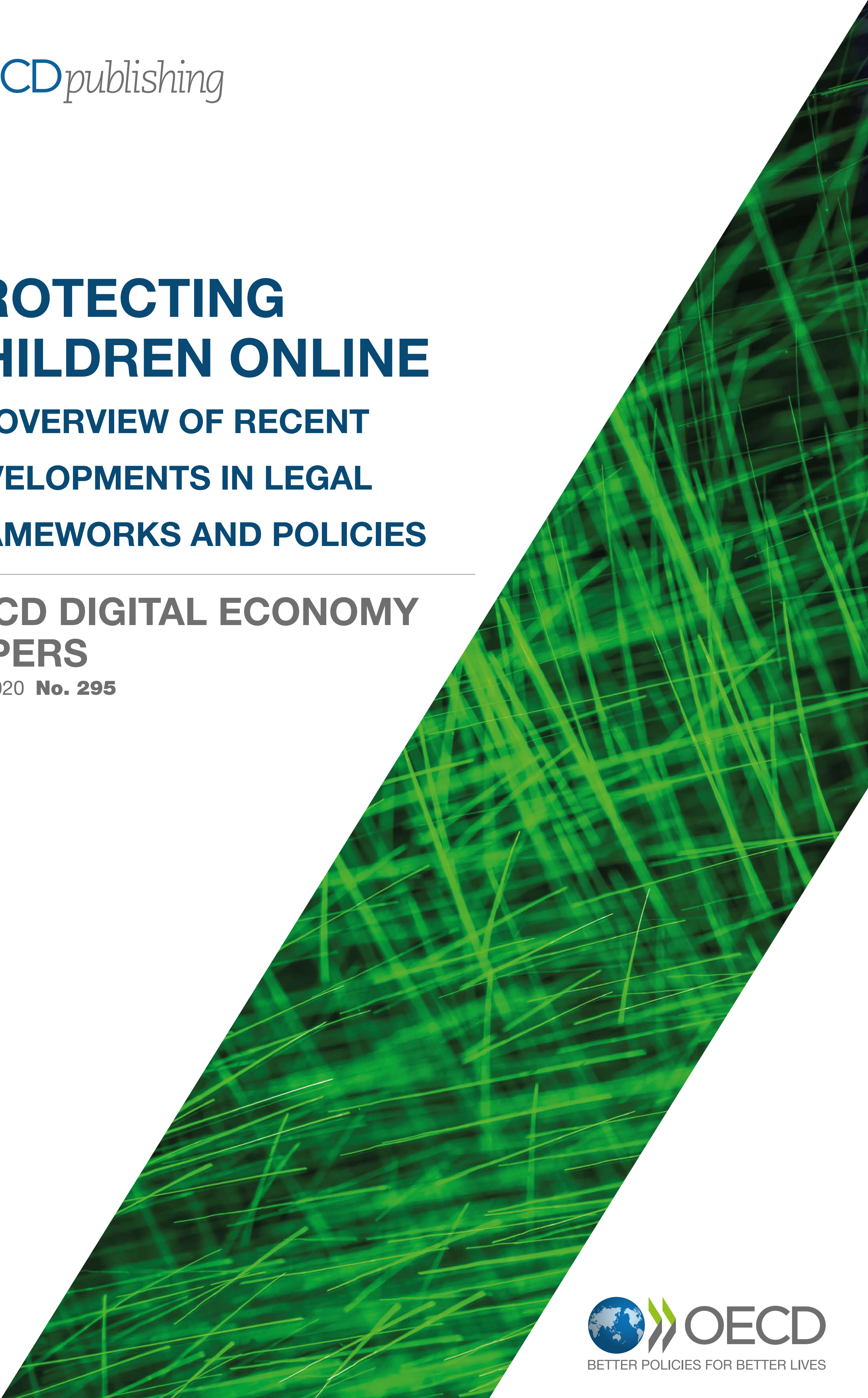
OECD publishing

PROTECTING CHILDREN ONLINE

AN OVERVIEW OF RECENT DEVELOPMENTS IN LEGAL FRAMEWORKS AND POLICIES

OECD DIGITAL ECONOMY PAPERS

May 2020 **No. 295**



OECD

BETTER POLICIES FOR BETTER LIVES

Foreword

This report aims to provide an overview of legal and policy actions taken by governments, international organisations, and other stakeholders to ensure a safe and beneficial digital environment for children. It analyses new and emerging risks since the adoption of the 2012 OECD Council Recommendation on the Protection of Children Online (hereafter the "OECD Recommendation") [OECD/LEGAL/0389], and the changing nature of previously existing risks. The report serves to inform the review of the OECD Recommendation to bring it into line with the current (and anticipated future) needs of children in a digital environment.

The report was drafted by Lisa Robinson, (Consultant to the OECD), and Elettra Ronchi, (OECD Secretariat). It was prepared under the aegis of the OECD Committee for Digital Economy Policy (CDEP), with input from delegates of the Data Governance and Privacy Working Party (former Working Party on Security and Privacy in the Digital Economy) and approved for publication by written procedure. Delegates contributed significantly with their comments and amendments, and in particular the support of delegates from Canada, France, the United Kingdom and the United States of America is gratefully acknowledged. As it developed the report benefitted significantly also from the 'first consultation of the informal group of experts' hosted by the Swiss Government in Zurich on 15-16 October 2018. Lastly, the authors would like to warmly thank Andras Molnar (OECD Secretariat) for his continued support throughout the drafting process.

Note to Delegations:

This document is also available on O.N.E under the reference code:

DSTI/CDEP/SPDE(2018)12/FINAL

This document, as well as any data and 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. The statistical data for Israel are supplied by and under the responsibility of the relevant Israeli authorities. The use of such data by the OECD is without prejudice to the status of the Golan Heights, East Jerusalem and Israeli settlements in the West Bank under the terms of international law.

Table of contents

Executive Summary

In 2011, the OECD sought to respond to the then emerging concern that the increased use of the Internet by a growing number of children carried with it a number of risks that are specific to children. At that time a comprehensive report was released, resulting in the OECD Recommendation on the Protection of Children Online that was adopted by the OECD Council in 2012 with an instruction to review its implementation within five years of its adoption.

