Chapter 10. Child protection online

Elettra Ronchi[1] and Lisa Robinson[2]

[1]OECD Directorate for Science, Technology and Innovation

[2]Université de Cergy-Pontoise, France

Children are online more than ever before. While a multitude of opportunities arise from the digital environment, so too can the potential for increased exposure to risks such as exposure to harmful content, cyberbullying, age-inappropriate advertising and data misuse. These risks can affect children's well-being and undermine their right to privacy. Online opportunities and risks are not mutually exclusive, and the right balance must be struck between promoting online use and protecting children from risks.

OECD countries implement various legal frameworks and policies to protect children online, and to promote the notion that what is illegal offline should also be illegal online. In 2012, the OECD Council adopted a Recommendation for the Protection of Children Online. This chapter highlights the work to update this Recommendation and considers some of the policy and legislative avenues countries take to protect children online and to promote positive online use.

Introduction

Children are spending more time online than ever before. Increasingly, children and young people are using mobile devices (smartphones and tablets) with Internet connectivity to go online. Time spent online provides many opportunities, such as socialising with peers, expressing themselves through the creation of online content and seeking information on just about any topic imaginable. While real and important opportunities exist, spending more time online can also increase exposure to digital risks. Many of these are online versions of long known offline risks (bullying, racism, cheating and sexual predation) (Livingstone et al., 2011[1]). And just as is the case in everyday life, a zero-risk digital environment is unattainable, however setting the conditions for a safer one is feasible. Children must be provided with the (digital) skills and tools necessary to recognise and manage these risks, without unnecessarily limiting their online opportunities. At the same time it is important to have strong frameworks and guidelines in place so that all stakeholders involved do their part in both protecting children from online risks, and to ensure that benefits can be realised.

To assist governments in this task, the OECD Council adopted in 2012 the Recommendation on the Protection of Children Online (hereafter the “Recommendation”) which calls for evidence-based policy making and enhanced co-ordination at the domestic and international levels in order to improve national policy frameworks. Since 2017, the OECD has been working to revise the Recommendation to take account of legal and technological developments since its adoption, and to ensure its continued relevancy.

This chapter will examine some of the different risks children can encounter online, using the typology of risks identified by the OECD in 2011 as a base for this analysis. It will provide an overview of how the risks have evolved since that time, consider the continued relevancy of the typology of risks, and finally will provide an overview of the Recommendation developed by the OECD in 2012 and the efforts underway to update it.

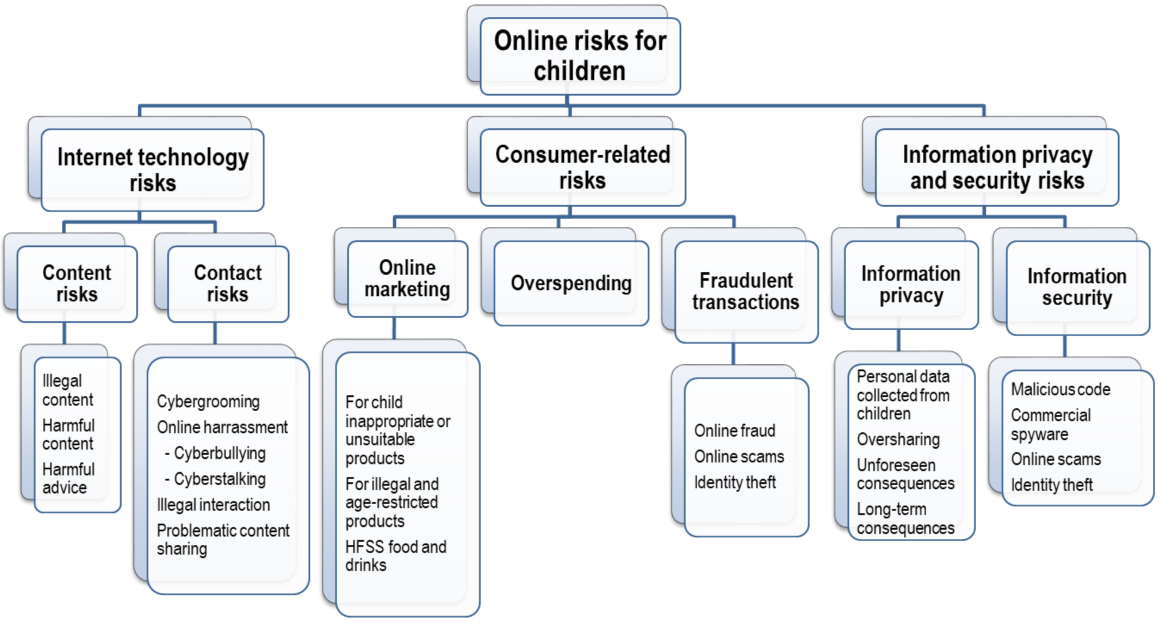
Typology of risks

The Recommendation was developed around a typology of risks (see Figure 10.1) including three broad categories: i) Internet technology risk – further subdivided as content and contact risks, including exposure to illegal or harmful content (e.g. pornography, cyber-grooming and cyberbullying) and advice; ii) consumer risks related, for example, to online marketing and fraudulent transactions; and iii) information privacy and security risks.

