, requiring age verification at account registration for all users may go against the privacy principles of proportionality and data minimisation. Studies show that teens use nearly 40 different apps every week in the US and we have some evidence that in European countries this app count could be even higher. While companies constantly work to keep services safe, requiring them to introduce age verification for all users might introduce additional risk by requiring users to share this personal information with multiple service providers across the internet.

- Second, many OS and app stores have existing processes in place to collect age. Verifying age once, at an app store or OS level is a privacy preserving option. It reduces the times of having to provide the same information across numerous apps

In addition, because the average teen uses dozens of different apps, with or without their parents knowing, and parental approval is required for many real-world activities, it should also be required for online activity. Parents should have an easy way to review the apps their children use and verify their children's ages to ensure they have age-appropriate experiences. Rather than having to keep track of the hundreds of apps out there - and the thousands that will be developed in the coming years (now that it's easier than ever to make new apps) - the industry should meet them where they are at - on their devices. The app store or operating system can provide a simple way for parents to verify their children's ages and review and approve apps their children are using right on their phones and tablets.

Ultimately, the way for us to do this is to work together as an industry. We can make a meaningful difference in keeping youth safe online, but only if we all work together. We are committed to youth safety and have instituted many safeguards in our design. However, we are only a part of the ecosystem. We can only protect youth if everyone is working together towards this goal–including apps of all sizes, operating system platforms, device manufacturers, and parents.

5. Conclusion

Meta reiterates its support to the development of Guidelines and welcomes the opportunity to provide feedback to the European Commission's Call for Evidence. We believe that the Guidelines represent a first step towards finding solutions to keep minors safer online. As Meta, we are committed to ensuring that teens have safer, more private, and age-appropriate experiences when they use our services. Over the past year, we've focused on a series of product and foundational investments to strengthen our protections for teens. Our efforts are expansive, and we're continuing to make progress. However, long-term solutions, including thoughtful legislation beyond these guidelines and industry standards will require everyone - from apps of all sizes, operating systems, device manufacturers, minors, parents and experts - working together towards this goal. As the work of the European Commission on the development of the Guidelines progresses, we remain at disposal for further feedback.

Annex. Inputs on Best practices

Content restrictions

- ***Content policies.*** A set of safety centric rules, such as Meta's Community Standards[1] and Community Guidelines,[2] should outline what is and is not allowed on the services . These rules should intend to keep these services safe for all users, regardless of age. They should cover a wide range of objectionable or harmful content and behaviour. For example, Meta's Community Standards identify 24 categories of violations grouped into five sections, including content or behaviour that:
    - promotes violent or criminal behaviour or that is fraudulent or deceptive (Section I: Violence and Criminal Behaviour);
    - threatens the safety of others, such as child sexual exploitation, bullying and harassment, or that violates others' image privacy rights (Section II: Safety);
    - is hate speech, cruel, insensitive, or violent, or that depicts nudity or sexual activity (Section III: Objectionable Content);
    - is designed to deceive or mislead others, such as spam or coordinated inauthentic behaviour, or attempts to gather sensitive personal information through deceptive methods (Section IV: Integrity and Authenticity); or
    - violates someone else's intellectual property rights (Section V: Respecting Intellectual Property).
- ***In-app tools to report violating content.*** Services should have reporting tools so that users can report content (e.g. accounts, posts, and comments) that they feel are inappropriate and go against the guidelines. In addition, serious harms such as child exploitation imagery and inappropriate interactions with teens are prioritised (as discussed below). These reporting tools should be easy to access and user-friendly, even for the youngest users.

Safety and security

Companies should employ and/or seek guidance from social psychologists, social scientists and sociologists to help ensure that its policies properly account for the presence of young people on its services. For example, Meta, as part of that, has dedicated health and well-being experts in its safety policy team. Meta has also consulted a range of external groups in the development of children's well-being policies, as well as to build programmes that focus on helping young people with everything from bullying to providing parents with the tools to have conversations with the young people in their lives.

[1] https://transparency.fb.com/policies/community-standards/

[2] https://www.facebook.com/help/477434105621119

- ***Best practice example:***
  Meta Safety Center. The Meta Safety Center, safety.meta.com, houses information about Meta's approach to safety across Facebook and Instagram. The Meta Safety Center is available in over 60 languages, and includes helpful information, resources and news about online safety.