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: the need for an evidence-based policy making approach, for managing policy complexity through enhanced policy co-ordination, consistency and coherence as well as for taking advantage of international co-operation to improve the efficiency of national policy frameworks and foster capacity building.

This report seeks to contribute to the review of the Recommendation by: *i)* analysing new and emerging risks; and *ii)* identifying whether or not laws and policies have kept pace with advances in technology.

This analysis is supported (and founded upon) responses received from 34 OECD countries who replied to a 2017 survey that sought to: gather information on recent developments in children online protection policy; identify areas where the OECD Recommendation may need to be updated; and assess the potential impact of contextual changes (e.g. technologies, usages, threats, etc.).

Today, even more children are using the Internet, and are doing so through a variety of hardware and software that was not commonplace in 2011. Increasingly, children and young people are using mobile devices (smartphones and tables) with wireless connectivity to go online. At the same time, children and young people are 'living their lives' in the digital environment, connecting with each other through platforms such as Instagram, Snapchat, Twitter, Facebook, TikTok and WhatsApp; and using connected devices for their leisure and education (for example through apps, websites and online games). Along with this evolution in the type (and frequency) of children's use of the digital environment is a recognition that the risks (and indeed the benefits) associated with this use may too have evolved.

In 2011, the OECD recognised a number of risks associated with children and the digital environment (then referred to as 'online risks for children').[1] At that time, the OECD placed online risks into three broad categories (content and contact risks; consumer related risks; and privacy and security risks). Whilst these categories are seen to persist today, the substantive acts underlying these risks have evolved and changed. For example, whilst cyberbullying was a definite concern in 2011, in the 2017 OECD Survey it was identified by member countries as the highest priority risk. Issues that did not exist (or were not highly visible) in 2011, such as sexting or sextortion, are identified as new concerns. The concept of a conduct risk – that is where the child is the actor in a peer-to-peer exchange, such as in sexting – was not previously recognised by the OECD.

As well as these specific risks, this report highlights challenges, differing responses and promising practices that emerged in response to other risks which have evolved as a result of increased Internet availability and use. Children today are more likely to face increased privacy risks that go hand in hand with more time spent in the digital environment; be exposed to hateful, harmful or offensive content online;

and increasingly they may be the subject of targeted advertising or face financial inducements associated with, for example, online gaming that they are not equipped to deal with.

All these issues present challenges for policy makers in finding measures that can both address risks, and be responsive to the particular needs and vulnerabilities of children. At the same time, there is an emerging recognition of the benefits that the digital environment can provide to children, for example in terms of connectivity and educational benefits. Ensuring children's digital literacy is seen as key to both reaping these benefits and to equipping children to protect themselves in the digital environment.

This report specifically considers legal and policy responses; the role of industry, civil society and multi-stakeholder initiatives; how the effectiveness of responses to date is measured and monitored; and the role of regional and international bodies. It is observed that:

- The **legislative response** is seen to be wide-ranging, largely made up of legislation that has been aligned to specific risks, and leaves responsibility for meeting needs and addressing risks with the ministries or departments who would be responsible for like acts in the offline space. This results in responsibility for individual concerns being siloed into different disciplines, ignoring the reality that this is a space that crosses traditional legislative boundaries. For example, the issues of sexting and cyberbullying imply a response from justice, health, and education (at a minimum) and impact on children's privacy rights. Consumer risks for children, may straddle both traditional consumer responsibility issues (*e.g.* through enticements to spend on in-app purchases), and privacy issues (*e.g.* where data is mined from app-users).

- By **keeping legislative responses separate** countries risk: a duplication of efforts; matters not being covered by any relevant law; and potentially creating new social issues arising out of a strict and at times indiscriminate adherence to laws.

- The response by some countries to create a **single oversight body** is promising in that it allows issues arising out of the digital environment to be addressed in a more targeted and coordinated manner.

- **Complementary policy actions and programs** are necessary to fill gaps and address challenges, however the responses are often scattered across sectors. This results in a large number of ministries taking steps to respond to risks, often without responses being coordinated across the board. Additionally, individual ministries may respond in accordance with their own traditional responsibilities and methods, potentially resulting in inappropriate responses and/or that the appropriate measures are overlooked

- A common understanding exists that online child protection policy rests on the commitment and shared responsibilities of all stakeholders. Whilst there is promising engagement with industry and civil society, dedicated **multi-stakeholder** bodies are rare, but clearly provide a meaningful and positive contribution to policy and programmatic efforts where they do exist.

- Regulating social media platforms and other industry that operate across borders is difficult to do, as is enforcing national law upon them. Moves to create **Industry Codes of Conduct** exist and are a promising means of fostering cooperation between government and industry.

- **Digital and media literacy** is seen as a vital underlying skill for children in ensuring their safety in the digital environment. A number of promising initiatives exist relating to supporting this in both community awareness and an educational space. However, despite it being recognised that children should be taught to be able to safely benefit from the positives that arise from the digital environment, there is less of a focus on **positive digital content** in policy measures.

- In **measuring and monitoring** the effectiveness of existing legal and policy measures consistent approaches to definitions, methodologies and indicators are lacking. Survey taking appears to be a common monitoring / measuring mechanism, but there is a lack of consistency regarding what is measured and how those results are used, as well as discrepancies in terminology. A need for a systemic approach to evidence based policy making continues to be essential in determining policy priorities and in maximising protections that may be afforded by national policies.

- There remains a common understanding across countries that **international and regional co-operation** is central to addressing the challenges of child protection in an inherently global medium. Regional and international bodies continue to seek to foster communication, coordination and cooperation across borders.

Overall, it is seen that the variety of digital devices and platforms, social contexts and online environments do not easily lend themselves to simple policy and legal measures, and most countries face the challenge of having to balance the tensions between promoting greater use of digital media while also protecting children and teens from the potential risks of that use.