In 2017, the OECD set out to examine whether the Recommendation remains relevant by carrying out a survey of OECD member countries (‘the Survey’), followed by an extensive review of the legal and policy environment, and an expert workshop held in Zurich in October 2018. Key findings from this work indicate that broadly, while the typology of risk remains relevant, the risk landscape has significantly evolved since 2012 and there are a number of issues that need to be taken into account or expanded upon in this typology.

Firstly, the concept of a conduct risk was not previously included. In 2011, the OECD Report covered behaviour by children that creates risks for themselves, however it specifically excluded online activities whereby children were creating risks for other children (OECD, 2011[2]). At the time the Recommendation was developed, Snapchat did not exist, and Instagram, WhatsApp, Twitter, Whisper, Tumblr and a host of other platforms were barely known. Teenagers today are enthusiastic users of social media sites, chatrooms and apps, and are more prone to creating and sharing user-generated content than before. A conduct risk refers to situations where the child is the actor in a peer-to-peer exchange, including when their own conduct can make them vulnerable (e.g. sexting). It is distinguishable from a contact risk whereby a child is a victim of an interactive situation (Livingstone et al., 2011[1]).

Figure 10.1. Typology of risks: OECD 2012 Recommendation



Secondly, it is not clear that the typology of risk has kept up to date with changes in the privacy space. There have been significant changes in this area since the adoption of the 2012 Recommendation. Today, children are more likely to be content creators and data subjects themselves. Lastly, the current typology of risk does not address the potential risks of overdependence and mental health issues (although robust evidence in this space is lacking; see Chapter 8).

The following section of this chapter will consider briefly the main risk areas identified above. Namely: contact risks (encompassing conduct risks), content risks, consumer risks and privacy risks. This includes an analysis of how legal and policy responses are able to respond to these risks today.

Contact risks

When considering contact risks – also encompassing situations where a child's conduct may place them at risk – three main areas and the consequent legislative responses are addressed below. These are cyberbullying and harassment, sexting and sextortion.

Cyberbullying

Cyberbullying has been defined as, "intentional harmful behavior carried out by a group or individuals, repeated over time, using modern digital technology to aggress against a victim who is unable to defend him/herself" (Campbell and Bauman, 2018[3]). However, several researchers have used differing terms and qualifiers to define cyberbullying, and how it may be distinguished from more 'traditional' forms of bullying and harassment. Some researchers stress the importance of a power imbalance weighted in favour of the aggressor, likening cyberbullying to the definition of traditional bullying, but adding 'digital technology' as the mechanism by which harm is inflicted. Others have suggested that anonymity and publicity are defining features of cyberbullying, a suggestion that is however, contested. Even though these two features are easier to accomplish through cyberbullying, they are not necessarily always present (the bully can be known and could use private channels) (Campbell and Bauman, 2018[3]).

This seeming inability for researchers to land upon a common definition of what constitutes cyberbullying, paired with divergent legislative responses (as will be seen below), renders the issue a moving target and makes trends difficult to reliably assess. In addition, the unique facets of the digital environment can increase risks for cyberbullying. These include: the huge size of the potential audience; continuous access; the permanency of online content; the ease of copying and distributing material; and a lack of oversight of online behaviour (Campbell and Bauman, 2018[3]). Large-scale studies have shown that cyberbullying is associated with high levels of stress (Cross et al., 2009[4]), social difficulties, depression and anxiety (Campbell et al., 2013[5]). Compared to traditional bullying, those who have been cyberbullied report higher levels of anxiety, depression and social difficulties (Perren et al., 2010[6]; Sticca and Perren, 2013[7]). In some studies, cyberbullying has been seen to have a stronger association with suicidal behaviour (thoughts, plans and attempts) than traditional bullying (Bonanno and Hymel, 2013[8]; Klomek, Sourander and Gould, 2011[9]). However, these findings are variable and do not establish the direction of the association (i.e. whether the bullying is the cause of the mental health struggles or vice versa, see also Chapters 12 and 14).

Perhaps as a result of this lack of consensus among research and policy actors as to what actually constitutes cyberbullying, countries tackle this problem in a variety of ways. Some continue to apply their traditional harassment laws to cyberbullying offences. For example, under UK legislation there is not a specific law that expressly makes cyberbullying illegal, although it can be considered a crime under different pieces of legislation. While this legislative framework is currently the subject of a law commission review, it is observed that spread of legislation creates some complexity in that it requires both applying the elements of traditional harassment offences to online behaviour, as well requiring that the appropriate offence be identified in the midst of multiple pieces of legislation.

Like the United Kingdom, Luxembourg and Norway have laws to address harassment, however, they do not specifically relate to online conduct. Interestingly, Luxembourg noted in their response to the Survey that a person who harasses someone through the dissemination of an image may be subject to sanctions if that image otherwise falls foul of a copyright law. Norway also indicated that the misuse of an image – namely, the reproduction of a photo of a person without their consent – could fall foul of copyright laws. These two responses are an interesting example of attempts made by governments to address issues as they arise using existing laws, and highlights the need for a targeted response. Unless the image falls foul of a copyright law, any person harassed in this way is left without a remedy should copyright law not apply. In addition, there is likely little awareness of the availability of these causes for legal action and redress.

As of August 2018, forty-nine states in the United States had authorised bullying laws, generally requiring schools to create policies to deal with bullying and include cyberbullying or online harassment as an offence. Furthermore, there are criminal sanctions for cyberbullying or for electronic forms of harassment. In Canada, legal responses available incorporate both civil and criminal law (i.e. suing for defamation, subject to suspension/expulsion, subject to traditional negligence laws). Harassment and defamatory libel in this instance are both prosecutable under criminal law.