  - In the Safety Center, users will find information about Meta's general safety work including its approaches to safety for young people, women, LGBTQ+ people, and others. Meta also provides information that is helpful for stopping bullying and harassment, preventing suicide and self-harm, thwarting the sharing of non-consensual intimate imagery, educating on sextortion and other issues. Finally, as finding the right localised help for online issues can be challenging, the Safety Center includes a directory of crisis resources around the world, including across Europe.

  - Meta works with global experts to include the most up-to-date information on an array of different topics. This is found throughout the Safety Center as well as in the linked resources at the bottom of each community or topic page. Meta's Safety Center is kept updated with the latest information.

- ***Safeguards against child exploitation.*** Services should maintain a zero tolerance policy when it comes to sharing sexual content involving children. For example, Meta's extensive efforts to combat child exploitation focus on preventing abuse, detecting and reporting content that violates its policies, and working with experts and authorities to keep children safe across its services. Safeguards services should maintain should include:

  - *Photo-matching technology*. photo-matching technologies that help detect, remove, and report the sharing of images and videos that exploit children. These photo-matching technologies create a unique digital signature of an image (known as a "hash") which is then compared against a database containing signatures (hashes) of previously identified illegal images to find copies of the same image. these technologies should also run on links from other internet sites shared on the services, and their associated content, to detect known child exploitation housed elsewhere on the internet. Not only would this help keep the services safer, but it also helps keep the broader internet safer, if all violating content would be reported to NCMEC or similar authorities, which then works with appropriate law enforcement authorities around the world.

  - *Improving detection capabilities*. In addition to photo-matching technology, services should uses machine learning to detect child exploitative content when it is uploaded to the public surfaces of the Facebook or Instagram services. Meta uses these technologies to more quickly identify this content and report it to relevant authorities, and also to find accounts that engage in potentially inappropriate interactions (e.g. "grooming") with teens on the Facebook or

Instagram services so that Meta can remove such accounts from these services and prevent potential harm.

- *Best practice example: Meta's Child safety hackathon*. Meta continues to invest in efforts to address child safety on its services. One such effort is by hosting a child safety-dedicated hackathon to bring together engineers and data scientists from across industry to develop technological solutions to help combat child sex trafficking. All code and prototypes developed for these hackathons are donated back to the Technology Coalition and Meta's NGO partners to help them in their work to protect children. As part of the child safety hackathon, Meta committed to help fund the Internet Watch Foundation's initiative for young people to confidentially report self-generated sexual images of teens. Meta also committed to help fund a project led by Tech Matters that will develop new technology to support child helplines and make them more accessible to children in crises.

- *Focus on prevention*. Services should develop targeted solutions, including tools and policies, to reduce the sharing of child exploitative content. For example, these tools should be aimed at preventing the searching and sharing of such content.

    - Best practice example: Meta has developed two new tools, the first is a pop-up that is shown to people who search for terms associated with child exploitation. The pop-up offers ways to get help from offender diversion organisations and shares information about the consequences of viewing illegal content. The second is a safety alert that informs people who have shared viral meme child exploitative content about the harm it can cause and warns that it is against Meta's policies and there are legal consequences for sharing this material. Meta shares this safety alert in addition to removing the content, "banking it" (for the photo-matching technology described above) and reporting it to NCMEC. Accounts that promote this content are removed. Meta also aims to prevent harm by educating young people through in-app advice and safety notices, such as reminders to teenagers on Facebook that they should only accept friend requests from people they know.

- *Best practice example: Reporting tools*. According to a study from Thorn, children who experience something negative online are more inclined to use in-app safety tools than to seek help offline. After consultations with child safety experts and organisations, Meta made it easier to report content for violating its child exploitation policies on the Facebook and Instagram services. To do this, it added the option to choose "involves a child" under the "Nudity & Sexual Activity" category of reporting in more places on the Facebook and Instagram services.