Introduction

This report examines and compares existing laws and policies to protect children online[2]. The analysis builds on responses from thirty-four countries[3] to a survey circulated in 2017 to OECD countries for the review of the 2012 Recommendation on the Protection of Children Online (hereafter 'OECD Recommendation'). The survey aimed to gather information on recent developments in children online protection policy; identify areas where the OECD Recommendation may need to be updated; and assess the potential impact of contextual changes (e.g. technologies, usages, threats, etc.).

The survey included seven sections, most of them asking respondents to provide detailed information. As a result, a vast amount of information was collected with varying levels of detail per question and per country, requiring in many instances follow-up clarification. This report does not, however, purport to provide a comprehensive inventory of the responses received. Its objectives are, first, to examine how policies have evolved since the 2011 OECD report "*The Protection of Children Online*" and second, highlight legislative change and promising practices, whilst at the same time identifying where gaps and challenges persist.

Specifically, the report considers how laws, policies and other initiatives respond to the need to protect children in the digital environment, from an overarching perspective. In turn, it considers at how domestic, regional, and international initiatives address the specific risks identified by the OECD in 2011 (contact risks, content risks, consumer risks, and privacy risks), the changing nature of these risks, any new and emerging risks, as well as the role that civil society and industry play in mitigating these risks.

Respondents to the survey were asked, '*which online risk categories should be addressed in a review, either because they are new or because they require updated evidence*'. Their responses provide a backdrop to this report and help to inform its structure.

The majority of the thirty-four countries ranked bullying and harassment highest, followed by sexting and cyber grooming. However, all of the risks listed in the questionnaire (see 'Figure 1' below) were considered relevant, with the exception of radicalization, which one country felt was out of scope.

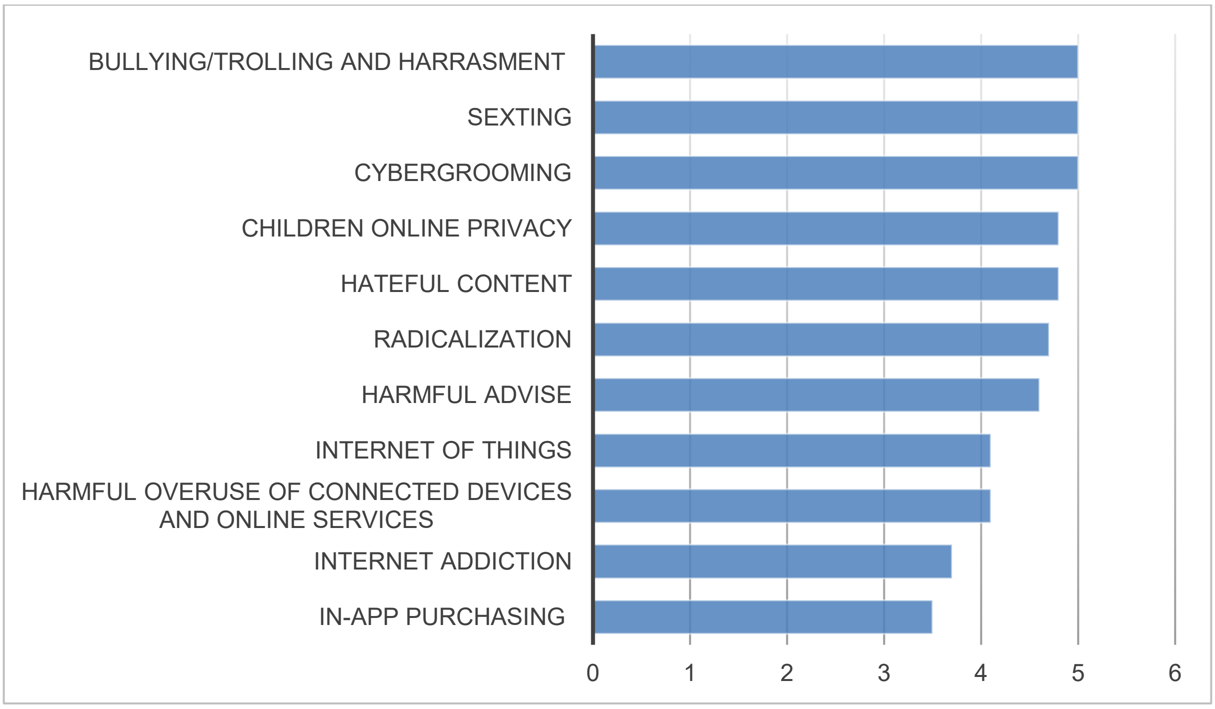
A large number of countries suggested that the OECD Recommendation should address the risks from online gambling and online gaming that encourage self-inflicted damage, as well as online drug and alcohol sales to minors.

In addition, countries noted that usage of mobile devices (smartphones, tablets) with mobile internet connection has increased among the very young since 2012. It is posited that this has changed the age-related risk profile, and as such it should be re-examined. Given the fast pace of technological developments some countries felt there is also scope to consider new and emerging developments such as Internet of Things (IoT), Artificial Intelligence (AI) and the risks of minors being profiled as a result of the data that is collected about them. An additional concern raised is the capacity for Learning Analytics programs having the capacity to analyse data traces left after a visit to an online learning platform. A majority of countries noted that in an IoT ecosystem, minors may be connected without recognizing that they are, meaning that their data (voice recordings, visual data, meta-data) may be collected from a range of devices not obviously recognizable as "computers" or as "being connected".

Finally, a few countries recommended that the review should provide an opportunity to address the risks from fake news and report on initiatives to teach minors how to become media-savvy and strengthen their critical thinking; and some countries raised questions regarding the exercise of digital right, namely rights of access, rectification, freedom of expression, and the right to be forgotten.

Figure 1. Rating of new and emerging risks

(From lower priority (1) - to higher priority (6))



Source: OECD 2017 Questionnaire

In the OECD Recommendation, three different levels of policy response are identified:

1. *National frameworks*: Comprising legislative responses, and direct and indirect policy instruments;
2. *Multi stakeholder policy making*: Relating to the various roles and responsibilities of stakeholders
3. *International policy making*: Comprising of cross-border cooperation and knowledge sharing initiatives.

