Growing Up Online
Addressing the Needs of Children in the Digital Environment

Greater connectivity, greater risks

Children today spend more time online than ever before, due to the wider use of Internet-connected smartphones and tablets. The digital environment offers real and important opportunities to children and young people, such as allowing them to socialise with peers, express themselves and find information on just about any topic imaginable. Although it is important to help children benefit from these opportunities, it is equally if not more important to understand and address risks.

Many digital risks are online versions of familiar offline risks, such as bullying, racism and sexual predation. As is the case in everyday life, a zero-risk digital environment is unattainable. Yet it is still possible to establish the conditions necessary for a safer digital environment, and to provide children with the skills and tools to recognise and manage risks – without unnecessarily limiting their online opportunities.

Policy responses in a changing landscape

Given that online risks to children cross borders and jurisdictions, policies and actions aimed at mitigating them demand international collaboration. In 2012, OECD countries adopted the Recommendation of the OECD Council on the Protection of Children Online. The Recommendation aims to support governments in setting the conditions for the protection of children online through better evidence-based policy making and enhanced co-ordination between all stakeholders. While not legally binding, OECD Recommendations carry a political commitment, and have proved highly influential in setting international standards and helping governments to design legislation in areas such as privacy.

The landscape that gave rise to the 2012 Recommendation has dramatically changed. Children and young people now spend much of their lives online, using the Internet not only to complete homework assignments, but to connect and socialise through platforms such as Instagram, Snapchat, TikTok and Facebook. As their online behaviour has evolved, so too have the risks that they face.

Since 2017, the OECD has been examining the relevance of the 2012 Recommendation by surveying OECD countries, undertaking an extensive review of the legal and policy environment, and holding expert consultations. Through this work, the following themes emerged:

- the increasing privacy risks and “datafication” of children
- the need for legislative and policy responses proportionate to the level of risk
- the role of online platforms and other digital service providers.

Privacy risks and datafication

The privacy space has significantly evolved since the adoption of the 2012 Recommendation. Today, children’s personal data include not only the information that they knowingly share, but also information that derived from their online actions. The data that children share online can fall into one of three categories:
1. **Data given**: the data children provide about themselves (e.g. name or date of birth), as well as data provided by their parents and/or friends that can follow them into adulthood.

2. **Data traces**: the data they leave online (e.g. through cookies, web beacons or device/browser fingerprinting, location data and other metadata).

3. **Inferred data**: the data derived from analysing data given and data traces.

Data can also be interpersonal, institutional and commercial. Although most children have an understanding of their private space and the data that they provide, they have a more limited understanding of the use of data traces and inferred data for commercial purposes.

In a highly commercialised digital world, children can be important targets for marketers looking to influence the next generation of consumers. The use of children’s data, and particularly the commercial use of inferred data, is therefore a key issue for policy makers.

The use and misuse of children’s data give rise to various potential risks. These include concerns that artificial intelligence algorithms may direct children toward harmful advertising content; that the sharing of children’s personal information could lead to inappropriate contact; and that data may be collected unknowingly and without consent through apps or connected toys.

**Age-appropriate and coordinated legislative and policy responses**

Legislative responses today are wide-ranging and largely made up of rules and norms addressing specific risks. Although digital issues cut across traditional legislative boundaries, responsibility remains siloed across government agencies whose actions are often uncoordinated. For example, justice ministries are often solely responsible for developing legal responses to sexting (the exchange of sexually explicit messages), yet bodies responsible for health and education should also likely be involved.

In responding to sexting, government agencies have also acted without clear evidence of the actual risks. In some cases, isolated legislative actions have led countries to hold children criminally liable because their own pictures are considered child pornography. In the case of sexting, the narrow conceptualising of laws and frameworks can in fact prove both ineffective and counter-productive, if not outright harmful. Legislative and policy responses should be evidence-based, and should appropriately address the needs of children online.

**The role of online platforms and digital service providers**

Concerns around risks such as sexting, cyberbullying and grooming have prompted calls for new legislation, and have put pressure on online service providers, platforms and social media sites to do more to protect children from online abuse and harmful content.

Some countries have already taken steps in response to these concerns. Examples include the introduction of the Age Appropriate Design Code in the United Kingdom, published in 2020 and expected to come into effect in 2021; the 2017 decision in the United States to modify the Communication Decency Act by including liability for websites that facilitate child sex trafficking; and Germany’s 2017 law, which levies significant fines on online platforms that fail to remove hate speech.

Multistakeholder dialogue and promoting children safety by design, as well as accountability as an obligation, are key to addressing a number of online concerns for children.

Further reading


This document, as well as any data and any map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.