Tithe an Oireachtais
Houses of the Oireachtas

An Comhchoiste um Leanaí, Comhionannas, Míchumas, Lánpháirtíocht agus Óige

Tuarascáil ar leanaí a chumhdach i ré na hIntleachta Saorga (IS)

Deireadh Fómhair 2024

Joint Committee on Children, Equality, Disability, Integration and Youth

Report on Safeguarding children in the age of AI

October 2024

33/CDEI/27

Contents

Related information

Publications

All publications for this committee are available on the Oireachtas website.

Committee videos

Footage of Committee proceedings can be found on the Committee videos page.

Terms of reference

Read the terms of reference for the Committee.

Contact details

The contact details for the Committee can be found on the Committee page.

Committee Membership

Cathaoirleach
Claire Kerrane TD, Sinn Féin

Leas-Cathaoirleach
Patrick Costello TD, Green Party

Members
Simon Coveney TD, Fine Gael

Holly Cairns TD, Social Democrats

Michael Creed TD, Fine Gael

Brendan Griffin TD, Fine Gael

Denise Mitchell TD, Sinn Féin

Jennifer Murnane O'Connor TD, Fianna Fáil

Sean Sherlock TD, Labour

Senator Tom Clonan, Independent

Senator Erin McGreehan, Fianna Fáil

Senator Ned O'Sullivan, Fianna Fáil

Senator Lynn Ruane, Independent

Senator Mary Seery Kearney, Fine Gael

Foreword

Some commentators have suggested that the current move by many administrations to address issues like phone use, AI and social media among young people is alarmist or reactionary. Having examined the issues, the Committee disagrees. Such technologies have profoundly changed the way we operate in the world, at such a new and large scale that we are truly living in a new paradigm. Amnesty International, The Irish Society for the Prevention of Cruelty to Children, teachers, the Ombudsman for Children, children themselves, parents and many others are sounding alarm bells. Health and wellbeing experts have linked this to major mental health challenges among our young, with the Irish Medical Organisation (IMO) having recently called for urgent action to tackle harm faced by young people as a result of social media.[1] It is essential that Ireland, being home to many of the main platforms' headquarters, acts on these issues. Some statistics to set the context are as follows:

- Ireland has the highest rate of daily internet use by young people in the EU.
- 84% of eight- to 12-year-olds have their own social media profile in Ireland.
- 24% of Irish six-year-olds have their own smartphone.
- 45% of 10-year-olds are allowed use their smartphones in their bedrooms.[2]

While the agenda title of the meetings the Committee held was 'the protection of children in the use of artificial intelligence', discussions naturally broadened into a consideration of phone use and social media, because both are so pervasive in children's lives today and draw heavily on AI technology. The report is a reflection of these hearings.

None of the recommendations made in this report will solve the issues around online safety and AI in isolation. Some of them, such as age verification and changes to recommender systems, are admittedly challenging and blunt instruments, but ones the Committee has decided to recommend despite their imperfections, because of the scale of harms the current status-quo enables. So, while those kinds of measures will be important elements of the toolkit, broader societal changes are needed across all age groups.

---

[1] Social media a "clear threat" to teenagers' mental health, say Irish doctors (thejournal.ie)

[2] Almost a quarter of six year olds have their own smartphone, survey finds – The Irish Times

While this report discusses children and young people, the impacts of AI and 'phone culture' are both societal and intergenerational. It is up to adults to set a good example and to ensure that our values are reflected online. To not acknowledge this would be at best hypocritical and at worst irresponsible. As adults, we need to be proactive in setting boundaries, modifying our behavior and educating ourselves on the social media landscape and the harm reduction tools and resources available on the apps young people are using. We need to ask ourselves some confronting questions about why there is so much harmful content online and we need to come up with some big answers about how we are going to reap the benefits of recent technological change while mitigating the accompanying harms.

The Committee makes some robust recommendations in this report, not to be critical, but centered on a concern for young people's safety online. It does so with respect to Coimisiún na Meán and acknowledges that this is new and complex territory, and there may be a desire to provide time and goodwill to platforms to act responsibly. For the Committee, that time has passed, because although we now have a new regulatory framework, platforms have continuously failed to sufficiently adhere to existing codes or agreements or to develop effective measures aimed at making the online world safer.

The majority of those who came before the Committee were united on three things:

1. Putting faith in voluntary action by companies themselves to address these issues is not viable. Strong enforcement by relevant authorities, such as Coimisiún na Meán and the Data Protection Commission is required.

2. A 'waiting for Europe to do it' approach in relation to the regulation, enforcement and legislation around AI and age verification on social media is a mistake.

3. Recommender systems should be off by default for young people.

The full list of the Committee's recommendations is available on page 11.

The Committee is very grateful to those who came before it. To centre young people's voices in this conversation, the Committee has also incorporated testimony from young people themselves who engaged with it as part of their work on the Ombudsman for Children's Youth Advisory Panel. Our thanks to them especially for their insights and

honesty. Unfortunately, it was not possible to cover all of the issues raised in the 120 pages of relevant meeting transcripts within this report, but we hope it provides a good overview.

_____

Claire Kerrane T.D.
Cathaoirleach to the Committee
9 October 2024

Introduction, witnesses and transcripts

Much good work has been produced and is ongoing to address AI both nationally and internationally. This report aims to provide a snapshot of the some of the main issues surrounding AI and child safeguarding online. It does so through the following key issues:

1. The problem with AI

2. Actions underway to address child safeguarding and AI

3. Designing with and for children

4. What children told us

5. Education, morality and the wider picture

In terms of definitions, the Committee heard that this is a challenging area to describe, with no agreed definition. One witness described the nature and omnipresence of AI as follows:

> "A system that performs tasks normally associated with requiring human intelligence. These include, for example, the ability to learn, reason, plan, understand language and vision... Children encounter AI systems every day they are working online, using smart devices or gaming, but there are many other modalities. The content they are presented with on their social media accounts, for example, is recommended to them using AI technology known as recommender systems. The movies suggested to them on Netflix and other platforms are curated using AI methods. Smartphones are packed with AI systems such as image editing, image filtering, video production, facial recognition and voice assistant technology."[3]

---

[3] Professor Barry O'Sullivan, 13 February 2024.

List of witnesses and transcripts

Meeting date	Witnesses
13 February 2024 Transcript	• CyberSafeKids Ms Alex Cooney, Chief Executive Officer Ms Clare Daly, Board Director • Irish Council for Civil Liberties Dr. Johnny Ryan, Director & Senior Fellow of the Enforce Unit Dr. Kris Shrishak, Senior Fellow of the Enforce Unit • University College Cork Professor Barry O'Sullivan • Special Rapporteur on Child Protection Ms Caoilfhionn Gallagher KC
20 February 2024 Transcript	• Coimisiún na Meán Mr Declan McLoughlin, Director of Codes and Rules Ms Karen McAuley, Director of Policy, Children and Vulnerable Adults Ms Niamh Hodnett, Online Safety Commissioner Mr Andrew Robinson, Corporate Secretary
16 April 2024 Transcript	• Tik Tok Ms Susan Moss, Head of Public Policy and Government Relations Ms Chloe Setter, Child Safety Public Policy Lead • Meta Mr Dualta Ó Broin, Head of Public Policy Mr David Miles, Director of Safety Policy, Europe, Middle East and Africa • X (Formerly Twitter) Ms Niamh McDade, Head of Government Affairs, UK & Ireland Ms Claire Dilé, Director for Government Affairs, Europe

All recommendations

Recommendations
1. Research should be conducted by the Department and relevant organisations to investigate the impact of AI systems for children with additional needs and particular vulnerabilities within that cohort.
2. In line with guideline F of UNICEFs Policy Guidance on AI for Children, measures must be taken to ensure transparency, explainability, and accountability are provided for children. The Online Safety and Media Regulation Act should be reviewed to determine whether adequate mechanisms are in place for those seeking redress for harm caused in the digital space.
3. Companies should have rigorous and effective age verification techniques in place. These should not impinge on privacy and security for users. Self-declaration, whereby the user inputs their age when setting up an account, should not be permitted as an appropriate age verification system.
4. Coimisiún na Meán, should publish specific deadlines, no later than year-end 2024, for when it requires companies to have in place and demonstrate effective measures for age verification and for recommender systems to be off by default for those under 16.
5. Recommender systems should be off by default for young people under the age of 16. Coimisiún na Meán should establish this as a legal requirement that is binding for all platforms. If Coimisiún na Meán lacks the powers to do so, then this should be rectified as a matter of urgency.
6. Government and Coimisiún na Meán need to tackle the issues discussed in this report head on and urgently.
7. Coimisiún na Meán should lead this urgent reform now by making robust demands on platforms and companies, using its powers to set the agenda, enforce and penalise where needed.
8. Government should support, encourage and back Coimisiún na Meán, using its expertise to inform policies and increasing its powers when necessary.