The following sections will consider these three layers of policy in light of the responses to the OECD Survey, the new and emerging risks that have been identified, and the legal and policy framework that presently exists.

Two issues stand out from the analysis and are worth highlighting. Firstly, the variety of digital devices and platforms, social contexts and online environments do not easily lend themselves to simple policy and legal measures. Secondly, most countries face the challenge of having to balance the tensions between promoting greater use of digital media while also protecting minors from the potential risks of that use.

All countries report a variety of approaches, including legislative, self- and co-regulatory, technical, awareness-raising, and educational measures. These multi-layered policy approaches depend on a range of agencies and distributed governance, raising a number of challenges. How successful any one policy action will be, is dependant (at least in part) on other actions. For example, a digital literacy program will not work effectively if it is unaccompanied by policies to promote responsible usage, digital citizenship or online safety. A lack of policy coordination is a fundamental problem in ensuring effective policies for children in the digital environment. Whilst governments might be expected to invest more in policy coordination, there are numerous examples of failure to do so.

Compared to 2011, there are, however, promising moves by a number of countries to address this complexity through, for example, the development of a strategic vision and the creation of a centralised institution. There is also on-going national and international debate on whether voluntary codes of conduct and guidance adopted by industry should become legally binding, underpinned by an independent regulator and backed up by a sanctions regime.

1. National legal and policy frameworks

All countries that responded to the survey indicated that they had some form of legislative and policy response in place to address risks to children in the digital environment.

As was the case in 2011, the response has largely been to either create new laws and policies to address risks, or to adapt existing ones. Whilst some countries have specifically legislated or created a policy to protect children in the digital environment, the response remains to some extent fragmented and without a comprehensive framework to drive policy action.

The analysis reveals that countries tend to extend (or layer) existing frameworks to respond to new and emerging risks/needs. Policies implemented by various agencies and ministries, are not necessarily part of a single strategic vision, nor are they necessarily child specific, and they may be found within policies which apply more broadly (*e.g.* as part of a broader innovation and skills plan). Most existing policy arrangements or regimes are developed in an ad hoc fashion and contain a wide mix of instruments and strategic goals. In some cases, these may be implemented through partnerships supported or regulated by the Government, but that are not necessarily under the auspices of a ministry, department or statutory body.

In other cases, countries report the adoption of a national digital strategy, which is designed to inform the country's overall policy direction and feed into the work of individual ministries and bodies. A growing number of digital agendas or strategies established by countries show a trend towards a whole-of-government approach. These strategies are not necessarily directed at protecting children in the digital environment, but rather aim to holistically incorporate digital issues into a whole of government policy direction. In some cases, these strategies take a protective stance, rather than provide an overarching vision. For example, Poland takes a protective stance, with its Cyberspace Protection Policy (2013)[4], which is focussed on ensuring the cyber security of the country, and its citizens. Likewise, whilst the Mexican Government's 2013 National Digital Strategy[5] includes actions to promote the digital health of the country, it also includes a number of protective actions targeted at children under the "public safety objective" (objective 5). Austria's 2017 Digital Roadmap[6] takes a whole of government approach, and although not a child specific policy, it aims to address both the opportunities and risks associated with the digital environment for children.

In some countries specific legislation has been passed that addresses digital issues in a more targeted manner. In most cases this legislation is complemented by the creation of a statutory oversight body, or guiding policy strategy, with specific responsibility for protecting children in the digital environment (sometimes as part of the community as a whole). The following table provides an overview of these more targeted responses[7].

Table 1. Examples of specifically created statutory oversight bodies

Country	Oversight body	Responsibilities	Child specific
Australia	-Office of the e-Safety Commissioner -Established under the *Enhancing Online Safety Act* (2015)	General oversight of children in the digital environment, administers complaints scheme, accredits/trains educators, can direct the removal of online content & issue sanctions	No – but with a strong focus on children
Costa Rica	-National Online Security Commission -Established under Decree N° 36274 of the Ministry of Science and Technology (2010)	Administers both the National Online Safety Plan, and the Child Online Protection Policy. The National Online Safety Plan aims to: protect minors online, reduce the use of technology in crime; and promote online security	No – but with a strong focus on children
Israel	-National Network for the Prevention of Violence and Network Crime against Children and Teenagers -Government Decisions January & September 2016	Promotes a safer Internet through educational activities, administers a complaints scheme and a hotline. Is headed by the Director of the Public Security Ministry with a multi-agency steering committee.	Yes
Italy	Permanent Observatory To Protect Children and Individuals Fundamental Rights on the Internet Established by Resolution no. 481/14/CONS (2014)	Analyses issues related to the use of the Internet and Social media networks Monitors content and contact risks (hate speech, objectionable content, threats, bullying harassment), Operates under the auspices of the Communications Regulator.	No – but with a strong focus on children
Japan	The Third Basic Plan on Measures for Providing Safe and Secure Internet Use for Young People	Administered by the Headquarters for the Promotion and Development and Support for Children and Young People, Provides policy guidance for awareness raising activities for the ethical use of the Internet, and promotes voluntary efforts by citizens and business to protect children from harm on the Internet.	Yes
New Zealand	Netsafe Established under the Harmful Digital Communications Act (2015)	Provides information, advice and support on a wide variety of online safety topics. E.g. Bullying; fraud; consumer complaints; image based abuse; and data protection.	No

As can be seen from the table above, although laws and policies exist to promote positive use of the digital environment and good digital literacy, there is a greater tendency for the responses to focus on protective measures, particularly with regards to minors. This is true even when a single focussed oversight body/policy exists (e.g. Costa Rica, Italy). This tendency was reflected in a recent mapping of EU countries, where 10 out of the 31 countries[8] reviewed had no national policy on positive online content for children (O'Neill and Dinh, 2018: 9).