Some governments have also recently sought to open up social media companies to direct oversight, and liability. On 1 January 2018, Germany introduced the Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act) also known as NetzDG (Bearbeitungsstand, 2017[10]). This Act protects against insult, defamation and intentional defamations (among other issues such as hate speech), and compels social media companies to remove content (in the face of significant fines). An Australian Senate Committee recently recommended that civil liability laws be amended to create a duty of care on social media platforms to ensure the safety of their users, and that regulatory measures backed up by significant financial penalties be used to ensure that such platforms both prevent and respond quickly to cyberbullying (Australian Senate, 2018[11]).

Most of the aforementioned laws operate, to some extent, in a silo. Some countries have thus sought to create a mechanism to facilitate reporting and legal action. In Australia, for example, the e-safety commissioner has powers in this area in conjunction with other responsibilities related to protecting minors online and to promoting digital literacy. In relation to cyberbullying, the e-safety commissioner provides an easy online process for reporting cyberbullying.

Sexting

'Sexting' refers to the exchange of sexual messages and it is a rising online phenomenon as mobile devices become more accessible. Sexting is an example of an emerging issue to which an isolated legislative response is not possible, and which may be both ineffective and in some cases damaging. This issue is a prime example of a new and emerging online risk where the narrow conceptualising of laws and frameworks can in fact prove both ineffective and often counter-productive, if not outright harmful (Byrne and Burton, 2017[12]).

While intuitively it may seem that sexting would emerge as a risk only if an image is shared without the subject's consent, when minors engage in sexting they may be self-producing child pornography material that can quickly spread online and remain on the Internet permanently. This fact contributes to a complicated legal environment in terms of criminal liability and victimisation. In a number of countries, the sharing of sexualised or nude images among teenagers is considered illegal, and can result in the prosecution and punishment of adolescents under national pornography laws (UNICEF, 2012[13]; Byrne and Burton, 2017[12]). In a number of countries, child pornography laws may require a mandatory placing of the offender on a child sex register list – a move which can have life-long negative impacts and consequences. There are examples of minors in different countries being prosecuted and charged for the production, distribution and/or possession of child pornography when in some instances this resulted from children sending nude personal images or "selfies" to each other.

Sexting has the potential to be very harmful to children's privacy and mental health. Sexual pictures can spread quickly online and remain on the Internet permanently. However, even in this space there is disagreement with regard to whether or not the simple act of sexting itself causes harm, or whether harm only arises when the exchange is unwelcome or harmful in some way (Livingstone and Görzig, 2014[14]; Gillespie, 2013[15]).

Gender can influence sexting behaviours (see also Chapter 12). There is research from Canada suggesting that youth that accept traditional gender stereotypes have a significantly higher tendency to share sexts (Johnson et al., 2018[16]). Boys who accept traditional gender stereotypes are more likely to share sexts than girls who share the same beliefs. At the same time, girls who share sexts can be perceived as violating gender norms and even giving up the right to their pictures. Consequently, sexism and gender stereotyping appear to play a significant role in the 'culture of sharing' (Johnson et al., 2018[16]).

The legal response to sexting is emerging in a space where it remains unclear exactly what the nature of the risk is. Is the risk the mere exchanging of messages with sexual content or images, or does it only arise when there is some coercion involved or forwarding of the images and associated consequences? It has been suggested that certain groups are more likely to experience harm from receiving sexual messages, notably girls, younger children, and those who face psychological difficulties; accordingly, policy responses should be aimed at ameliorating harm to these groups (Livingstone and Görzig, 2014[14]). In any event, it is clear that the current legislative response is inadequate to address the risk of harm. This response predominantly relies on criminal laws, which in many cases criminalise the young persons who are themselves at risk, rather than provide effective preventative measures or support. Recent research suggests that when minors are aware of the legal ramifications of sexting, they are less likely to engage in underage sexting. However, many youth are unaware of the legal consequences of sexting; therefore, accessible information campaigns may be a simple but effective way of reducing rates (Strohmaier, Murphy and DeMatteo, 2014[17]).

Sextortion

Sextortion is a new type of online exploitation of adolescents that is being identified by the media, law enforcement and policy makers. Sextortion refers to the threat to share or expose a sexual image in order to coerce the victim into doing something (e.g. sharing more pictures, engaging in sexual activity, paying money or other demands) – even if the sharing of the image itself never occurs (Wolak et al., 2018[18]). It is not to be confused with sexting and/or the non-consensual sharing of sexual images (often for a bullying or 'revenge porn' purpose), which fall into a separate category. Sextortion is not a term presently defined in legal instruments, and prosecutions for sextortion may rely on identifying criminal liability within the provisions of existing laws that cover related offences (for example, those against: hacking; child pornography; harassment; extortion; stalking; and privacy violations) (Wolak et al., 2018[18]).

Content risks

In 2011, the OECD identified three main subcategories of content risk: i) illegal content; ii) age-inappropriate or harmful content; and iii) harmful advice (OECD, 2011[2]). Broadly speaking, these three subcategories persist today, although advances in technology have altered both the potential volume of this material, and the ways by which children may become exposed to it. Some issues that stand out as either new or amplified since the 2012 Recommendation include: hate speech, offensive material and harmful content, traditional broadcasting regulation, and fake news.