- *Best practice example: Project Protect*. Recognising that child exploitation is a problem across the internet and there is a collective responsibility to fight this abuse and protect children online, Meta has joined Google, Microsoft, and 15 other tech companies to announce the formation of Project Protect, a plan to combat online child sexual abuse. Project Protect focuses on five key areas: (1) tech innovations – to accelerate the development and usage of groundbreaking technology powered by a multi-million dollar innovation fund; (2) collective action – to convene tech companies, governments and civil society to create a holistic approach to tackle this issue; (3) independent research – to fund research with the End Violence Against Children Partnership to advance a collective understanding of the patterns of child sexual exploitation and abuse online; (4) information and knowledge sharing – to continue to facilitate high-impact information and expertise; and (5) transparency and accountability – to increase accountability and consistency across industry through meaningful reporting, in conjunction with WePROTECT Global Alliance.

- ***Detecting and removing non-consensual intimate imagery ("NCII") (or "revenge porn").*** Services should deploy technology to detect and remove NCII (using image processing and media match software)

- ***Suicide, self-injury and eating disorders.***

  - Best practice example: In relation to self-injury and suicide prevention, the Facebook and Instagram Help Centres contain resources developed by partners that are experts in this field and links to suicide prevention hotlines. These tools were developed in collaboration with mental health organisations such as Save.org, National Suicide Prevention Lifeline, Forefront and Crisis Text Line, as well as with input from people who have personal experience thinking about or attempting suicide. Such guidance includes links to safety tools that the individual can use to help control their experience. As part of this, Meta has worked with suicide prevention experts to understand the best ways to support a person who is having suicidal thoughts. Informed by the work that expert organisations (such as Forefront: Innovations in Suicide Prevention) have done on suicide prevention, Meta provides guidance and a list of actions people can take to help friends or family that may need support regarding suicide and self-injury. Such advice includes directions to anonymously report posts that include suicide or self-injury content to Facebook and Instagram, so that Meta can send resources it has developed with suicide prevention experts to the person or in some cases contact emergency services if the person seems to be in immediate danger.

  - The Help Centres also offer expert-backed support and advice for those needing support regarding eating disorders or needing help supporting a friend. Meta worked with the National Eating Disorders Association to provide tips to individuals to help build body confidence, alongside links to country-specific eating disorder helplines. Meta has also worked with the National Eating Disorders Association to offer guidance to individuals who think their friend may be struggling with an eating disorder. Other advice includes that, upon seeing a friend post something that suggests they may have an eating disorder and need help, individuals report the post on Facebook or Instagram so that Meta can reach out to them and offer support.

- In addition to the Help Centres, Meta has also taken numerous other steps with respect to suicide, self-injury and eating disorders. For example:

    - At the end of 2016, Instagram integrated suicide prevention tools into Instagram Live, which allows people watching a live video to reach out to the person directly or report the video to Instagram if they have concerns.

    - In October 2020, Instagram started showing a message at the top of search results when users search for keywords that may be related to suicide and self-injury. The message offers support directing users to resources and local organisations that could help. A similar message is shown on Facebook when users search for keywords that may be related to suicide and self-injury.

    - While Meta does not allow content that promotes or encourages self-harm and eating disorders, it does allow people to share their own experiences and journeys with these difficult issues. Meta knows that these stories can prompt important conversations and provide community support, but can also be triggering for some. To address this, in February 2021, Meta announced new ways to support people on Instagram who may be affected by negative body image or an eating disorder, including surfacing more expert-backed resources when people search for eating disorder-related content.

- ***Extensive support for potentially vulnerable users.*** Services should use technical measures to proactively find and remove potentially harmful suicide and self-harm content without losing intermediary liability protections. For example at Meta, this enables the company to look for posts that likely break its rules around suicide and self-harm and make them less visible by down ranking them and, where Meta is confident that the content breaks its rules, remove that content from its services. Meta also provides anonymous reporting tools on both Facebook and Instagram for content such as self-injury posts. Meta may connect the account reported to organisations that offer help, as well as anonymous reporting for live videos to report at-risk behaviour during a live broadcast, so the person reported receives a message offering help, support and resources. Global teams work 24 hours a day, 7 days a week, to review reports, provide this help, support and resources - and our teams prioritise reports of live broadcasts. In addition, Meta provides support resources for users on topics such as suicide prevention, and information on who vulnerable users can reach out to in times of need. For example, Meta's Safety Center (discussed above) deals with suicide prevention, and contains resources developed by partners that are experts in this field and links to suicide prevention hotlines.