9. Coimisiún na Meán should use its special cooperation relationship with the European Commission under the Digital Services Act. The presence of so many large platforms with headquarters in Ireland should ensure action on age verification, recommender systems, misinformation and other online harms.

10. As well as taking measures to protect young people generally, companies, regulators and Government should develop specific protective mechanisms and safety by design for the protection of other vulnerable and protected groups.

11. The State must act to ensure that technological advances do not come at the expense of hard-won rights and equality.

12. Social media companies should be made to abide by their agreed community standards. They should amend their algorithms so that they are prevented from enabling and profiting from fake news and harmful content.

13. Platforms should prevent the propagation of disinformation and the platforming of racist or misogynistic or otherwise dangerous content that seek to undermine legally held and agreed upon human rights and entitlements.

14. The responsibility of platforms to flag and remove inaccurate, dangerous or extreme content must be acted on, enforced and applied rigorously, with penalties for failing to do so applied.

15. Guidance and educational resources for adults and children in relation to AI, social media and recent tech developments are much needed. Relevant Departments and organisations should produce and promote accessible, age-appropriate resources as a priority.

16. The enforcement of existing measures to prevent online harms should be strengthened, including those involving trusted flaggers.

17. Communities need to be given the tools and education to think critically and decipher disinformation. This should be done through schools, education and training boards, youth clubs and any appropriate body, be they statute bound, voluntary or by tender to include private entities.

18. Educators themselves need to be kept abreast of the best ways to prevent young people from becoming vulnerable to disinformation or engaged in hate-based groups or behaviours.

19. The Teaching Council or any other such similar accreditation body across preschool, primary, secondary and tertiary education should be provided with resources from the exchequer to assist in the provision of continuing professional development of educators within Higher Education Institutions.

20. Education for parents, educators and society in general about how to reach young people who have gone down the path of hate or extremism is needed.

21. Schools and curriculums need to adapt to challenges relating to technology in real time. The school curriculum should include modern media literacy to help equip young people with the tools to deal with content they encounter online that could negatively impact their mental health and to teach them how to avoid disinformation and develop critical thinking.

22. Overuse of, and addiction to, phones and social media among young people must be addressed.

23. Efforts to address bullying, in the context of current technology, should be stepped up.

24. Measures must be taken to address the criminal activity associated with recent technological developments, including that associated with AI, generative AI, extortion, identity fraud and sex abuse.

25. The legislation surrounding all of the issues identified in this report must now be revisited, analysed to establish any gaps, and then updated in line with current and emerging threats and technology. It is vitally important that this is done from a children's rights-based perspective, first and foremost.

26. As recommended by the UN Committee on the Rights of the Child, the root causes of suicide and self-harm need to be addressed, through psychological, educational and social measures and therapies for children and their families.

27. An amendment should be made to the Harassment, Harmful Communications and Related Offences Act, to clarify that deepfakes or AI-generated material are included in the prohibition on the recording, distribution or publishing of an intimate image of another person without consent.

28. Child centred design needs to be a guiding principle from the outset in AI involved products, platforms and services. Funding and incentives should be provided to support research on AI for and with children, as well as child-centred AI policies and strategies.

29. Another national youth assembly on AI should be held this year and its findings should be responded proactively to by all government Departments.

30. Further consultation with young people on these issues with established pathways for the integration of their perspectives into policy responses is essential.

31. UNICEF guidance and the United Nations Convention on the Rights of the Child should inform Irelands response to AI and child safeguarding.

32. The United Nations Convention on the Rights of the Child should be incorporated into domestic legislation.

33. While creating protections for young people online, adults should bear in mind that children have evolving capacities and needs for information and privacy.

34. The Ombudsman for Children's office and Coimisiún na Meán should continue to engage, with quarterly meetings and other opportunities for collaboration, to ensure children's rights are central to the Coimisiún's policies and are effectively being upheld by platforms.

35. The broader societal harms that have emerged online, such as a pattern of conduct which is dangerous to the public in general or a pattern of conduct which is dangerous to protected groups, such as women and girls, for example, or particular minorities, need to be addressed.

36. A whole-of-society approach is now needed to keep people safe and to ensure that AI and social media are forces for good. This will need to involve adults self-reflecting, making behavioural changes and setting boundaries.

1. The problem with AI

Two major issues became clear during the Committee's meetings on AI and child safeguarding. Firstly, companies do not have reliable age verification systems. Secondly, there is significant potential for harm inherent in recommender systems, which platforms use to push content onto users based on their assumed interests or browsing patterns, with the aim being to keep the user on the platform for longer.

Together, these two issues exacerbate several other potential harms to young people online, like addiction, criminal activity such as sexual exploitation or extortion and peer-on-peer abuse. The consequences of these harms for young people can be severe, and the ripple effect on families and society at large is profound. Age verification and recommender systems in particular must be addressed, so that technology, including AI, benefits rather than harms. This section gives a brief description of the situation regarding age verification and recommender systems and details some of the harms the Committee heard about. Porn has been identified as a contributor in many of these harms.

The submission made by the Irish Medical Organisation (IMO) touches on all of the harms identified in this section and references a body of evidence linking increasing phone and social media use with increasing rates of suicide, depression, mental health issues, loneliness, dissatisfaction with life, cyber-bullying, body image issues, eating disorders/disordered eating, addiction, and anxiety. The research referenced in that submission points towards adolescents spending somewhere in the region of two to five hours online daily.

Age verification

The digital age of consent in Ireland is 16 but young people are online and encountering content that is age-inappropriate much younger. CyberSafeKids informed the Committee that they have been tracking usage among children over the last six to seven years. Their data shows that currently, 84% of eight to 12-year-old children have online accounts, with the top five most popular platforms being YouTube, TikTok, Snapchat, Instagram and WhatsApp.

The Committee heard that companies do not currently have effective systems in place to verify someone's age, relying predominantly of self-declaration, whereby the user inputs their age when setting up an account. While it was acknowledged that privacy and security

concerns can arise from more rigorous systems of verification that may require identification to be provided, there was a sense of unease among Members and many stakeholders around the scale of the harms currently being caused by the lack of effective verification in place. Privacy and security concerns cannot be dismissed. None-the-less, the companies that reap such financial benefits from online spaces and have been instrumental in the design and operation of such spaces, can and should overcome these challenges and find an age verification method that protects people's privacy and security. The consequences of not doing so have already been too great.

Coimisiún na Meán informed the Committee that there are several initiatives underway at EU level to address the issue of age verification, such as a taskforce set up through DG Connect which includes the Data Protection Commission, an EU consent project and work ongoing to develop an age-appropriate design code. While these early steps are welcome, the Committee heard that there is a lack of consensus on the issue internationally. Many stakeholders the Committee heard from emphasized the importance of addressing the issues head on and urgently, rather than waiting for Europe to develop solutions.

When asked about timelines for when Coimisiún na Meán would like age verification to be implemented, it highlighted the complexity of the problem and said that it alone cannot provide the full solution. Under the current plan, individual companies will have discretion about what form their age verification measures take. However, the Coimisiún reassured Committee Members that the requirement for effective age verification is mandatory and that if it determines companies' mechanisms are not robust enough, it will require them to produce more stringent measures. This derives from Article 28b(3) of the audiovisual media services directive.

While the Committee appreciates the challenges involved in resolving age verification, and respects that other bodies and mechanisms will need to be involved, it appeals to the Coimisiún to lead this urgent reform now. Part of that work will entail making robust demands on platforms and companies and using its powers to set the agenda, enforce and penalise assertively. Government should encourage and back the regulator in relation to this. Coimisiún na Meán should use its special cooperation relationship with the European Commission under the Digital Services Act and the fact that so many of the large platforms have headquarters here in Ireland to spearhead action on age verification.