The number of children affected by exposure to hate content online is rising. According to Ofcom, the United Kingdom's Communications Regulator, in 2017, 45% of children aged 12-15 in the United Kingdom reported seeing hateful content online over the previous year (2016) (Ofcom, 2017[19]). This was an increase from the year before when 34% of children in this age group made this report (Ofcom, 2016[20]). However, it is also noted that although this is a rising trend, there is also evidence that children and young people are becoming more aware of how to respond to exposure to hateful content online and how to make a report. Additionally, this type of conduct may fall within criminal legislation in countries, such as those that cover hate crime in offline spaces. However the available legal responses to date have been largely ineffective, suggesting the need for targeted action adapted to the digital environment. At the European Union (EU) level in 2016 the European Commission developed the Code of Conduct on Countering Illegal Hate Speech Online. The Code was developed with the input and agreement of major platforms such as Facebook, Twitter, Microsoft and YouTube. In the course of 2018, Instagram, Google+, Snapchat and Dailymotion joined the Code. Jeuxvideo.com joined in January 2019. The Code requires the review of all reports of hate speech online within a 24-hour time frame. The latest 2018 evaluation shows that the companies are now assessing 89% of flagged content within 24 hours and 72% of the content deemed illegal hate speech is removed (European Commission, 2019[21]).

In New Zealand, the Harmful Digital Communications Act (Parliament of New Zealand, 2017[22]) deals with both the sending and the publishing of offensive material (among other matters). The Act's guiding principles include that: 'a digital communication should not be grossly offensive to a reasonable person in the position of the affected individual' (Principle 3); and, 'a digital communication should not be indecent or obscene' (Principle 4). The Act provides sanctions, enforcement and take down provisions.

Several countries have also recently taken policy or programmatic steps to try and specifically address the issue of fake news, which is perceived as an urgent and emerging threat. Media and digital literacy, and critical thinking are generally viewed as essential skills in this regard. Increasingly, government action in this area includes programmes addressed to teaching children and young people to be able to distinguish between what is fact and what is fiction in information distributed online. This is a particularly critical skill given that children and young people predominantly obtain their news from social media sources, which may or may not be reliable, and accordingly children must be able to critically analyse the content they are consuming. In 2017, a public broadcaster in the United Kingdom undertook a survey on consumers' capacity to identify "fake news". Of the people surveyed, only 4% were able to distinguish what was real from what was fake. In the same year, the United Kingdom's Communications Regulator identified that 73% of 12–15 year-olds were aware of the concept of fake news, while 39% said that they had ever seen something online that they thought was a fake news story (Ofcom, 2017[19]).

The United Kingdom has since indicated a commitment to ensuring that minors' critical thinking skills are enhanced through digital literacy training, so that young people can better recognise reliable from unreliable sources and intentionally misleading information on the Internet. Australia's e-safety commissioner has publicly available information designed to help minors identify what is real and what is not on the Internet.

Consumer risks

In 2011, the OECD indicated that children may "face consumer risks online when *i*) they receive online marketing messages that are inappropriate for children (e.g. for age-restricted products such as alcohol); *ii*) they are exposed to commercial messages that are not readily identified as such (e.g. product placements) or that are intended only for adults (e.g. dating services); or *iii*) their credulity and inexperience are exploited, possibly creating an economic risk (e.g. online frauds)" (see (OECD, 2012[23])). This statement remains true today, however a host of emerging practices potentially pose a risk to children. This includes online marketing, in-app purchases, digital and viral marketing strategies, and the growing prospect of 'big data' mining. All these issues may pose risks to children in that they may amount to commercial or peer pressure, have implications for protecting children's privacy, or lead to the exposure of a child to inappropriate products or messages. In response to the 2017 OECD Survey, few countries indicated that their laws specifically addressed consumer risks to children, and/or that they had any specific statutory safeguards in place to prevent inappropriate advertising to, and/or dealings with, children.

Privacy risks

Legal responses today are striving to keep pace with technological advancements and how this affects children's privacy and the processing of their personal information. Before considering the legal responses, it is useful to first briefly review the relevant data typologies that the legal responses are attempting to address, and how children of different ages comprehend these typologies in terms of their privacy. Data can be typified by:

- 'data given' – the data contributed by individuals (about themselves or about others), usually knowingly though not necessarily intentionally, during their participation online
- 'data traces' – the data left, mostly unknowingly – by participation online and captured via data-tracking technologies such as cookies, web beacons or device/browser fingerprinting, location data and other metadata
- 'inferred data' – the data derived from analysing data given and data traces, often by algorithms (also referred to as 'profiling'), possibly combined with other data sources (Livingstone, Stoilova and Nandagiri, 2018[24]).

Research has shown that while children are aware that they may have contributed data about themselves or about others as a result of their online activities, the extent to which they understand the consequences for their privacy will depend upon their own understanding of interpersonal relationships, which in turn depends on their age, maturity and circumstances. Primarily, children are aware of 'data given' in interpersonal contexts (e.g. because they provide data themselves, or they may be aware that their family and friends do too). Children are becoming more aware of the commercial uses of 'data traces', however their understanding of 'inferred data' and its value to businesses will be dependent upon their understanding of business models operating in commercial and institutional contexts – something that they are rarely taught about (Livingstone, Stoilova and Nandagiri, 2018[24])

At the same time, these commercial uses of children's data are themselves seemingly becoming a more prevalent and visible concern. More apps are being designed and targeted towards children and the invention of 'smart connected toys' creates more opportunities for children's data to be collected and used – often in a manner contrary to protections designed to protect the privacy of children in this regard as demonstrated in two recent studies (Norwegian Consumer Council, 2017[25]; Reyes et al., 2018[26]).