- ***Services should implement measures minimising interactions between teens and adults.*** Meta takes steps to make it more difficult for adults to find and follow teens. On Instagram, for example:

    - Meta has developed new technology that allows us to find accounts that have shown potentially suspicious behaviour and stop those accounts from interacting with young people's accounts. By "potentially suspicious behaviour", we mean accounts belonging to adults that may have recently been blocked or reported by a young person for example. We prevent potentially suspicious adults from finding, following or interacting with teens, for example we don't show young people's accounts in Instagram Explore, Reels or 'Accounts Suggested For You' to these adults. If they find young people's accounts by searching for their usernames, they won't be able to follow them. These accounts are not shown comments from young people on other people's posts and young people will not be shown comments from these adults.

    - By default, all new under 18 accounts on Instagram in the EU are set to private when they sign up. This means that the teen's account will only be set to public if the teen intentionally makes that change after signing up to Instagram. We sent teens already on Instagram with public accounts a notification reminding them of the benefits of a private account and encouraging them to check their settings. Further, existing teen users who change their account privacy settings are invited to review and update their tagging settings via a blocking notice.

    - Teens who have a public account on Instagram are provided with the ability to control at a more granular level who can remix their content on Reels. They can choose to set this control to "Everyone", "People you follow" and "No one". However, new teen users who have chosen to set their Instagram account to public will be defaulted into the "People you follow" control. Content posted by teens with private accounts, like all private accounts, cannot be remixed by others.

    - Since March 2021, teens are notified via safety notices on Instagram when an adult who has been exhibiting potentially suspicious behaviour is interacting with them. For example, if an adult is sending a large amount of friend requests to teens, the recipients will be alerted and given an option to block, report or restrict the adult.

- ***Wellbeing best practice: Hiding likes and view counts.*** Meta gives users on Instagram and Facebook the option to hide likes and view counts on all posts in their feed and like counts on their own posts, so others can't see how many likes their posts got.[3]

- ***Best practice viral challenges: Dedicated policies to address high-risk viral challenges.*** To ensure the safety and security of its online communities and prevent real-world harm, Meta's content policy expressly prohibits "Coordinated Harm", explaining to users: "*Do not post content that falls into the following categories… Depicting, promoting, advocating for*

[3] https://about.instagram.com/blog/announcements/giving-people-more-control

or encouraging participation in a high risk viral challenge". Similarly, Instagram's Community Guidelines state: "*We're working to remove content that has the potential to contribute to real-world harm, including through our policies prohibiting coordination of harm... that contributes to the risk of imminent violence or physical harm*". Meta has specialists within its Content Policy team that identify high-risk viral content (on and off the services). These specialists may identify a high-risk viral challenge by examining content reports on Meta's services, through news sources or other information sources. This kind of attention helps Meta to stay prepared should a viral challenge begin on an online service (or offline) and later appear on the Facebook or Instagram services. Meta deploys a number of techniques (including a combination of technology and human reviewers) to remove high-risk viral content that expressly violates its terms and policies and/or to curtail its ability to spread across Meta's services. For example, in addition to the reporting tools discussed above, Meta may curtail the use of "hashtags" that are often associated with a policy-violating, high-risk viral challenge.

- ***Services should implement effective anti-bullying tools and features.***
    - For example, with respect to an issue of particular relevance to teens, Meta has been seeking to lead in the fight against online bullying. Meta has put in place strong policies designed to provide heightened protection against bullying, provides anonymous reporting for bullying content, and has developed technology to detect and remove bullying content even before it is reported. These tools and features include:
        - *Bulk blocking.* This tool helps users manage unwanted interactions on Instagram by allowing them to easily delete comments in bulk, and block or restrict multiple accounts that post negative comments.
        - *Pinned comments*. This gives users an easy way to amplify and encourage positive interactions by pinning a select number of comments to the top of their comments thread.
        - *Tag controls*. This allows users to manage who can tag or mention them. Located within their privacy settings under "Tags" and "Mentions", users can choose whether they want everyone, only people they follow, or no one to be able to tag or mention them in a comment, caption or Story.
        - *Blocking, unfriending, unfollowing*. When a user blocks, "unfriends" or "unfollows" another user, that other user is not notified. Meta also provides tools that allow users to easily limit their interactions with others, including limiting another user's ability to see their posts and the posts they are tagged in, or limiting who can see their past posts. On Instagram, Meta makes it harder for someone who a user has already blocked from contacting them again through a new account. With this feature, whenever a user decides to block someone on Instagram, they'll have the option to

both block that specific account, as well as any other accounts they currently have or may go on to create.