The Platforms that Committee met with shared some thoughts on age verification. Meta for example, suggested that the most efficient and effective way forward would be verifying at the operating system or app store level, although there are other alternatives. This would not remove responsibility from every app to have processes in place to manage age effectively, Meta said. X also put forward the position that verifying users' ages and soliciting parental consent for app downloads could play a pivotal role in addressing age verification. TikTok said it tries to identify underage users, removing on average 20 million suspected underage accounts every quarter globally, and pointed to the age settings applied to a device on its initial setting up and the need to input an age when creating an account as other mitigations.

In their submission, Google did not suggest a particular solution to age verification, but cautioned that:

1. More data-intrusive methods (such as verification with "hard identifiers" like government IDs) should be limited to high-risk services (e.g., alcohol, gambling, or pornography) or age correction.

2. Flexibility is initially needed to allow platforms to trial and adapt age verification technologies being developed in good faith.

Vulnerable groups

Vulnerable groups include, for example, children, elderly people, people with disabilities and mental health challenges, women and girls, ethnic and racial minorities, LGBTQ+ people, and refugees. Throughout the Committee's discussions, reference was made to various vulnerable groups potentially being more exposed to the effects of AI, including recommender systems, and harms online generally. As the following sections explore, this feeds into increased experiences of peer-on-peer abuse, scams and many other online harms.

The new online world poses challenges to long fought for rights and protections for vulnerable groups, and these rights and protections are routinely ignored or attacked online. Given the tendency platforms appear to have to amplify hate and extremism, Members raised concerns about vulnerable groups, social media and AI. The potential impact in terms of rolling back on equality is immeasurable and already being felt, with

teachers, for example, now reaching out to external organisations and academics for help to get students back to respecting things like gender, race and orientation.[4]

The Coimisiún told the Committee that from its consultation and submissions processes it is aware that many individuals and organisations are rightly concerned about online harms for vulnerable people, stating:

> "We are aware that, at a minimum, with AI tools and recommender systems it is not only children and vulnerable adults who may be more at risk but also individuals who have protected characteristics. Some people, by virtue of having, for example, a disability, a particular ethnicity, nationality or immigration status or being LGBTQI+, women and so on, may be more at risk. It is less about the technology itself but about its uses, its impact and how it is applied."[5]

As well as taking measures to protect young people generally, companies, regulators and Government should develop specific protective mechanisms and safety by design for the protection of other vulnerable and protected groups. The State must act to ensure that technological advances do not come at the expense of hard-won rights and equality. Ms Caoilfhionn Gallagher, Special Rapporteur on Child Protection, emphasized the importance of addressing the issues around vulnerable groups, inclusion and non-discrimination when she came before the Committee. She said the UNICEF issued policy guidance on AI for children is instructive in this regard.

Recommender systems

Although a wide range of potential harms to young people were discussed during the hearings, discussions focused most on the pushing of content onto young people through recommender systems. The ICCL described what a recommender system is and does to the Committee as follows:

> "The AI of these corporations builds a tailored diet of content and pushes it into each child's feed... They are pushing it into the feeds and that system is known, loosely, as a recommender system. A recommender system builds a feed based on each person's estimated likelihood of engaging with material. Often that requires salacious or outrageous content or things that play upon the individual's sensitivities

---

[4] [Normies, incels and red-pilled: What are the dangerous ideas boys are being fed online? – The Irish Times](#)
[5] Karen McAuley, Coimisiún na Meán, 20 February 2024.

and vulnerabilities. That is very bad news for society, but it is excellent news for the tech companies because it keeps the person on the platform for longer, which massively increases advertising opportunities. This is how the companies make money today… In the case of Meta, YouTube, Instagram, X and TikTok, their AI recommender systems are manipulating and addicting our kids. They are promoting childhood hurt, hate, self-loathing and suicide."[6]

The recommender system selects content to push on someone using past datasets or behavior. The less serious (yet important) risks this can entail includes the potential to limit the young person's views, create missed opportunities, reinforce stereotypes and create negative self-perceptions.

More concerning risks emerge from the pushing of more harmful content onto young people which can lead to seriously concerning views and behaviors. This could for example include the pushing of content related to white supremacy or racism onto young people who have shown an interest in gaming or military history, or the pushing of content related to self-harm or suicide to those that had consumed content about diet and fitness.

Some recent studies or examples that have tested or illustrated the tendency for such systems to do this were discussed before the Committee, including:

- The DCU Anti-Bullying Centre and Debbie Ging, Professor of Digital Media and Gender, recently conducted an experimental study that tracked content recommended to 10 experimental or "sockpuppet" accounts on 10 blank smartphones, by YouTube Shorts and TikTok. It found that all of the male-identified accounts were fed large volumes of masculinist, antifeminist and other extremist content, irrespective of whether they sought it out, within, at most, the first 2-23 minutes of the experiment.

- A study by the Center for Countering Digital Hate (CCDH) on TikTok's recommendation algorithm which found that the platform pushed and promoted self-harm and eating disorder content, tummy tuck surgery and content romanticising suicide to teenagers within minutes, even if they were registered as under 18. The study was based on accounts registered as age 13 in the US, UK, Canada and Australia.

---

[6] Dr Johnny Ryan, ICCL, 13 February 2024.

- An [investigation](#) by the Anti-Defamation League showed that Facebook, Instagram, and X late last year were pushing hate and conspiracy content into the feeds of 14-year-old test users.

- [Investigations](#) by the Institute for Strategic Dialogue found that young boys were having extremely hateful misogynistic content routinely pushed at them through YouTube's new video shorts feature.

- A [study](#) by Amnesty International on how TikTok's 'for you' feed encourages self-harm and suicidal ideation.

- [Findings](#) that Snapchat added its "My AI" feature to every subscriber's account in 2023 when it was still in testing, resulting in inappropriate information being given to children. 37% of eight to 12-year-olds in Ireland have Snapchat accounts. Nine months later, Snapchat added a parental control to restrict the use of My AI.

- A Prime Time [special programme](#) on artificial intelligence aired on RTE in 2024. Before it aired, researchers undertook experiments on accounts registered as being 13-year-olds and found they quickly encountered content relating to self-harm and suicidal ideation. On foot of the programme, TikTok undertook a review of the harmful content but reportedly refused to disclose how many videos were removed as a result.[7]

- In a January 2024 [submission](#) to Coimisiún na Meán on its draft Online Safety Code, over sixty civil society organisations, including for example; LGBT Ireland, Community Work Ireland, NASC, ILMI, Outhouse, The National Women's Council, Age Action and Women for Election, urged it to require that recommender systems are off by default. The submission cited widespread international consensus on the issue.

Companies would dispute the findings and faults identified in these studies and discussed by those who came before the Committee, framing the pushing of such content as more of an unfortunate side effect of the current online landscape than something they actively encourage or benefit from. Meta, for example, stated:

> "It is sometimes claimed that Meta is financially motivated to promote harmful or hateful content on our platforms to increase engagement. This is simply untrue. This

---

[7] [TikTok completes review into harmful content following RTÉ story (rte.ie)](#)

content violates our policies and prevents our users from having enjoyable experiences. As a company, the vast majority of our revenue comes from advertising. Our advertisers do not want to see such content next to their ads. It is clear therefore that we are financially motivated to remove content which violates our policies as quickly as possible once we become aware of it."[8]

The overriding question discussed in relation to recommender systems was, what Coimisiún na Meán is going to do about them. Unlike age verification, recommender systems and the amplification of harmful content are not included in Article 28b(3) of the Audiovisual Media Services Code. Therefore, the Coimisiún said that it is proposing to include something on recommender systems as a supplementary measure, separate to its first online safety code, which will require further engagement with the European Commission through a process called the TRIS directives. The Coimisiún is in contact with the European Commission about these issues and the European Commission has opened an investigation into TikTok in relation to its recommender systems. Several experts who came before the Committee said that establishing a requirement for recommender systems to be off by default is something the Coimisiún can and should be doing and cautioned that taking a 'waiting-for-Europe' approach would be unwise.