Legal and policy responses

At the national level, almost all countries responded to the OECD 2017 Survey that their privacy laws act to protect children in some way, although issues relating to consent, to the processing of data, and to the breaches of these laws may differ. As was the case in 2012, at the time the OECD Recommendation was adopted, information privacy and information security risks are largely covered by privacy and general data protection rules, and criminal laws. Operationally, privacy issues may fall under the responsibility of a specific regulator or commissioner, who in their role, undertake actions that may directly or indirectly relate to the protection of children online. Countries in the EU that are bound by the General Data Protection Regulation (GDPR) (see also Chapter 12) now uniformly recognise that children merit special protection as it relates to their personal data, particularly in relation to marketing, creating profiles, and the collection and storage of data; and provides special rules related to the provision of consent for the processing of a child's data.

In addition to the GDPR, special protection for children in the processing of their data is also found at the European level in the revised Audiovisual Media Services Directive (AVMSD). Its article 6a(2) provides that the personal data of minors collected or otherwise generated by media services are not to be processed for commercial purpose, such as direct marketing, profiling and behaviourally-targeted advertising. However, this is a relevantly new provision, and it will take time to see its efficacy in practice.

In other OECD countries, consent is required by the information subjects themselves or has to be given on behalf of children under a certain age (e.g. 15 in Australia). In the United States, the Children's Online Privacy Protection Act (COPPA) of 1998 prohibits the collection, use and dissemination of personal information from children under the age of 13 without informed, advance parental consent. In some countries the violation of children's privacy is criminalised.

The 2012 OECD Recommendation on the Protection of Children Online

This last section will consider the Recommendation, and the process for its review. Consistent with the 1989 United Nations Convention on the Rights of the Child, the Recommendation includes principles for all stakeholders involved in making the Internet a safer environment for children. It focuses on three main challenges faced by governments which underline the emerging nature of the protection of children online as a public policy area: *i)* the need for an evidence-based policy making approach; *ii)* the need to manage policy complexity through enhanced policy co-ordination, consistency and coherence; and *iii)* the need to take advantage of international co-operation in improving the efficiency of national policy frameworks and fostering capacity building.

The Recommendation focuses on the protection of children as users of the Internet, and was grounded in the typology of risks and the 2011 report, as has been reported above. It is noted that the Recommendation does not address child pornography or sexual abuse images online, a decision made based on the notion that child pornography or sexual exploitation called for radically different measures to protect minors and were covered in other international instruments, in some cases requiring law enforcement co-operation such as through Interpol.

The Recommendation is divided into three sections. The first section covers policy making for all stakeholders and includes principles on:

- empowering children, recognising the primary role of parents in minimising risks to their children online (as they do offline)
- the adoption of policy measures proportionate to the risks, respecting fundamental values, and seeking to avoid undermining the framework conditions that have enabled the Internet to succeed
- flexibility to address differing ages and vulnerabilities among children.

The second main section covers domestic policy making by governments and recognises that good policy making requires leadership, co-ordination, coherence, awareness raising, evidence and technology solutions. The final section addresses international policy making by governments and addresses the importance of international networks, information and data sharing, capacity building, and the participation of other intergovernmental organisations.

The changing nature of online risks & updating the Recommendation

The Recommendation on the Protection of Children Online instructs the OECD Committee on Digital Economy Policy (CDEP) to review this Recommendation and its implementation, and to report to Council within five years of its adoption. Beginning from the end of 2016, steps have been taken to carry out this task as described in the box below.

Box 10.1. Process for review of the OECD Recommendation on the Protection of Children Online

At its 40th meeting on 15-16 November 2016, the Working Party on Security and Privacy in the Digital Economy (SPDE) discussed the process for the review and agreed to circulate a questionnaire to delegations on the implementation and continued relevance of the Recommendation. The questionnaire was circulated in 2017 seeking to gather information on recent developments in child online protection policy, identify areas where the OECD Recommendations may need to be updated and to assess the potential impact of contextual changes (e.g. technologies, usages and threats).

Thirty-four countries responded to the questionnaire and a preliminary report was presented in May 2017. The findings suggest that compared to 2012, the environment that gave rise to the Recommendation has significantly evolved. Much of this evolution is due to the growth in the use of mobile devices and social networks - for many countries, cyberbullying is a significant and growing concern, followed by sexting, children's privacy and hateful content.

As a result of the survey, it was agreed by delegates that more evidence was needed to explore potential options for updating the Recommendation. There was consensus that a review of recent legal and policy developments as well as an expert meeting would be a useful way forward. Consequently, a review of recent developments in legal frameworks and policies for the protection of children was undertaken, as well as a meeting of experts in Zurich in October 2018. As a result of this analytical work, a multi-stakeholder international expert group was established in 2019 to provide guidance for the revision of the Recommendation.

Three layers of policy making

The OECD Recommendation set out three different levels of policy responses:

- national frameworks: this comprises legislative responses and policy instruments (direct and indirect)
- multi-stakeholder policy making: this is related to the different roles and responsibilities of stakeholders
- international policy making: this comprises cross-border co-operation and initiatives targeting knowledge-sharing.