- *Snoozing*. Users can use the "Snooze" feature on the Facebook service to stop seeing posts from certain people, Pages or groups in their News Feed for 30 days; the person, Page or group is not notified when they have been "snoozed" by another user.

- *Mute*. Users are also able to "mute" interactions, to hide posts from certain accounts, without having to unfollow the account.

- *Restrict*. On the Instagram service, people can 'restrict' an account. This means only you and the person you've restricted can see their comments on your posts, until you approve them. They won't know you've restricted them, and it allows young people to take control back from someone who may be bullying them.

- *Comment controls dashboard*. The Instagram service has a Comment Controls dashboard, easily located in users' privacy settings. Within the dashboard, users can choose to select "Allow Comments From" and allow comments from "Everyone", "People You Follow", "Your Followers" or "People You Follow and Your Followers". The "Block Comments From" option allows the user to block comments made by specified users. The dashboard also allows users to select "Filters". The "Hide Offensive Comments" filter uses machine learning to detect and automatically hide comments on the user's posts and live videos that may be offensive. Users can also select "Manual Filter", which allows them to create their own list of words or emojis they do not want to see in the comments section of their posts. They can also always use the in-app tools to remove individual comments from their posts, or turn off commenting altogether by selecting the "Turn Off Commenting" option.

- *Limits*. To help protect people when they experience or anticipate a rush of abusive comments, Meta introduced Limits on Instagram: a feature that is easy to turn on and automatically hides, e.g., comments from people who are not followers or only recently started following a user. Limits allows a user to hear from his/her long-standing followers, while limiting contact from people who might only be coming to their account to target them with negativity. For example, we proactively encourage people to turn on the Limits feature when we detect a sudden rush of comments.

- *Hidden Words*. The Instagram service has a Hidden Words dashboard, easily located in users' privacy settings. When turned on, Hidden Words automatically hides abusive comments. People can either use the default list of offensive terms, or they can create their own custom list of words, phrases and emojis they do not want to see in their comments.

    - *Comment warnings to discourage harassment*. Meta shows a warning when someone tries to post a potentially offensive comment – reminding the person of the Community Guidelines and warning them that Meta may remove or hide their comment if they proceed. We have found that these warnings discourage people from posting something hurtful. For example, in a one-week period, Meta showed warnings about a million times per day on average to people when they were making comments that were potentially offensive. Of these, about 50% of the time the comment was edited or deleted by the user based on these warnings.

    - *Bullying prevention resources*. Meta has developed a dedicated Bullying Prevention Hub on Facebook and Anti-Bullying Centre on Instagram. Meta continues to explore and develop safeguards in this important space.

- ***Services should implement settings wrt. sensitive content:***

  Best practice example: "Sensitive Content" control. On Instagram, the Sensitive Content Control allows users to select whether to see less content that does not violate the Community Guidelines but that some users may not want to see or may find upsetting, offensive or sensitive (e.g. content that may depict violence, such as people fighting; content that may be sexually suggestive; content that promotes certain regulated products, cosmetic procedures, or sells health-related products and services) on different Instagram surfaces, like Explore, Search, Reels, Accounts You Might Follow, Hashtag Pages and In-Feed Recommendations. The Sensitive Content Control has three options: "More", "Standard", and "Less". "Standard" is the default state, and means we use technology to try and avoid recommending sensitive content and accounts. "More" enables people to see more sensitive content and accounts, whereas "Less" means they see even less of this content than the default state. For teen users, the "More" option is unavailable, and existing teen users are sent a prompt encouraging them to select the "Less" option. New Instagram users under 16 years old aredefaulted into the "Less" state. These measures reduce the risk of teens coming across potentially sensitive content and accounts. Further, in January 2023, Meta introduced new features that allow users even more control over the content they see on Instagram. These updates allow users to choose to hide content in the Explore tab that a user is not interested in. By selecting "Not interested" on posts, users can hide that content in Explore, and Meta will aim to avoid showing them this kind of content going forward in other places where Instagram makes recommendations, like Reels, Search and Feed Recommendations.