With this in mind, it is appropriate to note that where laws and policies are designed to be protective of minors online, they remain largely reactive in nature, coming about in response to a particular event, such as is the case for cyber-bullying. For example, both Italy and Austria indicated in response to the OECD survey that their anti-cyber bullying laws were drafted following high profile cases of suicide[9]. It has similarly been noted by other researchers that policy development may be more responsive to sensationalised media reports and high profile incidents, rather than being driven by reliable and representative data, this has led to an increased policy focus on child sexual exploitation online (Byrne and Burton, 2017: 42). This tendency will be further discussed and illustrated below in the discussion on the legislative response to the specific risk categories.

1.1. Legislative response

In 2011, the OECD reported that most countries would subscribe to the statement that what is "*illegal offline should be illegal online*" and champion a normative approach to child protection online (p. 33). In such countries, the main challenge was then, and remains now, finding ways to enhance compliance with / enforcement of existing instruments, rather than adopting additional laws and regulations. At that time, in a majority of countries, regulating online content was a cornerstone of national policy framework. A focus on regulation remains relevant today, however some countries are now doing so through specifically created bodies, in addition to relying on existing instruments (as seen in Table 1).

From a substantive perspective, the laws that are in place cover three main aspects: *1)* criminality (i.e. to address to risk of sexual abuse / harassment); *2)* content regulation; and *3)* privacy protection.

The majority of laws are general in their nature and either have been amended to apply specific provisions to digital risks (for example criminal laws which now include specific offences relating to material on webpages or online communication); or apply existing laws to new technologies (for example, content regulation laws which now apply to streaming services). This distinction can again be divided in two: *i)* laws relating directly to children; and *ii)* laws which cover the whole population, and necessarily extend to children.

Recalling the risks identified by the OECD in 2011, this next section considers how countries legislative responses have met the risk aspects identified, and how/if the various regulatory frameworks are keeping pace – both with those risks that had previously been identified, and with those that are new and emerging.

Before doing so however, it is noted that in 2011, whilst the OECD Report covered conduct by children that creates risks for themselves it specifically excluded online activities whereby children were creating risks for other children (OECD, 2011; p. 7). Despite this distinction at that time, it is noted that other risk typologies include the concept of a 'conduct risk'. This is a risk where the child is the actor in a peer-to-peer exchange, including when their own conduct can make them vulnerable (i.e. bullying, sexting), distinguishable from a contact risk whereby a child is a victim of an interactive situation (Livingstone et al., 2011; p 13).

This extra category of risk is highlighted here, given that it applies (in particular) to the risks associated with sexting and cyberbullying, which will be discussed in detail below. It is further included as it is becoming increasingly clear that this is a growing and significant risk for children, particularly compared with the situation in 2011. Since that date, the methods and manners in which children access the Internet and interact in the digital environment have changed significantly; and young people are (as is noted throughout this report) increasingly living their lives in the digital environment[10]. A conduct risk is now recognised by most stakeholders. For example, the UK's Safer Internet Centre (see paragraph 155) explicitly refer to this category of risk[11]. Additionally, in its work updating the Typology of Risk for Children in the Digital Environment, the OECD intends to specifically include a conduct risk as a category of risk.

During the OECD's October 2018 Workshop in Zurich on 'The Protection of Children in a Connected World' (hereafter, 'Zurich Workshop') this was directly addressed and discussed as a clear and recognised category of risk (OECD, 2019). Notably, Prof. Dr. Uwe Hasebrink elucidated a '4-C model of Online Risks' – Content, Contract, Contact and Conduct. Whilst the former two relate to service providers with the minor acting as a recipient and a market participant respectively, the latter two are related to communication. In a contact risk a child is a communication participant, whilst in a conduct risk the child themselves is the communicator. Here, children can be considered as agents who themselves produce or spread content that affects others in a negative, or indeed positive way.

1.1.1. Contact risks

Before considering the main issues which arise in this space, it is important to note that, while not being a focus of the OECD Recommendation, the predominant legislative responses identified in countries responding to the OECD Survey were criminal laws aimed at cyber grooming and child online pornography.

Nonetheless, other prominent risks were consistently identified as concerns, and consequently are often the subject of a legislative response. Compared to 2011, and as highlighted in the OECD Survey results, online harassment and cyberbullying are a growing area of concern. A number of countries also raised concerns about sexting and sextortion. Each of these issues are potentially justiciable or liable to trial, either as a prosecutable offence under criminal law, and/or as a civil liability matter. Whilst the legalities / criminality of sexting is perhaps the most complex in this space, each concern warrants deeper examination of: *i)* the issue itself; *ii)* the legal responses; and *iii)* their effectiveness.

1.1.2. Legal responses to online harassment and 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 & Bauman, 2017; p. 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 contested as even though these two factors are easier to accomplish through cyberbullying, they are not necessarily always present (the bully can be known and could use private channels) (Campbell & Bauman, 2017; p. 4).

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 somewhat of a moving target and makes trends difficult to reliably assess. Whilst on balance cyberbullying is considered to be a form of bullying, there is however additional disagreement on whether or not it is in fact a form of bullying or instead is a discrete form of aggression (Dooley, Pyżalski, & Cross, 2009; Campbell & Bauman, 2017). This debate further contributes to the 'moving target' element of cyberbullying. If cyberbullying is recognized as a form of bullying, then traditional anti-bullying programs may be appropriate; whereas if it is a completely new and unique phenomenon, then perhaps new and unique programs need to be developed (Campbell & Bauman, 2017; p. 6).

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 & Bauman, 2017; p. 4). Large-scale studies have shown that cyberbullying is associated with high levels of stress (Cross et al., 2009), social difficulties, depression and anxiety (Campbell, et al., 2013). Compared to traditional bullying, cyberbullying has been found to have a more negative impact on mental health, with those who have been cyberbullied reporting higher levels of anxiety, depression, and social difficulties than those who have been 'traditionally bullied' (Perren et al., 2010; Sticca & Perren, 2013). In some studies, cyberbullying has been seen to have a stronger association with suicidal behavior (thoughts, plans, and attempts) than traditional bullying (Bonanno & Hymel, 2013; Klomek, et al., 2011).