Policy makers are encountering different issues as digital technologies become increasingly integrated into children's daily life. The complexity of digital spaces, the pace of change, including the different devices and platforms available, social contexts and differing online environments mean that simple legal and policy measures are not sufficient. There is further need for a balancing act between actions to promote greater use of digital technologies (for example through their integration in national curricula and the promotion of digital skills and literacy) and actions designed to protect minors from risks associated with their use. Policies must be holistic, taking into account the many different and interconnected ways of being online, including for learning, communication, entertainment, creativity, self-expression and civic participation, and whether children use it at home, school or elsewhere. Also too often, policy on risks are developed independently of those on opportunities, and vice versa. For example, promoting digital literacy through policy action will be more effective if it is incorporated into a holistic programme, also targeting responsible usage, digital citizenship and online safety. Strategic visions and centralised institutions can help systems deal with this complexity and overcome fragmentation in the system.

The following will briefly consider the analysis of each of the three levels of policy making outlined above.

National legal and policy frameworks

Of the 34 respondents to the OECD Survey (see Box 10.1), all had some form of legislative and policy responses in place addressing risks to children online. However, in general, these responses are fragmented and countries largely appear to lack a comprehensive framework.

In terms of legislative responses, in 2011, the OECD reported that most countries would subscribe to the notion that things that are illegal offline should also be illegal online, thereby championing a normative approach. The main challenge at that time, which still persists today, is finding ways of ensuring and enhancing compliance/enforcing existing instruments, rather than developing and adopting additional measures. The laws that are in place cover three main elements: *i)* criminality (i.e. to address risks of sexual abuse, harassment); *ii)* content regulation; and *iii)* privacy protection. There are two distinct types of laws as well: those which relate directly to children and those which cover the entire population, and by virtue of that, extend to minors.

In terms of policy making, the results indicate that countries also tend to either create new policies (or laws) or adapt existing ones to address child safety online and new and emerging risks. Often, these policies are not child-specific, and in some instances are found embedded within policies that apply more broadly, such as those targeting innovation and skills for example. The ad hoc development of policy arrangements and wide implementation instruments and strategic goals further highlight that these policies are not always implemented as part of a single strategic vision for the protection of children online.

Countries with a national digital strategy, designed to inform the direction of the overall digital transformation of a country, may more readily adopt a whole-of-government approach in policy making. This being said, while some national digital strategies take this holistic position, a majority still take a protective stance on children instead of providing an overarching vision taking into account both risks and opportunities. Similarly, statutory oversight bodies may often focus on protective measures rather than promoting positive Internet use and digital literacy.

Lastly, the OECD Survey results highlights the largely reactive nature of national policy and legislation, consistent with the findings of O'Neill and Dinh in their mapping of 31 EU countries who found a similar tendency (2018[27]).

Multi-stakeholder policy frameworks

There is a common understanding that an online child protection policy rests on the commitment and shared responsibilities of all stakeholders. Multi-stakeholder policy making occurs when governments enter into partnerships for the delivery of complementary policy actions, for example through the promotion of industry codes of conduct or self-regulation actions. For example, the OECD Privacy Guidelines recognise a multi-stakeholder group as comprising of experts from governments, privacy enforcement authorities, academia, business, civil society and international technical experts (OECD, 2013[28]).

A number of countries have sought to enter into partnerships with industry and civil society to address risks to children online. In some countries specific bodies have been created to coordinate the activities of private and public stakeholders. One specific example is the United Kingdom's Council for Internet Safety (UKCIS – previously the Council for *Child* Internet Safety, however now with an expanded role). This council brings together Government, industry, law enforcement, academia, charities and parenting groups to work in partnership to help keep people safe online, on a non-statutory basis (Government of the United Kingdom, n.d.[29]).

In addition to such a body, several countries rely on both consultation and engagement with civil society and with industry to develop and implement strategies and programmes for child online protection. This may take the form of direct policy input, joint initiatives, and representation on larger multi-stakeholder forums. It may include the offer of services, awareness raising activities, resource development, research and education.

From the industry perspective, a number of companies take an active stance in relation to ensuring the protection of children online. In particular, the major social media and other Internet sites have policies regarding child protection, although with varying efficacy. For example, Google has taken steps to enforce COPPA compliance (see above under Privacy risks). Its 'Designed for Families' programme provides app developers with information on COPPA and requires that they certify they are in compliance. However, there is limited enforcement of this (Reyes et al., 2018[26]).

International policy frameworks

There is a common understanding across countries that international and regional co-operation is central to addressing the challenges of child protection in an inherently global digital environment. Intergovernmental organisations at international and regional levels have a role to play in this space within their respective remits. The work that is undertaken in this space includes some useful actions towards harmonisation of policy responses in particular to address the potential risk of digital divides and for inclusivity as well as measurement and monitoring. Regional and international co-operation takes place at both policy and operational levels.

At the regional level, both the Council of Europe (COE) and the EU have developed policy frameworks to protect children online. The work of the COE emerges largely in a rights space, while the EU's actions are centralised in the *Better Internet for Children Strategy* ('the BIK Strategy') and its associated activities.

The COE and the United Nations Committee on the Rights of the Child – the body of 18 independent experts that monitors implementation of the Convention on the Rights of the Child by its State parties – have taken steps seeking to ensure that children's rights are appropriately protected and upheld in any legislative or policy response. While to date, policy measures focus to a large extent on the need to protect children, this emphasis has been noted as contributing to a diminishment of children in their role as individual rights holders. It neglects the fact that they themselves are creators of online content, have a right to participate in matters that affect them, have a right to provision of information and a right to a freedom of expression (Byrne and Burton, 2017[12]).