- ***Services should implement time management tools.***

  For example, Instagram offers tools to help teens (and families) better understand and manage how much time they are spending on the service and create healthy digital habits.

These tools include: an activity dashboard; settings to activate reminders to take breaks and set daily limits; and a way to limit notifications.

- ○ The activity dashboard allows users to see how much time they spent on the service over the past day and week, as well as the average time they spent.
- ○ Within the dashboard, they can set a reminder to help limit the time they spend on the service in a given day by creating an alert that will let them know when they have reached their time limit (e.g. every 15 minutes; 30 minutes; 45 minutes; 1 hour; or 2 hours).
- ○ With “take a break”, a user can set a cadence at which they would like to receive reminders to take a break if they’ve spent a certain amount of time at once on the service (e.g. every 10 minutes; 20 minutes; or 30 minutes). To ensure that teens are aware of this feature, Meta served teen user notifications suggesting that they turn these reminders on.
- ○ Users can also silence push notifications for a select period of time.
- ○ Quiet Mode is a new feature that helps teens manage their relationship at night via fewer engagement triggers and a less stimulating experience when browsing. When Quiet Mode is switched on: (i) notifications will be muted (by default from 10pm - 7am); (ii) app badge counter will be suppressed; and (iii) a push notification with a digest will be sent in the morning. Teens also have the option to customise an up to 12-hour window for Quiet Mode.

- ***Parental supervision best practice:***

  Supervision on Instagram. Instagram's Parental Supervision tools have been developed in consultation with experts, parents and teens, and are designed to strike the balance between bringing parents into their teens' experience and encouraging offline conversations, while still respecting teens' privacy and autonomy. The current set of parental supervision tools allows parents and guardians whose teens opt in to or agree to use supervision to: (i) view how much time their teen spends on the Instagram service across devices in the last 7 days; (ii) set daily time limits; (iii) set scheduled breaks that limit a teen’s use of the service during select days and hours; (iv) get notified when their teen shares that they have reported someone; (v) view and receive updates on what accounts their teen follows and the accounts that follow their teen; (vi) see which accounts their teen is currently blocking; and be notified if their teen changes any of these settings. With supervision set up, a teen can: (i) visit Family Centre to see a preview of what the parent sees while using supervision; (ii) see a preview of what the parent sees while supervising; and (iii) notify their parents after reporting something. Parents will be able to see the report type selected and the name of the account reported. To ensure teens’ privacy is respected, Meta makes clear that even, if supervision is set up, the teen still owns their own account. The parent/guardian is not able to see the teen’s messages, change their password or delete their account. Nor is the parent/guardian able to see the teen's posts, likes or comments unless the teen allows them to follow them or their account is public.

  - ○ Ending Supervision: Supervision will automatically end when a teen turns 18 according to the birthday they provided on Instagram. The parents and teen will be notified that supervision is ending.

- ***Services should encourage use of these tools.*** For example, Meta is testing a new way to encourage teens to update their safety and privacy settings on Instagram. Meta will show prompts asking teens to review their settings including: controlling who can reshare their content, who can contact them, what content they can see and how they can manage their time spent.

Privacy and transparency

Meta strives to provide the highest standard of privacy for teens.

- ***Best practice: Account audience defaults.*** New teen accounts on Facebook are automatically defaulted to share their posts with "friends". This means only accounts that are a "friend" can view the content they share on Facebook, unless and until the teen changes their privacy settings. New teen accounts on Instagram are "private by default", meaning that during the new user flow, new teen accounts are presented with a screen containing two radial buttons ("private" or "public"), with the "private" option pre-selected by default and placed above the "public" option. The screen also explains to teens the implications of selecting either option, including explaining that "[a]*nyone can see your photos and videos*" if a teen chooses to move away from the default and selects "public". For private accounts, only approved followers can see the account's posts and stories. Existing teens with a public account were served a notification in their Home Feed reminding them of their account audience status, detailing the more privacy protective aspects of having a private personal account, and providing them a direct link to their settings should they wish to switch to a private personal account. Existing teens with public accounts received up to three such notifications. Notifications are also presented to new teens who choose to select "public" during the new user flow. Such new teens receive up to three notifications in both their Home and Activity Feeds reminding them that they have the option to switch the audience setting for their personal account to "private" at any time. At present, the notifications are served at the following time intervals: (i) 120 days after account registration; (ii) seven days after the first notification; and (iii) 180 days after the second notification. Meta also initiated a process whereby teens who have provided Instagram with an email address receive an email if they select a "public" audience setting (whether during the new user flow or at any other time), confirming their selection and reiterating what it means to have a public account.