Despite this, a number of countries 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 constitute a crime under different pieces of legislation. This is complex 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. One example is the Protection from Harassment Act 1997, which creates an offence when a person pursues a course of conduct that amounts to the harassment of another, which the perpetrator knew or ought to have known amounts to harassment. This could include sending a person multiple abusive emails with the intention of causing alarm or distress. However, the Malicious Communications Act 1988, the Obscene Publications Act 1959, the Public Order Act 1986 and the Computer Misuse 1990, among others, are also potentially applicable in this space. In 2014 (Muthanna et al, 2017) a House of Lords Committee reviewed whether a dedicated Act was needed. Ultimately, it was decided that the existing legislation is "generally appropriate for the prosecution of offences"[12]. However, there continued to be increasing concern that the current legislation is not entirely effective (Muthanna et al, 2017).

In February 2018, the Prime Minister announced a Law Commission review on the law regarding abusive and offensive online communications. The review aimed to highlight any gaps in the criminal law that may cause problems in tackling this abuse. In its scoping report, the Law Commission concluded that although there are some ambiguities and technical issues with the law the breadth of the current communications offences available for offensive and abusive online communications means that in most cases, criminal offences are available for such behaviour online, as there would be for similar offline behaviour. In some cases, those offences capture words and behaviour that would not be a criminal offence offline. At the time of finalising this report, it is understood that government is now finalising the details of the second phase of the Law Commission work[13].

Like the United Kingdom, Norway and Luxembourg 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 through the use of existing laws, and highlights the need for a targeted response. The use of a copyright law to protect persons from online harassment, is likely ineffective both from the perspective of community awareness of the availability of these causes of action, and prevention. Here, any measures which force the take down of a picture, or which result in sanctions would only be available should the image fall foul of a copyright law, leaving any person harassed in this way without a remedy, should copyright law not apply.

Additionally, in Norway whilst as of today there are no strong legal sanctions in place for those who commit bullying in school or through the digital environment, the national authorities are considering new measures. Currently, Norwegian anti-discrimination legislation protects against harassing remarks directed against one or more specific persons on the grounds of gender, disability, ethnicity (including national origin, skin colour, descent, language), sexual orientation, gender identity and gender expression. The Equality and Anti-Discrimination Ombuds Office and the Equality and Anti-Discrimination Tribunal enforce anti-discrimination legislation, but are not authorised to award compensation, even if a violation of the law is demonstrated. The victims of such harassing remarks may seek compensation by taking the matter to court, but very few do so in practice[14].

In the United States (US) as of August 2018, forty-nine states had authorised bullying laws[15]. Predominantly, these laws require schools to create policies to deal with bullying, and include cyberbullying or online harassment as an offence (49 states in each instance). Almost all states impose a criminal sanction for cyberbullying or for electronic forms of harassment (44 states) or a specific school sanction for cyberbullying (45 states). Nonetheless, there exists great variation across states regarding exactly what is mandated. Additionally, no bullying laws exist at the federal level, despite a Bill being introduced to the US Congress in 2009[16].

Two countries, in response to the survey indicated that they have specifically introduced legislation which criminalises cyber bullying – Italy and Austria. Although both Acts are age neutral, they expressly criminalise online harassment, and both were inspired by the suicides of teens related to online bullying. The Italian law places an obligation on website operators to remove offensive material, with the capacity for the national body in charge of protecting personal data to intervene if the material is not removed within 24 hours.

Additionally, a 2014 French law provides criminal sanctions for harassment or bullying17. A more serious sanction applies should the offence be committed against a person aged less than 15 years, or by using online means. It is reported that this reform in the law both recognised cyber-harassment as a crime for the first time in France, and has allowed victims to defend themselves more effectively than before, allowing them to have their complaints handled more quickly[18].

Whilst the responses discussed above are mostly criminal in nature, some laws provide for measures to be taken at the civil law, or policy/programmatic level. For example, Colombia introduced a law in 2013 which obligates actors at all levels of the education administration (national departmental, municipal, school) to mitigate risks against acts which would disturb the ‘peaceful coexistence’ of students in schools. Whilst this law is not specific to cyberbullying, it is inclusive of it. In some countries, the laws in place may straddle either different legal problems (*e.g.* cyberbullying and privacy risks) or differing levels of responsibility (*e.g.* by covering both civil and criminal aspects).

New Zealand’s 2015 Harmful Digital Communications Act is an example of the former. This legislation cover the issues discussed in this section (on harmful contact) and those which are addressed below regarding harmful content and privacy risks. The Act creates an offence of causing harm via digital communication, for example through sending messages, or posting material online (pictures, photos, videos) that is both intended to cause harm, and does cause harm[19]. As well as creating offences, this legislation creates a pathway for the removal of harmful digital content[20].

Canada’s response is an example of one which bridges both civil and criminal liability, as dependant on the situation, cyberbullying can be dealt with under civil or criminal law. Under civil law, three responses are available: *1)* the cyberbully may be sued for defamation; *2)* the cyberbully may find themselves subject to suspension or expulsion should the cyberbullying be occurring between two school students – even if it happens outside of school; and/or *3)* the person may be subject to traditional negligence laws, should the consequences of their actions be reasonably foreseeable (e.g. the cyberbully may face a wrongful death suit, should suicide be a reasonably foreseeable consequence of the cyberbully’s actions). Under criminal law, both harassment and defamatory libel are prosecutable offences[21].

Whilst most of the laws mentioned here operate, to some extent, in a silo, Australia’s e-safety commissioner (established under the Act mentioned in Table 1 above) has powers in this area in conjunction with other responsibilities related to protecting children in the digital environment and to promoting digital literacy. In relation to cyber-bullying, the e-safety commissioner provides an easy online process for reporting cyber bullying[22], is empowered to issue an end user notice to the poster of any cyberbullying material, and may direct them to, *inter alia*, remove the material and apologise to the subject of the harassment (including prescribing the manner of apology)[23].