The other regional body somewhat active in this space is the Asia-Pacific Economic Cooperation (APEC), which at its 2012 Telecommunications and Information Ministerial Meeting acknowledged, for example, that vulnerable groups, especially children, are particularly susceptible to risk in an online environment, and has since called upon its members to implement strategies and promote cyber safety and cyber security (Asia-Pacific Economic Cooperation, 2012[30]).

The International Telecommunication Union (ITU) Child Online Protection Initiative (COP) links an international collaborative network (including countries, other international organisations, the private sector and civil society) with the common aim of promoting the protection of children online and has released Guidelines for Child Online Protection targeted separately at: children; parents, guardians and educators; policy makers; and industry. These Guidelines are currently under review. UNICEF is also active in this space. For example, the UNICEF Office of Research - Innocenti has prepared a number of reports on the safety of children online and has launched the Global Kids Online Research Initiative in partnership with the London School of Economics and Political Science and EU Kids Online. This project seeks to fill a gap that previously existed regarding comprehensive global research. Separately, UNICEF partnered with ITU to develop the above-mentioned guidelines for industry on online child protection

Finally, the Insafe and INHOPE networks are examples of international work at an operational level acting to respond to reports of risk through hotlines and helplines (European Commission, n.d.[31]).

In sum

This chapter has considered new and emerging risks that have come to light since the OECD first considered the protection of children online, through its 2011 report and resulting Recommendation. This has been done through a survey of member countries, analysis of the laws and policies in place today as well as a consultation with international experts. This body of work examined in particular whether laws and policies have kept pace with the changing environment. While some promising practices are seen – such as the creation of (although few) single oversight bodies and a continued common understanding of the importance of international and regional co-operation – a number of issues remain.

These include:

- the wide-ranging nature of the legislative responses (combining/segregating online and offline responsibilities; siloed responsibilities)
- the drawbacks of separating legislative responsibilities (duplicating efforts; overlooked matters; the creation of new social issues)

- fragmented policy responses and few single oversight bodies
- a lack of consistent measurement and reporting – including varied definitions and terminology; and consequently, a lack of evidence-based policy making
- a recognition of the importance of engaging business and a need to better capitalise on multi-stakeholder action
- a recognition of the importance of digital and media literacy, and the promotion of the positive benefits of online content and engagement, and a need to better balance promotion of the positives with protective actions
- the changing nature of the privacy space, and a need to better recognise children as data subjects and content creators, and consequently how best to protect them in this space
- the need to consider including the concept of a conduct risk within the OECD's typology of risk.

References

Asia-Pacific Economic Cooperation (2012), *2012 Leaders' Declaration*, www.apec.org/Meeting-Papers/Leaders-Declarations/2012/2012_aelm. [30]

Australian Senate, L. (2018), *Adequacy of existing offences in the Commonwealth Criminal Code and of state and territory criminal laws to capture cyberbullying*, www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Cyberbullying/Report. [11]

Bearbeitungsstand (2017), *Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act)*, www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf;jsessionid=829D39DBDAC5DE294A686E374126D04E.1_cid289?__blob=publicationFile&v=2. [10]

Bonanno, R. and S. Hymel (2013), "Cyber bullying and internalizing difficulties: Above and beyond the impact of traditional forms of bullying", *Journal of Youth and Adolescence*, Vol. 42/5, pp. 685-697, http://dx.doi.org/10.1007/s10964-013-9937-1. [8]

Byrne, J. and P. Burton (2017), "Children as Internet users: How can evidence better inform policy debate?", *Journal of Cyber Policy*, Vol. 2/1, pp. 39-52, http://dx.doi.org/10.1080/23738871.2017.1291698. [12]

Campbell, M. and S. Bauman (2018), "Cyberbullying: Definition, consequences, prevalence", in *Reducing Cyberbullying in Schools*, Elsevier, http://dx.doi.org/10.1016/b978-0-12-811423-0.00001-8. [3]

Campbell, M. et al. (2013), "Do cyberbullies suffer too? Cyberbullies' perceptions of the harm they cause to others and to their own mental health", *School Psychology International*, Vol. 34/6, pp. 613-629, http://dx.doi.org/10.1177/0143034313479698. [5]

Cross, D. et al. (2009), *Australian Covert Bullying Prevalence Study (ACBPS)*, Child Health Promotion Research Centre, Edith Cowan University, https://docs.education.gov.au/system/files/doc/other/australian_covert_bullying_prevalence_study_executive_summary.pdf. [4]

European Commission (2019), *The EU Code of conduct on countering illegal hate speech online*, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/countering-illegal-hate-speech-online_en. [21]

European Commission (n.d.), *Better Internet for Kids - Insafe and INHOPE*, www.betterinternetforkids.eu/web/portal/policy/insafe-inhope. [31]

Gillespie, A. (2013), "Adolescents, sexting and human rights", *Human Rights Law Review*, Vol. 13/4, pp. 623-643, http://dx.doi.org/10.1093/hrlr/ngt032. [15]

Government of the United Kingdom (n.d.), *UK Council for Child Internet Safety (UKCCIS)*, www.gov.uk/government/organisations/uk-council-for-internet-safety. [29]