  Meta has made resources easily available for teens, and their parents and guardians, to ensure that they are fully informed of the applicable standards and available options.

- ***Teen resources in the Privacy Centre.*** Meta created a new Privacy Centre, where users can learn about Meta's approach to privacy across its services. Privacy Centre provides information about five common privacy topics: sharing, security, data collection, data use and ads. The Privacy Centre also offers a teen-specific module called "Teen privacy explained". In general, Meta's privacy policy provides information on how user information is processed and how it is shared on Meta's services .[4]

- ***Best practice: Educational resources for teens.*** Meta provides education for teens about its privacy features in the Youth Portal (https://www.facebook.com/safety/youth) (e.g. reviewing their timeline and tags, accessing their information, how ads work, and how to customise their privacy settings, including information on how to choose the audience for posts and how to take a privacy check-up). The Youth Portal also provides tailored and engaging information to help teens understand Meta's privacy policy. This youth-friendly privacy information helps to mitigate the risk that teens may not understand how their personal data is processed. For Instagram users, Meta also offers a guide specifically aimed at teens, dedicated to staying safe online and creating a positive experience.[5] Meta also developed the Community Safety Centre (https://about.instagram.com/community/safety), which contains step-by-step instructions to guide them through using the privacy tools and features available on the Instagram service, links to additional resources, and programs to help them have a safe and positive experience.

- ***Best practice: Educational resources for parents.*** Meta also offers additional dedicated resources for parents, guardians, and other caregivers about the Facebook and Instagram services. These include a Parents Portal (https://www.facebook.com/safety/parents), Parent Centre (https://about.instagram.com/community/parents), and Parent's Guide (https://about.instagram.com/community/parents/guide), with information about the privacy and safety tools available to their teens on the Facebook and Instagram services, top questions from parents, and advice for talking to their kids about staying safe.

- ***Best practice: Family Centre.*** Family Centre (https://familycenter.instagram.com/) is a place for parents and guardians (with their teens' permission) to oversee their teens' accounts on Instagram, set up and use supervision tools (discussed above), and access resources from leading experts. Meta has worked closely with experts, parents, guardians and teens to develop the Family Centre. Meta's vision for the Family Centre is to allow parents and guardians to help their teens manage experiences across Meta's services, all from one central place.

- ***Best practice: Education Hub.*** The Family Centre also includes an Education Hub (https://familycenter.instagram.com/education/) where parents and guardians can access resources from experts and review helpful articles, videos and tips on topics like how to

[4] https://www.facebook.com/privacy/guide/teens

[5] https://www.instagram.com/instagram/guide/take-charge-create-a-positive-instagram-experience/17865134450117820/

talk to their teens about safe use of social media, which are available to access at any time. Parents can

- also watch video tutorials on how to use the supervision tools available to them. Meta worked closely with groups like Connect Safely and Net Family News to develop these resources, and will continue to update the Family Centre's Education Hub with new information.

- ***Best practice: Transparency Centre[6] and the Community Standards Enforcement Report.[7]*** Meta has created a Transparency Centre for Facebook and Instagram that provides detailed information on the Community Standards and Community Guidelines, with explanations about its approach to content enforcement and a quarterly report that provides data about its enforcement efforts, the Community Standards Enforcement Report ("**CSER**"). The CSER contains metrics on how Meta has enforced the Community Standards across 14 policies on the Facebook service and 12 policies on the Instagram service, which broadly cover the areas of safety – including issues that have particular relevance to teens, like Bullying and Harassment; Child Endangerment; Nudity and Physical Abuse and Sexual Exploitation; and Suicide and Self-Injury – violence and criminal behaviour, objectionable content, and integrity and authenticity.