Members raised concerns about whether the Coimisiún's powers are strong enough and whether the regulator is willing to use them effectively and intervene to make the online world safer for young people, in general, but especially in relation to recommender systems. On this, Coimisiún na Meán provided some reassurance, citing ample tools and serious intentions of using them. Some examples include the Digital Services Act, through which fines of up to 6% of worldwide turnover can be imposed, and the Terrorism Content Online Regulation, which is underpinned by sanctions of up to 4% of relevant online turnover. In the case of breaches of its online safety code, it:

"Can impose fines of up to 10% of relevant turnover or €20 million, whichever is the greater. Indeed, there can even be criminal sanctions for some of the more egregious breaches of non-compliance with the Act. It is important to say that self-regulation is over and we are now into an era of effective regulation."[9]

---

[8] Mr Dualta Ó Broin, Meta, 16 April 2024.
[9] Ms Niamh Hodnett, Coimisiún na Meán, 20 February 2024.

However, when asked what existing law is in place to curtail harm from recommender systems, the Coimisiún said:

> "It is already a binding obligation for the large platforms, for example, to deal with the mitigation of harmful content as part of their need to do a risk assessment of their platforms and to introduce mitigation measures. These are binding obligations already imposed on the very large online platforms under Articles 34 and 35 of the Digital Services Act. In addition, Article 28 places an obligation on all platforms to address the safety of minors."[10]

When pressed about whether it is possible to police recommender systems and regulate for them to be off as default for young people, the Coimisiún was less clear, stating:

> "In our draft online safety code we have proposed as a supplemental measure that the platforms would carry out a risk or safety impact assessment specifically in respect of recommender systems. Some of the measures on which the platforms will report to us will include whether they should default to off or on."[11]

So, the Coimisiún did not indicate that it, as a regulator would be prescribing an off by default rule for recommender systems. Instead, it is talking to Europe and asking platforms to decide on the matter themselves. This jars with what many witnesses said should be done. From discussions the Committee had with other experts in the field, and with young people themselves, it is clear that the 'already binding obligations' and codes platforms have to curb harms are not being adequately adhered to. In this context, allowing platforms themselves to report to Coimisiún na Meán on whether recommender systems should be on or off for young people seems naïve.

Some stakeholders have expressed strong disappointment at the steps taken by Coimisiún na Meán so far, saying it did a U-turn by omitting previously proposed requirements for social media companies to turn off recommender systems. Overall, the Committee is uncomfortable with the familiar approach of asking platforms to self-regulate, as in, describe the risks and solutions as they see it, while waiting for action at EU level. It is also mindful that, to date, platforms have failed to adequately meet their existing obligations.

---

[10] Ms Niamh Hodnett, Coimisiún na Meán, 20 February 2024.
[11] As above.

The harms being experienced outweigh any gains that could be made by going easy on platforms or waiting for European-wide measures.

The Committee recommends that recommender systems are legally required to be turned off by default for young people under the digital age of consent, that is, those under 16 and that Coimisiún na Meán establishes this as a legal requirement for platforms. If the Coimisiún lacks the powers to do so, then this should be rectified as a matter of urgency. If there is an issue of legislative unclarity in the Digital Services Act or elsewhere preventing the Coimisiún from taking this measure, then the legislation should be amended. Ireland could lead on this issue now, in addition to participating in EU-wide measure being developed for implementation down the line.

Addiction

Frances Haugen, is an ex-Facebook employee turned whistleblower who was referenced during the Committee's deliberations. She has said Instagram's algorithms can lead to addiction in its young users by creating dopamine loops whereby children get caught in the crosshairs of the algorithm and sent down rabbit holes, engaging with frightening or enraging content because, as Haugen conveyed, it's easier to inspire people to anger than it is to other emotions.

CyberSafeKids echoed her fears about addiction and shared Members' concerns that some young people are more vulnerable than others, such as those with additional needs, stating:

> "There is some evidence that children with, for example, attention deficit hyperactivity disorder, ADHD, are more likely to become addicted. The challenge is the way the algorithm works is that it is designed to be addictive for all users. Children are more vulnerable, perhaps, because they do not have such high awareness about the techniques that are being used to hold their attention, keep eyes on screen, and so on. There are greater vulnerabilities within that wider cohort... I believe that children with ADHD are more vulnerable."[12]

Overuse of, and addiction to, phones and social media among young people must be addressed. Measures to address the emerging risks and challenges stemming from AI and

---

[12] Ms. Alex Cooney, CyberSafeKids, 13 February 2024.

similar technology should take account of the distinct needs and vulnerabilities of people with disabilities or who are neurodivergent.

Fake News and the proliferation of hate

Coimisiún na Meán also told the Committee that, as the national digital services coordinator, it can award the status of a trusted flagger to a third-party entity and has published an application form and guidance for organisations that may wish to apply. The idea is that, because of their expertise or competence, trusted flaggers have a priority pathway to notify platforms about inappropriate content so that the platforms can take action. However, other organisations have previously informed the Committee that despite their trusted flagger status, platforms have failed to respond to their reports appropriately. Again here, we see the platforms potentially not abiding by or acting on the measures supposedly in place to reduce online harm. The Committee recommends that the enforcement of existing measures to prevent online harms is strengthened, including those involving trusted flaggers.

The tendency for AI and social media generally to proliferate untruths, disinformation and content that can influence people to harm, hate or anger was discussed. The online world, in its current form, can enable popular, but fringe, extremist views to take hold among some groups of young people, such as misogyny or racism. By utilising the reach and freedoms platforms provide, the far right and various hate-based groups have sought to portray themselves as trustworthy anti-establishment sources online. Increasingly we are seeing op-eds, agony aunt columns, podcasts and social media posts from parents desperately looking for advice on how to deal with their children having gone down rabbit holes of hate "incel" ideology[13] and misinformation.[14][15]

Teachers have reported the 'Tate effect' whereby boys are consuming content from the social influencer and mimicking him. Recent coverage of the issue revealed that almost all boys in the UK had heard of Tate, and about half had a positive view of him, despite the

---

[13] Incel ideology blames women/society for men's lack of romantic success and is a part of the online misogynist "manosphere", with incel being a short term for involuntary celibates/ involuntary celibate.

[14] [More than half of parents feel unable to keep child safe online, survey finds (irishexaminer.com)](#)

[15] [Teachers and Parents Talk About Andrew Tate's Influence on Kids - Business Insider](#) , [How to stop my child from using harmful content on the internet during online classes in 2020 - Quora](#) , [What's the right age for my daughter to get a smartphone? I asked her older siblings – The Irish Times](#)

toxicity of his content, or the fact that he has been arrested on suspicion of human trafficking, rape and forming an organised crime group. Some schools have been praised for their reaction, where they have tackled these issues head on by having discussions about toxic masculinity and providing workshops on positive male role models, critical thinking and healthy relationships.

In 2023, Women's Aid, one of Ireland's main organisations offering domestic abuse support, received its highest ever number of domestic abuse disclosures in its 50-year history.[16] In Northern Ireland, one judge explicitly linked the recent rise in domestic violence with the rise of social media influencers like Andrew Tate, stating:

> "There needs to be a coordinated, planned change to the school curriculum whereby the school curriculum is to focus on the whole question of domestic violence, abuse, the wider question of respect for each other as human beings.... If that's successful that will lead to less offending."[17]

In this context, it is important to seriously consider how increased online harms are feeding into increased real-life gender-based violence, and how the effects of technological 'progress' can result in serious regressions in terms of equality. As well as the clear harms to women, this kind of extreme misogyny harms men as well. Equipping people with the tools to think critically and progressively in this context is arguably more important than ever.

The Committee's report on CAMHS and Dual Diagnosis flagged recent technological change as contributing to the mental health challenges facing young people today and recommended youth work and a school curriculum that reflects this and which prevents children from being vulnerable to harmful content. Furthermore, education for parents, educators and society in general about how to reach young people who have gone down the path of hate or extremism is needed. The Committee has previously recommended digital media literacy training for pupils, teachers and others, and it reiterates that recommendation. The Committee was very concerned at early reports that the proposed new school curriculum does not include modern media literacy and recommends that this is

---

[16] ['Alarming increase' in physical and economic domestic abuse, says report – The Irish Times](#)

[17] [The Andrew Tate Effect. Who is Shaping the Values for School Boys? (legal-island.com)](#)

rectified. If schools fail to tackle these issues head on, they will face more serious problems down the line by leaving students exposed and unaided in the face of these challenges.