Johnson, M. et al. (2018), *Non-Consensual Sharing of Sexts: Behaviours and Attitudes of Canadian Youth*, http://mediasmarts.ca/sites/mediasmarts/files/publication-report/full/sharing-of-sexts.pdf. [16]

Klomek, A., A. Sourander and M. Gould (2011), "Bullying and suicide: Detection and intervention", *Psychiatric Times*, Vol. 28/2, www.psychiatrictimes.com/bullying-and-suicide. [9]

Livingstone, S. and A. Görzig (2014), "When adolescents receive sexual messages on the internet: Explaining experiences of risk and harm", *Computers in Human Behavior*, Vol. 33, pp. 8-15, http://dx.doi.org/10.1016/j.chb.2013.12.021. [14]

Livingstone, S. et al. (2011), *EU Kids Online: Final Report 2011*, EU Kids Online, London, http://eprints.lse.ac.uk/id/eprint/45490. [1]

Livingstone, S., M. Stoilova and R. Nandagiri (2018), "Conceptualising privacy online: What do, and what should, children understand?", http://eprints.lse.ac.uk/90228/. [24]

Norwegian Consumer Council (2017), *Significant security flaws in smartwatches for children*, Forbrukerrådet, www.forbrukerradet.no/side/significant-security-flaws-in-smartwatches-for-children/. [25]

O'Neill, B. and T. Dinh (2018), *The Better Internet for Kids Policy Map: Implementing the European Strategy for a Better Internet for Children in European Member States*, www.betterinternetforkids.eu/bikmap. [27]

OECD (2013), *The OECD Privacy Framework 2013*, OECD Publishing, Paris, www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. [28]

OECD (2012), *The Protection of Children Online: Recommendation of the OECD Council - Report on risks faced by children online and policies to protect them*, www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf. [23]

OECD (2011), "The protection of children online: Risks faced by children online and policies to protect them", *OECD Digital Economy Papers*, No. 179, OECD Publishing, Paris, https://dx.doi.org/10.1787/5kgcjf71pl28-en. [2]

Ofcom (2017), *Children and Parents: Media Use and Attitudes Report*, www.ofcom.org.uk/__data/assets/pdf_file/0020/108182/children-parents-media-use-attitudes-2017.pdf. [19]

Ofcom (2016), *Children and Parents: Media Use and Attitudes Report*, www.ofcom.org.uk/__data/assets/pdf_file/0034/93976/Children-Parents-Media-Use-Attitudes-Report-2016.pdf. [20]

Parliament of New Zealand (2017), *Harmful Digital Communications Act 2015*, www.legislation.govt.nz/act/public/2015/0063/latest/DLM5711810.html. [22]

Perren, S. et al. (2010), "Bullying in school and cyberspace: Associations with depressive symptoms in Swiss and Australian adolescents", *Child and Adolescent Psychiatry and Mental Health*, Vol. 4/1, http://dx.doi.org/10.1186/1753-2000-4-28. [6]

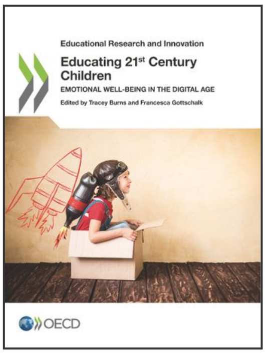
Reyes, I. et al. (2018), ""Won't Somebody Think of the Children?": Examining COPPA compliance at scale", *Proceedings on Privacy Enhancing Technologies* 3, pp. 63-83, http://dx.doi.org/10.1515/popets-2018-0021. [26]

Sticca, F. and S. Perren (2013), "Is cyberbullying worse than traditional bullying? Examining the differential roles of medium, publicity, and anonymity for the perceived severity of bullying", *Journal of Youth and Adolescence*, Vol. 42/5, pp. 739-750, http://dx.doi.org/10.1007/s10964-012-9867-3. [7]

Strohmaier, H., M. Murphy and D. DeMatteo (2014), "Youth sexting: Prevalence rates, driving motivations, and the deterrent effect of legal consequences", *Sexuality Research and Social Policy*, Vol. 11/3, pp. 245-255, http://dx.doi.org/10.1007/s13178-014-0162-9. [17]

UNICEF (2012), *Child Safety Online: Global Challenges and Strategies. Technical report*, Innocenti Publications, www.unicef-irc.org/publications/652-child-safety-online-global-challenges-and-strategies-technical-report.html. [13]

Wolak, J. et al. (2018), "Sextortion of minors: Characteristics and dynamics", *Journal of Adolescent Health*, Vol. 62/1, pp. 72-79, http://dx.doi.org/10.1016/j.jadohealth.2017.08.014. [18]


Educational Research and Innovation
Educating 21st Century Children
EMOTIONAL WELL-BEING IN THE DIGITAL AGE
Edited by Tracey Burns and Francesca Gottschalk
OECD

From:

Educating 21st Century Children

Emotional Well-being in the Digital Age

Access the complete publication at:
https://doi.org/10.1787/b7f33425-en

Please cite this chapter as:

Ronchi, Elettra and Lisa Robinson (2019), "Child protection online", in Tracey Burns and Francesca Gottschalk (eds.), *Educating 21st Century Children: Emotional Well-being in the Digital Age*, OECD Publishing, Paris.

DOI: https://doi.org/10.1787/796ac574-en

This work is published under the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of OECD member countries.

This document 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.