- ***Best practice: Community & Safety webpages.*** Meta provides an overview of safety controls and how users can utilise features to create and explore safely within Instagram[8] and Facebook[9]. Teens can also access the "Programs" page, which contains resources on topics important to teens, such as the "Pressure to be Perfect" and "Fostering Body Acceptance".[10]

- ***Best practice: Help Centre.*** The Facebook and Instagram Help Centres are resources where users can find additional information on how to explore, interact and create safely within Instagram and Facebook.[11] Users can easily navigate through the Help Centres to learn more about the various features available to them; how to manage their account; tips for staying safe; understanding privacy, security and reporting; and explanations of terms and policies.

- ***Best practice: In-product transparency and notices.*** Meta serves numerous in-product notices and pop-ups aimed at informing teens about their controls and product features, including multi-step user flows with numerous screens providing robust transparency. For instance, if a teen chooses to have a public personal account during the new user flow on the Instagram service, Meta serves notifications on their Home and Activity Feeds to remind them that they have the option to switch the audience setting to "private" at any time. Similarly, if a teen switches from a private personal account to a Business Account

[6] https://transparency.fb.com/

[7] https://transparency.fb.com/data/community-standards-enforcement/

[8] https://about.instagram.com/community/ and https://about.instagram.com/safety

[9] https://www.facebook.com/safetyv2

[10] https://about.instagram.com/community/programs

[11] https://help.instagram.com/; https://www.facebook.com/help

(which must be public), Meta does not present the option to add or display contact information at all (options that are otherwise available to Business Accounts); instead teens must actively find the Contact Button feature in their settings and complete detailed user flows that provide just-in-time transparency detailing the implications/risks of providing a Contact Button on the Professional Account profile. Prior to toggling on the feature, teens are invited to discuss potential risks with a parent/guardian and receive additional in-app transparency the next time they use the service, reminding them of the decision to display a Contact Button. Further, in November 2022, Meta began launching privacy-forward updates to default values for five privacy settings on Facebook. These new defaults apply to all new Facebook accounts for users aged 13 - 15 years old, in order to create an even more privacy-protective experience for younger teens. With these new settings updates, users aged 13 - 15 years old – as determined by their stated age during registration – are automatically defaulted to the more privacy protective settings. These users can review or change these settings at any time in their "Settings" tab.

Product development, review, and partnerships

Meta has put in place several processes aimed at ensuring that the development of new products takes into account the specific needs of teens and leads to the highest level of product integrity and safety for them.

- ***Best practice: Best Interests of the Child ("BIOC") Framework.*** Meta created a BIOC Framework, which distils six considerations for product work from the UNCRC; each consideration has guiding questions to help teams apply it. Each question has context and resources to make the questions actionable. The BIOC Framework helps product teams ensure that products match the needs of all teens – designing not just to accommodate general ages and stages but to support evolving privacy needs and diverse individual developmental trajectories, family structures, and fluctuations in available care. When educating product teams about these values and principles, Meta includes context on how to use the BIOC standard to make decisions and to establish a teen focus to new and existing services. These youth values and principles instil the knowledge from Meta's child safety and privacy specialists to all stakeholders involved in developing services across Meta.

- ***Best practice: Youth Knowledge Library.*** Meta recently launched an internal Youth Knowledge Library, which includes best practices for product teams throughout the company. Rooted in Meta's youth values and principles, the Youth Knowledge Library pulls together the many existing resources found throughout the company, adds new resources and builds out a robust catalogue of materials that deep dive into specific elements of teen-product development including age-appropriate design, data minimisation, parental control development and more. Teams can reference these as they build products to make sure their work is rooted in global best practices and expectations for youth privacy. These guidelines will also be included in privacy onboarding training materials for product makers. The Youth Knowledge Library is modelled off of external guidance and frameworks developed by organisations like the UNCRC, OECD, IDPC, ICO and children's rights groups, in addition to consultations with third party experts, young people, and parents/guardians.

- ***Best practice: Establishing a dedicated cross-functional team.*** Meta has supported the establishment of a significant cross-functional and cross-jurisdictional team focused on addressing youth-related regulatory requirements. This team consists of a wide variety of teams within the company, including Engineering, Legal, the Office of the Data Protection Officer, Policy (Safety, Privacy, and Public), Communications, and Research. Part of this team's responsibility is to consider the needs of teens and, by doing so, take into account the BIOC standard – the key objective of the IDPC Youth Guidance Fundamentals. This work evidences Meta's commitment to keeping up with relevant recommendations and advice.