The UN Committee on the Rights of the Child previously called on Ireland to address the root causes of suicide and self-harm through psychological, educational and social measures and therapies for children and their families.[18] The Committee emphatically supports that call and, based on the testimony it heard, sees the current online landscape as a big driver of mental health issues among our young people today. Platforms need to be enforced to flag and remove harmful, hateful and disingenuous content. This illustrates the problem of value misalignment, whereby the principles, standards and aims on one group (in this case platforms seeking profit) misalign with another group (in this case society seeking to curb online harms). This misalignment is discussed further in sections three and five, which deal with 'Designing with and for Children' and 'Education, Morality and the Wider Picture'.

Bullying, criminality, image-sharing and deepfakes

The Committee heard that while bullying has always been a challenge, peer-on-peer ill treatment generally seems to be exasperated by the proliferation of sinister content online, the pervasive use of phones and social media. Before this 'always on' era, a child was able to escape their abusers to an extent, once they went home and closed the door behind them. Now, there is often no such escape, given that most young people are instantly contactable on a range of platforms, all the time. The situation worsens when we consider that those same platforms have a habit of serving harmful content to young people, especially those who indicate they are struggling.

The Committee was informed that Children at Risk in Ireland (CARI) has highlighted that peer-on-peer abuse using AI is increasing significantly and that the courts in Ireland have reported underage access to online pornography as being a major contributing factor in serious crimes. Furthermore, Interpol and the Garda National Protective Services Bureau have previously highlighted that sexualized self-taken photos of Irish children are being shared further afield and commercially exploited worldwide.[19] This underlines the

---

[18] FINALMHRCMHCSubmissionUNCRC.pdf (mentalhealthreform.re or situation into soemehtogn ie)

[19] Sexualised self-taken photos of children and teens being commercially exploited online - gardaí – The Irish Times

importance of education around the risks entailed in sharing photos, whether sexual or non-sexual and whether taken by friends, partners or parents.

In addition to the risks posed by bullying or the creation or sharing of compromising content by peers, AI and social media have created opportunities for bad actors to threaten and extort. This often involves someone thinking they are talking to a real-life person who then asks for sexual images and goes on to attempt extortion. One such case put to the Committee was that of a teenage boy who was persuaded to share intimate images and immediately told that if he did not pay several thousand euro, they would be shared in a private Instagram group of his peers and younger siblings. The Committee heard that has led to tragic outcomes for some families. In a similar vein, apps now widely exist that use AI to make someone appear naked, removing the need to get the person in the compromising position in real life at all.

By creating the ability to turn an innocent picture or sample of someone's voice into a seemingly real but actually fake portrayal of them, known as a deepfake, AI has now hugely increased the potential for harm in this space. Regardless of whether this is carried out by peers, by someone looking to interfere in someone's life or by sexual predators looking to create child porn material, the consequences can be devastating.

Institutions such as the UK's Internet Watch Foundation have warned that they are also seeing a proliferation of AI-generated child sexual abuse material.[20] These are real children who have appeared in confirmed sexual abuse imagery, whose faces and bodies have been built into AI models designed to reproduce new imagery of these children.

As previously mentioned, a Prime Time special programme on artificial intelligence aired on RTE on 16 April 2023.[21] One of the concerns it discussed was that by 2030 many of today's children will have had their identities used in identity fraud due to information that has been shared by their parents through seemingly innocuous content they post online. The importance of 'informed scepticism' in terms of what we post and encounter online was raised in this context. It is likely that parents and many young people are unaware of the extent of risk involved in everyday social media activity. For example, even if someone's profile is set to private, their profile photo can be viewed. AI technology that is now

---

[20] How AI is being abused to create child sexual abuse material (CSAM) online (iwf.org.uk)

[21] Game Changer: AI & You - RTÉ Player (rte.ie)

available widely and free can tell from one profile picture where it was taken, what the area is like what the GPS coordinates are and more. This information is at the fingertips of potentially anyone who may want to find someone, for whatever reason.

More generally, deepfake technology appears to be seriously affecting women. Several studies of deepfakes have shown that the vast majority generated are non-consensual and sexual, and almost all are of women. CyberSafeKids cited a report by Sensity AI which found that 96% of deepfakes were non-consensual sexual deepfakes. Of those, 99% were of women. Again here, we see the advances in technology, in this case AI, coming at an unacceptable cost and eroding hard won gains previously made in relation to equality, child protection and consent.

Witnesses told the Committee that there are some legislative tools in relation to deepfakes, citing GDPR, the forthcoming AI Act and the EU Digital Services Act. However, the Committee heard that these are limited by a lack of enforcement and by only dealing with labelling and reporting, rather than the generation of deepfakes. ICCL are of the view that, harnessed correctly, GDPR Article 9 on 'specially protected data' and the office of the Data Protection Commissioner, and Coimisiún na Meán, through their powers to act on social media video platforms, could address these issues. Enforcement is what is lacking, according to ICCL, who stated:

> "We have got two players: the DPC and Coimisiún na Meán. We have tools to solve these problems."[22]

An amendment should be made to the Harassment, Harmful Communications and Related Offences Act, to clarify that deepfakes or AI-generated material are included in the prohibition on the recording, distribution or publishing of an intimate image of another person without consent.

The International Context

Some witnesses cited companies' ability to adjust their service or product across jurisdictions and to correspond to different regulatory requirements geographically, as evidence that their operations can be adjusted and should be, to prevent harm, especially to young people. Steps to protect children from online harms can and do happen where there

---

[22] Dr. Johnny Ryan, ICCL, 13 February 2024.

is political will. This must happen domestically, particularly given that Ireland has the highest rate of daily internet use by young people in the EU, coming in at 100%.[23]

France was noted as having recently made efforts to legally enforce age verification and parental consent for those under 15 years of age.[24] A recent study commissioned by French president Emanual Macron recommended that children should not be allowed to use smartphones until they are 13 and should be banned from accessing conventional social media such as TikTok, Instagram and Snapchat until they are 18.[25]

The University of Bristol recently reported on the success of a series of measures taken by China to curb sedentary behavior among children. The measures were unusual in that they introduced regulatory interventions across multiple settings, such as the education sector by limiting homework, and the gaming industry by introducing restrictions.[26] CyberSafeKids informed the Committee that legislation is in place in Australia, that puts some onus or responsibility on the individuals who post harmful content.

In the US, Individual States have banned particular apps.[27] The Surgeon General's Advisory on [Social Media and Youth Mental Health](#) from 2023 makes recommendations for young people, parents, companies, policymakers and researchers on the best way forward for tackling what he has recently called "the defining public health challenge of our time."[28] He has also recently called for health warning labels on social media, as has been successfully implemented on cigarette packaging.[29] The ICCL praised elements of the US approach in dealing with amplification, stating:

> "The international best practice we should be thinking about is the change we have had in the last three-to-four years at the US Department of Justice and in the USFTC. If we had a similar change here, a real culture of enforcement, of dedicated investigation and of people who are willing to actually do the work of taking a scalp, we would be best practice because we have the law."[30]

---

[23] [96% of young people in the EU uses the internet daily - Eurostat (europa.eu)](#)
[24] [France: New parental consent law to regulate children's social media use | Irish Legal News](#)
[25] [Stop children using smartphones until they are 13, says French report | France | The Guardian](#)
[26] [China's restrictive approach to children's screen time and homework showing promising benefits | Euronews](#)
[27] [France Senate passes legislation requiring age verification for minors on social media - JURIST - News](#)
[28] [Social media and youth mental health defining challenge of our time: Surgeon general (yahoo.com)](#)
[29] [US surgeon general wants social media warning labels (bbc.com)](#)
[30] Dr. Johnny Ryan, ICCL, 13 February 2024.

Internationally, a number of countries, such as Germany, Australia and the UK are moving towards penalizing the actual generation of deepfakes, as opposed to just looking at their labelling or sharing. The Committee recommends that Ireland does the same. In the meantime, the existing powers of the Data Protection Commission and Coimisiún na Meán should be used to tackle deepfakes.