Whilst a number of the above initiatives are positive, difficulty lies in the ability of countries to regulate and enforce national law on the actions of social media platforms. Social media platforms are online intermediaries that enable user-generated content and allow for interactivity among users and direct engagement with the content (DeNardis & Hackl, 2015). These platforms operate across borders, and are often a host or conduit for the behaviour of others – both issues which arguably make it difficult for domestic regulation or sanctions. According to a recent study by Milosevich (2016), the cyberbullying policies of the social media companies are generally enforced through self-regulatory mechanisms that social media companies themselves have in place to address incidents on their platforms. These mechanisms can include reporting tools, blocking and filtering software, etc. (Milosevic T, 2016). In 2017, Instagram was reported in a study as the most popular vehicle for cyberbullying (Wakefield, 2017), with more youths experiencing cyberbullying on Instagram than any other platform at 42%, with Facebook following at 37% and Snapchat ranked third at 31% (Grigonis, 2017).

Some governments have thus 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[24] that (among other issues such as hate speech) protects against insult, defamation and intentional defamation 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 cyber bullying[25].

The United Kingdom is considering introducing an industry levy that would be used to support the activities of an independent regulator, proposed to be appointed to oversee and enforce any new regulatory framework (not yet in force)[26]. Whilst this proposal was initially made in 2017, calls for regulation continued to be made in the United Kingdom. In January 2019, the health secretary wrote a letter to Social Media companies in the wake of the suicide of a 14-year-old girl, who had easily accessed material about suicide prior to her death. The letter warned the companies addressed (including Facebook, Google, and Twitter) that the minister would not hesitate to use the law to force companies to act, should they fail to remove inappropriate content[27]. On 8 April 2019, the Department of Culture, Media and Sport published the "Online Harms White Paper"[28] comprising legislative and non-legislative measures to make companies more responsible for their users' safety online, especially children and other vulnerable groups. The White Paper, which was open for consultation until July 2019, proposed establishing in law a new duty of care towards users, to be overseen by an independent regulator. It proposes that companies be held to account for tackling a comprehensive set of online harms, ranging from illegal activity and content to behaviours which are harmful but not necessarily illegal.

Conversely, in the United States, the "Good Samaritan" (which is the statutory language used by Congress) provision of the Communications Decency Act of 1996 (CDA, codified at 47 U.S.C. § 230(c)(1)) can act to shield social media platforms from liability related to certain types of third party content, including user-generated content. In other words, any "provider or user" of an "interactive computer service" cannot be treated as the "publisher or speaker" of any information provided by "another information content provider". In practice this could include a user's Tweets or video content uploaded to YouTube. Online platforms are thus exempt from liability for cyberbullying incidents that take place on their platforms. The expansive "Good Samaritan" immunity has extended to the protection of "interactive computer service" providers from claims of, inter alia, defamation (considered the prototypical cause of action in this area of law), discriminatory housing advertisements, negligence, violation of anti-sex-trafficking laws (however note discussion below under 'liability of intermediaries') and public nuisance. It is noted however that the policies of the social media platforms against cyberbullying and the mechanisms of their enforcement include extensive involvement with content, which can put their intermediary status into question (Milosevich, 2016 pg. 2).

1.1.3. Summary conclusion

The responses to cyberbullying either rely on criminal sanctions, the availability of civil liability laws, or the cooperation of the platforms which host material. Undoubtedly however, the most common (and readily available) response is a criminal justice one. Where criminal laws apply to cyberbullying, they may be remedial, retributive, or used as a deterrent for young people (Chan, 2009; p. 157). The appropriateness of a heavy reliance on criminal remedies is worth questioning in circumstances where perpetrators are likely to be children, particularly given that in a number of countries criminal responsibility commences from as young as 10 or 12 years of age[29], and where a reliance on a criminal justice response risks the criminalising of young children.

Simply having a sanction as a deterrent has not been seen as sufficient for changing behaviours, and addressing cyberbullying is likely to require responses that are developmentally appropriate, which incorporate education for children and parents on digital citizenry, and, where sanctions are involved, they are used to deter without being unnecessarily punitive (Spears, et al., 2014; p. 11, 50). In addition, despite the previously noted uncertainty around how to define cyberbullying, there is increasing consensus that policies and rules to prevent cyberbullying should not be seen separately but rather within the context of traditional bullying. Successful interventions to tackle traditional bullying may therefore also reduce cyberbullying (Livingstone, Stoilova and Kelly, 2016)[30].

Other researchers have noted that levels of digital literacy can have an effect both on perpetrators and victims, for example reporting that a greater level of digital literacy in the hands of a cyberbully, may help create the power imbalance which is inherent in many forms of bullying (Görzig & Machackova, 2015). This power imbalance could arise out of the social and cultural background of those involved, and highlights the importance of balancing legal responses with community awareness and education initiatives which not only aim to ensure digital literacy across the board, but which take into account the individual, social and cultural background of those targeted for such initiatives (Görzig & Machackova, 2015).

Other initiatives are clearly also important in this space. Technology oriented solutions may be able to complement traditional approaches (Livingstone et al, 2016b) and warrant consideration. Moves to place civil liability at the hands of social media and Internet platforms are as yet very much in their infancy, but may yet prove effective in holding these platforms more responsible and accountable, and consequently help in effecting change.

1.1.4. Legal responses to sexting

'Sexting' refers to the exchange of sexual messages and, as mobile devices become more accessible, is a rising online phenomenon. 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 risk in the digital environment where the narrow conceptualising of laws and frameworks means that the responses are not sufficiently able to address the risks, and can in fact prove counter-productive (Byrne & Burton, 2017, p47).

Whilst, 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 in the digital environment and remain there permanently. This fact contributes to a complicated legal environment with regards to 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; p. 80; Byrne & Burton, 2017; p. 47). 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. For example in the state of Washington in the US, convicting a child of sending child pornography material (including a picture of themselves) would result in compulsory registration of the child for 10 years on a sex offender register. This requires complying with registration requirements such as keeping police informed of any change in address, and of any change in work or schooling[31].