It should also be noted that a Motion on a Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child sexual abuse material was recently debated and agreed by the Dáil and Seanad. This Directive will update the definition of the crime child sexual abuse material in deepfakes or AI-generated material. The EU text reads:

> "In light of recent technological developments and, in particular, of the development of augmented, extended and virtual reality settings, the criminalisation of the solicitation of children should not be limited to voice, text or mail conversations, but also include contacts or exchanges in augmented, extended or virtual reality settings, as well as largescale solicitation of children through the use of chat-bots trained for that purpose, as this phenomenon is itself expected to increase in light of the foreseeable evolution of artificial intelligence applications. Therefore "by means of information and communication technology" should be understood in a sufficiently broad way to cover all those technological developments."[31]

The legislation surrounding all of the issues identified in this report must now be revisited, analysed to establish any gaps, and then updated in line with current and emerging threats and technology. As the witnesses who came before the Committee underlined, it is vitally important that this is done from a children's rights-based perspective, first and foremost. Witnesses also stressed that Ireland should be leading the charge in this, given that we are regarded as one of Europe's leading tech hubs. Our legislation needs to match this status. The Committee is not concerned with what lever is pulled to address the harms identified in this report, be that increased enforcement of existing legislation or the creation of new law or a combination of both.

---

[31] resource.html (europa.eu)

Recommendations

1. Research should be conducted by the Department and relevant organisations to investigate the impact of AI systems for children with additional needs and particular vulnerabilities within that cohort.

2. In line with guideline F of UNICEFs Policy Guidance on AI for Children, measures must be taken to ensure transparency, explainability, and accountability are provided for children. The Online Safety and Media Regulation Act should be reviewed to determine whether adequate mechanisms are in place for those seeking redress for harm caused in the digital space.

3. Companies should have rigorous and effective age verification techniques in place. These should not impinge on privacy and security for users. Self-declaration, whereby the user inputs their age when setting up an account, should not be permitted as an appropriate age verification system.

4. Coimisiún na Meán, should publish specific deadlines, no later than year-end 2024, for when it requires companies to have in place and demonstrate effective measures for age verification and for recommender systems to be off by default for those under 16.

5. Recommender systems should be off by default for young people under the age of 16. Coimisiún na Meán should establish this as a legal requirement that is binding for all platforms. If Coimisiún na Meán lacks the powers to do so, then this should be rectified as a matter of urgency.

6. Government and Coimisiún na Meán need to tackle the issues discussed in this report head on and urgently, rather than waiting for solutions from Europe, platforms themselves or elsewhere.

7. Coimisiún na Meán should lead this urgent reform now by making robust demands on platforms and companies, using its powers to set the agenda, enforce and penalise assertively where needed.

8. Government should support, encourage and back Coimisiún na Meán, using its expertise to inform policies and increasing its powers when necessary.

9. Coimisiún na Meán should use its special cooperation relationship with the European Commission under the Digital Services Act. The presence of so many large platforms with headquarters in Ireland should ensure action on age verification, recommender systems, misinformation and other online harms.

10. As well as taking measures to protect young people generally, companies, regulators and Government should develop specific protective mechanisms and safety by design for the protection of other vulnerable and protected groups.

11. The State must act to ensure that technological advances do not come at the expense of hard-won rights and equality.

12. Social media companies should be made to abide by their agreed community standards. They should amend their algorithms so that they are prevented from enabling and profiting from fake news and harmful content.

13. Platforms should prevent the propagation of disinformation and the platforming of racist or misogynistic or otherwise dangerous content that seek to undermine legally held and agreed upon human rights and entitlements.

14. The responsibility of platforms to flag and remove inaccurate, dangerous or extreme content must be acted on, enforced and applied rigorously, with penalties for failing to do so applied.

15. Guidance and educational resources for adults and children in relation to AI, social media and recent tech developments are much needed. Relevant Departments and organisations should produce and promote accessible, age-appropriate resources as a priority.

16. The enforcement of existing measures to prevent online harms should be strengthened, including those involving trusted flaggers.

17. Communities need to be given the tools and education to think critically and decipher disinformation. This should be done through schools, education and training boards, youth clubs and any appropriate body, be they statute bound, voluntary or by tender to include private entities.

18. Educators themselves need to be kept abreast of the best ways to prevent young people from becoming vulnerable to disinformation or engaged in hate-based groups or behaviours.

19. The Teaching Council or any other such similar accreditation body across preschool, primary, secondary and tertiary education should be provided with resources from the exchequer to assist in the provision of continuing professional development of educators within Higher Education Institutions.

20. Education for parents, educators and society in general about how to reach young people who have gone down the path of hate or extremism is needed.

21. Schools and curriculums need to adapt to challenges relating to technology in real time. The school curriculum should include modern media literacy to help equip young people with the tools to deal with content they encounter online that could negatively impact their mental health and to teach them how to avoid disinformation and develop critical thinking.

22. Overuse of, and addiction to, phones and social media among young people must be addressed.

23. Efforts to address bullying, in the context of current technology, should be stepped up.

24. Measures must be taken to address the criminal activity associated with recent technological developments, including that associated with AI, generative AI, extortion, identity fraud and sex abuse.

25. The legislation surrounding all of the issues identified in this report must now be revisited, analysed to establish any gaps, and then updated in line with current and emerging threats and technology. It is vitally important that this is done from a children's rights-based perspective, first and foremost.

26. As recommended by the UN Committee on the Rights of the Child, the root causes of suicide and self-harm need to be addressed, through psychological, educational and social measures and therapies for children and their families.

27. An amendment should be made to the Harassment, Harmful Communications and Related Offences Act, to clarify that deepfakes or AI-generated material are included in the prohibition on the recording, distribution or publishing of an intimate image of another person without consent.

2. Action underway to address child safeguarding and AI

Stakeholders were divided on whether the tools needed to address the issues discussed in this report are readily available. Some witnesses cited the fact that young people are actively encountering harms online everyday as evidence that the tools aren't working and said that none of young people's digital rights ([referenced in UNCRC general comment No. 25](#)) are being upheld in the current online environment. Others said we have the tools to make sure they are, but that will, and enforcement is the problem. This section focuses on some of the measures that Coimisiún na Meán and the companies who came before the Committee said they are taking to counteract some of the harms discussed in this report.

Coimisiún na Meán

Coimisiún na Meán, established in 2023, is a relatively new regulator for broadcasters and online media. Its remit includes regulating online platforms based in Ireland and carrying out the previous functions of the Broadcasting Authority of Ireland. The European Commission also plays a role in relation to the largest platforms.

The Coimisiún was quite emphatic in telling the Committee that "the era of self-regulation is definitely over." Some of the measures it told the Committee it is taking in relation to AI, child safeguarding and online safety in general include:

- The establishment of, and ongoing consultation with, a youth advisory committee.

- Supporting Safer Internet Day which focused on young people's views on technology and the changes they want to see.

- Providing information on its website about online safety and how to make complaints to platforms and seek support in relation to harmful content.

- The establishment of a contact centre and a forthcoming individual complaints scheme.

- Putting in place the online safety framework in Ireland, which makes platforms accountable for how they protect users, especially children and is composed of three elements:

1. The Online Safety and Media Regulation Act which is the basis for Coimisiún na Meán's draft online safety code.

2. The EU Digital Services Act, which became fully applicable on 17 February 2024.

3. The EU Terrorist Content Online Regulation (Coimisiún na Meán has been a competent authority on that, together with An Garda Síochána).

- Establishing a draft online safety code which proposes measures such as:

1. Age verification and parental controls requirements.

2. Safety by design is being promoted through its guidance and supplementary measures.

3. Recommender system safety.

4. Supporting 'trusted flaggers.'

Companies that came before the Committee

On 16 April 2024, the Committee heard from X (formerly Twitter), TikTok and Meta (Meta operates Facebook, Instagram, Threads, and WhatsApp, among other products). Google was invited to participate but Google representatives were not in a position to attend, so a written submission was received instead. Google's [submission](#) is available here. Page three may be of interest to parents as it contains information and links related to safety features, including those for YouTube.

Some of the measures these companies told the Committee they are taking in relation to AI, child safeguarding and online safety in general are detailed below.

X (formerly Twitter)

- Those registered as young users have high privacy, safety and security settings in place on their accounts by default, so they don't see sensitive media and their direct messages are closed and location is turned off.

- X is a member of several child protection initiatives, such as the Tech Coalition, WeProtect, the Internet Watch Foundation and the Children Online Protection Lab.

- Content, including that generated by AI, is subject to X rules and X enforces policies irrespective of the source.

- X remains committed to the fulfilment of the Digital Services Act compliance obligation and intends to fully comply with relevant legislation in relation to AI.

- X removes any material that features or promotes child sexual exploitation and continues to invest in human and automated protection and content moderation.

- X's synthetic and manipulated media policy prohibits users from sharing synthetic, manipulated or out-of-context media that may deceive or confuse people and lead to harm.

- Community Notes functionality enables contributors to write notes on media and the note will be shown automatically on other posts with matching media. This community-led approach has significantly increased the scale and speed by which potentially misleading media is detected and labelled on the platform. In the month leading up to the meeting, there had been 130 million note impressions on community notes in the EU region.

- People having the option on X to select "for you" or "following" mode which gives them choice in terms of recommender systems and these are designed to exclude harmful and violating content.

- X published its algorithm and is open to feedback.

- Not interested, Mute, Block and filter options help people curate their own experience.

TikTok

- TikTok has a transparency centre, 40,000 trust and safety professionals and an expected €2 billion assigned to trust and safety efforts for this year.

- Content undergoes moderation and product design, along with evolving AI processes, help threats and violative content to be spotted and stopped.

- As videos rise in popularity, they are more likely to be checked for inappropriate content by the safety team.
- TikTok has robust community guidelines in place governing the use of AI-generated content and has a labelling tool for creators to support transparent and responsible content creation.
- The automatic labelling of AI-generated content is currently in testing.
- TikTok has launched a Global Youth Council to strengthen safety by design for teens.
- TikTok provides transparent access to its research Application Programming Interface in Europe and recently announced a STEM feed - a space dedicated to enriching videos related to science, technology, engineering, and mathematics.

Meta (Facebook and Instagram)

- Clear community standards and guidelines show what is and is not allowed on the platforms and Meta regularly consults with experts, advocates and communities around the world to update them.
- Meta is developing sophisticated technology to detect and prevent abuse from happening in the first place; and providing tools and resources for people to control their experience or get help. AI is used for reducing the volume of harmful content and is extremely effective at identifying fake accounts.
- An online and publicly accessible transparency centre contains quarterly reports on addressing harmful content on platforms.
- Over 30 tools and 20 AI system cards have been built/published to increase transparency and help parents and teens. Information on these can be found on the Instagram Parent Guide and Family Centre and the Education Hub for Parents and Guardians.

3. Designing with and for children

Witnesses emphasised the importance of designing and developing tech with and for children. Child centred design needs to be a guiding principle from the outset, the Committee heard, not an add on or afterthought. The UNICEF guidance was discussed as a good starting point for embedding children's rights in AI, but many difficulties persist in making the principles a reality, particularly principle six and nine. Principle six refers to providing transparency, explainability and accountability for children. Some witnesses said

the Online Safety and Media Regulation Act is not sufficient in terms of meeting principle six. On this, Professor Barry O'Sullivan told the Committee:

> "Transparency, explainability and accountability are really about understanding where the content is coming from, why the person is getting it, what data was used and so on. These are not easy problems to solve but they should be solved."[32]

Professor O'Sullivan also told the Committee about his experience participating the [national youth assembly on AI](#) in October 2022, which was hosted by the Departments of Children, Equality, Disability, Integration and Youth, and Enterprise, Trade and Employment in partnership with the National Participation Office and which brought together a diverse group of 41 young people from across the country aged between 12 and 24 years. The Committee recommends another national youth assembly on AI is held this year and that its findings are responded proactively to by all government Departments. Further consultation with young people on these issues with established pathways for the integration of their perspectives into policy responses is essential.

Ms Gallagher, the Special Rapporteur on Child Protection, cited a good case study that showcased principle six's call for age appropriate language to describe AI to children, whereby an AI-powered chatbot, codesigned with children, uses natural language processing to help adolescents and teenagers in Finland open up to learn about mental health issues (page 49 UNICEF guidance doc).

On principle nine of the UNICEF guidance, which deals with creating an enabling environment, the Committee heard that although Ireland has the potential to be a world leader, currently not enough is being done to make that a reality. The four elements of principle nine that countries should strive to meet include:

- Supporting infrastructure development to address the digital divide aiming for equitable sharing of the benefits of AI.
- Provide funding and incentives for child-centered AI policies and strategies.
- Supporting research on AI for and with children across the systems life cycle, including in the design phase.
- Engaging in digital co-operation across border and learning lessons.

---

[32] Professor Barry O'Sullivan, 13 February 2024.

Ireland can and should be making these four elements a reality.

As highlighted by CyberSafeKids, in 2021, the UN Convention on the Rights of the Child formally adopted general comment No. 25. which recognized children's rights in a digital environment to be the same as their rights offline, including the right to participate, the right to access accurate information, the right not to be exploited and the right to be protected from harm. The Committee reiterates its longstanding recommendation that the UNCRC should be incorporated into domestic legislation.

During the Committee's deliberations, the need to not underestimate children was highlighted, as well as the need to respect their evolving and legitimate needs for information and privacy to facilitate their growth and development. Tiered access was recognised as important in this regard, whereby a young person's access to tech changes as they mature and evolve. On this, Ms Caoilfhionn Gallagher, Special Rapporteur on Child Protection, said:

> "In respect of privacy, the general comment makes the point that one of the rights protected in the UNCRC is the principle of evolving capacities and the idea that as a child grows older, he or she develops in a different way. They are not mini adults. A child who is eight is very different to a child who is 15, of course. Children also have a right of access to information and freedom of expression. It is a nuanced area."[33]

The Ombudsman for Children, Mr Niall Muldoon, met with the Committee on 2 July 2024 to discuss his annual report. He informed the Committee that his office has engaged with Coimisiún na Meán and provided advice in relation to their Youth Advisory Panel and the intention is to hold quarterly meetings between the two bodies. The biggest message coming from children at this point in relation to AI, he said, is the need for guidance and education resources for adults and children. The Committee sees the need for such resources as vital at this point and urges relevant Departments and organisations to produce and promote such resources quickly. The collaboration between these two offices also offers an important opportunity to centre children's right in Coimisiún na Meán's policies.

---

[33] Ms Caoilfhionn Gallagher, 13 February 2024.

Recommendations

28. Child centred design needs to be a guiding principle from the outset in AI involved products, platforms and services. Funding and incentives should be provided to support research on AI for and with children, as well as child-centred AI policies and strategies.

29. Another national youth assembly on AI should be held this year and its findings should be responded proactively to by all Departments.

30. Further consultation with young people on these issues with established pathways for the integration of their perspectives into policy responses is essential.

31. UNICEF guidance and the United Nations Convention on the Rights of the Child should inform Irelands response to AI and child safeguarding.

32. The United Nations Convention on the Rights of the Child should be incorporated into domestic legislation.

33. While creating protections for young people online, adults should bear in mind that children have evolving capacities and needs for information and privacy.

34. The Ombudsman for Children's office and Coimisiún na Meán should continue to engage, with quarterly meetings and other opportunities for collaboration, to ensure children's rights are central to the Coimisiún's policies and are effectively being upheld by platforms.

4. What children told us

While the young people who came before the Committee recognized the importance of AI and phones for accessibility and safety, they generally lamented getting access to phones and social media at such young ages, wished for their younger siblings to do so at a later stage, and praised limits, parental controls and phones without social media apps that just facilitate calls and texting, for example. Here are some extracts from what they told the Committee:

"I get it now when my mother says to me, 'It is always the phone's fault; that is the thing that is giving you the headache and that is why you cannot sleep at night.' I understand what she says now because she is right."

"I am worried about my godson getting a phone. He is three and I am worried about him watching TV too much with a device in his hand that has no restrictions because his parents do not know how to put restrictions on it. I am going back to the issue of education but if there were something available stating how you should set up your child's phone and have it do anything you require it to do, how to restrict it, how to add guidelines and how to ensure the child cannot access anything inappropriate, it would be really helpful."

"It would be good if social media platforms checked ID to make sure users are not really young children. The same applies to AI."

"As a teenager, I think that social media is a nuisance. When I got my first phone, I was only allowed to have a small Nokia phone until I was 13. Then I got a phone from my godmother. I was going into secondary school at the time and it was important that I had a phone. At that time, there were a lot of things I did not know about social media because I was stuck in Covid and not at school. People do not know much about social media and they are doing things they should not be doing. My younger sister was never given the same treatment as me. She should have been treated the same because social media is such a bad place."

"I really do wish I did not get social media as young as I did. I was around seven or eight, and it definitely had a big impact on my mental and physical health... Kids get phones too young now... there are different phone brands you can buy that only let children have the FaceTime and Messages apps, with no games, social media or anything. There should be more awareness about these types of phones if people do want to get their young child a phone so they do not have access to social media."

"As someone who got a phone at 11 ... it impacted on my mental health a lot. Many children are now up till 4 a.m. or 5 a.m. scrolling on their phones. As a teenager, I am definitely one of those. I do not think primary school children should have phones until sixth class. ... Even going back to the topic of pornography, they do not know about this or expect it. I will not name social media sites, but people could try to text you and speak to you. Because you are so young, you do not expect what they are saying and you tell them what to do. They could

be older than you and you think that an adult has more power than a child so they could take advantage of the child."

"The alternative is going online and finding out about things in a way that is not healthy and not how it should be. We should be learning about these issues from a trusted adult or trusted teacher, not finding out for ourselves, as my peers and I may have had to do."

"I am quite negative about AI in general. I can go onto Snapchat and have an artificial conversation. I tried it and it felt like talking to a real person. It felt like I was having a social interaction with one of my friends. That is how real it was to me. That is scary and worrying f I do not want my family to grow up on that, saying they do not need a conversation with their best friends as they have their AI. That is not a real person. Using it will limit people. It will limit their social interaction, increase social anxiety, increase stress levels in public places and make people unable to do something like we are doing now."

"A specific worry I have about AI is sexual violence online, specifically grooming. Older men or women can go online, on Google or Google Chrome, get photos of young teenage boys or girls and portray themselves as them. They can go onto Snapchat and talk to young people... it is so easy for people to get sexually assaulted online from the way AI is progressing and its technological advancements. It is so easy... You will not be able to tell if it is an actual teenage boy you are talking to, or a 50-year-old man behind a phone screen or laptop."

"I agree there should be parental monitoring when you are on social media and when you are using AI and with all of the regulations. There should also be more education for young people on AI, to talk about how to use it and how not to use it, who made it and who gets the benefit of using the content... On the subject of verification for social media platforms and AI, young people are smart and they evolve and will figure ways around IDs. They can get fake IDs fairly easily. They will figure out ways to go around things."

"We need more education around the topics of consent, sexual safety and so on. Everyone will benefit crucially from that."

"Showing ID to prove you are a certain age or some means of proving your age should be required to access social media, just so we will know that really young kids will not see fake

content or material that is not completely true that can completely damage their mental health. An ID system to prove you are a certain age would benefit."

"Even with age restrictions, there is an issue...I was around five when I got a phone... as you got older you learned about Snapchat, which has the add button. You find yourself adding away, wondering who you are adding, and then, all of a sudden, a pop-up jumpscare. It is important to really know what you are getting your child into. It is so easy for parents, when they see their children crying, to give them a phone to watch ... It is really important to know the dangers. There are advantages and disadvantages."

These contributions are extracted from a meeting the Committee held on 23 April 2024, with the youth advisory panel which supports the Ombudsman for Children in relation to Ireland's international obligations under the UNCRC and emerging issues for children in Ireland, including artificial intelligence. The transcript and video of that meeting can be accessed here.

5. Education, morality and the wider picture

During the Committee's discussions with experts in the field, some big philosophical questions arose about the online word as a sometimes-poor reflection of our real-world values and priorities. Questions about why so much sinister content and behaviour flourishes online, why anonymity and pseudonyms are omnipresent online but not elsewhere, and why many parents feel they can allow their children into that potential darkness unsupervised online but not in real life, proved difficult to answer. The tech landscape and the challenges it poses to young people can be overwhelming, and while this may encourage us to bury our heads in the sand, the experts that came before the Committee recommended the very opposite.

Witnesses acknowledged that while we have some rules, around things like cyber-harassment, for example, they focus on the idea of a pattern of conduct aimed at a single particular victim. The Committee heard that the broader societal harms that have emerged online, such as a pattern of conduct which is dangerous to the public in general or a pattern of conduct which is dangerous to protected groups, such as women and girls, for example, or particular minorities, need to be addressed.

Two seeming impasses were discussed, in terms of value alignment. The first being the profit driven motives of platforms versus the societal wish for the online world to be safe and positive. The second being the need to support jobs and inward investment versus needing to regulate how platforms operate for the sake of the public good. Overall, Members reflected that the gains in terms of investment no longer justify fence sitting in the face of the harms being discussed, with one Member surmising that "money has no morals."

In this context discussions turned to the need to hit companies responsible for the proliferation of harms where it hurts, namely their profits. CyberSafeKids highlighted that a recent Harvard study found that collectively in 2022, Meta, X, Snapchat and TikTok made $11 billion from advertising to children in the US, $2 billion of which was to children under the age of 12. CyberSafeKids suggested that a State-funded research and development laboratory with representatives from academia, industry and the not-for-profit sector should be set up to look at how to better protect users in meaningful ways. Members cautioned against regulatory capture. The Ombudsman for Children has acknowledged the tension between Ireland being attractive to tech innovators versus a place where children are effectively protected, but said emphatically that we should be the latter. The Committee wholeheartedly agrees.

It was agreed that education and a whole-of-society approach is now needed to keep people safe and to ensure that AI and social media are forces for good. This links back to comments in the foreword of this report, which acknowledge the need for adults to self-reflect on all of these issues and lead in behavioural changes and boundary setting. Blunt instruments like parental controls on apps or devices and limiting or banning phone use or time online will not work in isolation. It was widely acknowledged that young people can bypass any such measures, with one of the young people who came before the Committee saying that kids can use Snapchat AI to circumnavigate controls on Google, for example. Our approach to these issues needs to be thoughtful and comprehensive. Resources and education opportunities for adults need to be made available and promoted.

Professor Barry O'Sullivan informed the Committee that a free online course called the 'elements of AI' is available through UCC, which teaches the basics of AI to anyone

interested in the topic. It is UCC's aim to educate at least 1% of the Irish population on the basics of AI and both an English- and Irish-language version of the course are available.

While this report does not focus on the benefits of AI, the Committee acknowledges that there are many. The Committee values the positive role AI can play as an accessibility and inclusivity tool. It recognizes the good work platforms are doing with AI to identify and filter out underage users, harmful content and bad actors, at scale. International AI expert, Professor Barry O'Sullivan, told the Committee about how AI is also being used to tackle child sexual exploitation, including through initiatives such as GRACE, which equipped European law enforcement agencies with advanced capabilities to respond to the spread of online child sexual exploitation material.

In a similar vein, Ms Caoilfhionn Gallagher, Special Rapporteur on Child Protection, and others who came before the Committee, were keen to stress the importance of modern media in helping at risk or marginalized children. They reminded the Committee that there are sometimes risks to children from caregivers. So, measures to protect young people must also maintain their privacy and ability to access information and get help, especially where a child may be at risk in their home environment or within their community. Ms Gallagher cited LGBT+ young people and girls in some communities, as examples where this is of particular importance. AI systems can uphold or undermine children's rights, depending on how they are used.

Recommendations

35. The broader societal harms that have emerged online, such as a pattern of conduct which is dangerous to the public in general or a pattern of conduct which is dangerous to protected groups, such as women and girls, for example, or particular minorities, need to be addressed.

36. A whole-of-society approach is now needed to keep people safe and to ensure that AI and social media are forces for good. This will need to involve adults self-reflecting, making behavioural changes and setting boundaries.

Appendix 1: Submissions

List of written submissions

Stakeholder
Irish Medical Organisation
Google
Google (2)