In South Africa, for example, the provisions of the Film and Publications Act (Act 65 of 1996) can result in children of any age who take and share sexual images of themselves being prosecuted for the production and distribution of child pornography. In 2017, it was noted that under these laws a number of charges have been brought, albeit each being successfully challenged before a court (Byrne & Burton, 2017; p. 47). In the US, a variety of charges have been laid, and in some cases upheld by appeals courts. In 2010, in Indiana, a 13 year old girl and a 12 year old boy were charged with child exploitation and the possession of child pornography for sending nude images to each other. In Pennsylvania, a prosecutor is reported to have charged 10 minors in two sexting cases in 2010, and in Florida a 16 year old girl was convicted of 'producing, directing or promoting a photograph or representation that she knew included sexual conduct of a child', after she and her 17 year old boyfriend took nude pictures of themselves engaged in sexual conduct and emailed them to each other – this decision was upheld by an appeals court (Thompson, 2014; p. 13, 14). In the United Kingdom, it has been reported that thousands of children have been investigated for sexting – including in one case a five year old boy, and in another a 10 year old boy who received a caution. In one instance, a 12 year old girl who was reported to be groomed online, was reportedly told by police that she may face criminal charges and a criminal record for the creating and sharing of explicit images of a child, despite herself being a victim of grooming[32].

Compounding this, is a lack of general awareness on the behalf of children and young people that they may face such criminal charges should they engage in underage sexting (Strohmaier, et al., 2014). Additionally, where awareness does exist, it has been found to only have a moderate deterrent effect (Strohmaier, et al., 2014). At least one jurisdiction has amended their laws to remove criminality from acts of sexting between consenting teens. In the state of New Mexico in the US, a law was introduced in 2016 which legalised sexting between consenting teens aged 14 to 18, and therefore removed any risk of child pornography charges[33].

At the European level, on 6 June 2019 the Lanzarote Committee (Committee of the parties to the Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse – see further under 'International Policy Making') issued an opinion on 'child sexually suggestive or explicit images and/or videos generated shared or received by children'[34]. The Opinion concluded that where children generate, receive or share sexual images of themselves, they should not be considered to be in possession of child pornography; and that whilst the practice of sexting is not endorsed by the Committee, its recommendation aims to ensure that the child's best interest is always the primary consideration in any response.

The Opinion provides guidance to States on how to address the challenges which arise out of sexting, including that: where the image is generated by particularly vulnerable children (*i.e* very young, children with a disability) or a child is exploited, the child should be referred to victim support and not subject to prosecution; that self-generated images (or the possession of same) should not amount to the production / possession of child pornography; and that where a child may intentionally act to obtain, store or share another child's self-generated image, and criminal prosecution is considered it should be only used as a last resort, with priority given to using more appropriate methods of dealing with harmful behaviour (*i.e.* educational or therapeutic methods).

From the perspective of the countries responding to the OECD survey, whilst sexting as an issue was raised as a concern by a number of countries as an emerging risk, few indicated that they had laws aimed at specifically addressing these issues to protect minors, exceptions being Spain and Mexico. Spain has a law (not age specific), which criminalises the on-transfer to a third person initially consensually transferred images or recordings. This offence is aggravated if the victim is a minor (or otherwise a vulnerable person)[35]. Mexico indicated that the country was in the process of implementing laws that address criminal behaviours which occur with (or through) technology, a move which (among other issues such as cyberbullying) covers sexting, but is not specific to it. At the same time, Mexico indicated that the government has partnered with NGO's on specific campaigns, including one on sexting.

Whilst the risks associated with the criminalising of sexting has been discussed, sexting also has the potential to be very harmful to children's privacy and their mental health. Sexual pictures can spread quickly in the digital environment and remain there permanently. However, even in this space there is disagreement with regards 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 & Görzig, 2014; p.3; Gillespie, 2013)

Some recent research on sexting was presented at the Zurich 2018 Workshop – research which is valuable both from the perspective of understanding the issues underlying sexting, but is additionally a more generally promising research practice as it seeks to understand the specific ways that harms are manifesting (OECD, 2019). More research of this kind (across the spectrum of issues) would likely be valuable in identifying solutions. This research undertaken in Canada by Media Smart (Canada's Centre for Digital and Media Literacy) considered the behaviours and attitudes of Canadian Youth and looked specifically at the issue of non-consensual sharing of intimate images. The study considered the issue from the standpoint that it is not the consensual sending of sexts which cause harm, but rather the sharing of these images – which can reach a wider audience. The study found that sending sexts are less common than many people believe (whilst 93% of youth thought their friends had sent sexts, in fact only 41% had) and more youth received sexts (solicited, unsolicited and on-shared) than had sent them. According to the authors, the findings support a distinction between sending and receiving, and the non-consensual sharing of such images and text; and consequently, a distinction between how educators and parents (and policy makers) should deal with the two issues (Johnson. et. al., 2018).

Two notable aspects arise from this research, and the presentation given at the Zurich workshop. Firstly, it was found that youth that accept traditional gender stereotypes have a significantly higher tendency to share sexts. Half of those who had the highest beliefs in traditional gender stereotypes, had shared a sext and were also more likely to believe in rape-myths and tolerate or even participate in sexual harassment. Boys who accept traditional gender stereotypes were much more likely to share sexts than girls who shared 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 were found to play a significant role in the 'culture of sharing'. (Johnson. et. al., 2018, p. 12, 13).

Secondly, the researchers found a certain level of moral disengagement in those youth who share sexts, as a way to justify or excuse their behaviour. This 'moral blind spot' has four moral disengagement mechanism: *1)* Justifying an action (66% of participants agreed that when a girl's sext is shared, it shows other girls the risk)*; 2)* Denying the harm (14% of participants agreed that sharing sexts is so common, that nobody cares about it); *3)* Shifting of responsibility (38% of participants agreed that there is nothing that you can do to help when a sext is passed around); and *4)* Blaming the victim (43% of participants agreed that it's a girls fault if she sends a sext and it gets shared around).

A number of key recommendations of relevance to policy makers came out of this research and were presented at the Zurich Workshop. Namely that:

There should be a focus on publicising accurate information. Even though rates may be rising, they are lower than youth believe;

The moral aspect of sharing sexts needs to be addressed, and victim blaming needs to be avoided. A culture of abstinence was not seen to be effective, and in fact reinforced gender stereotyping, by minimising the role and responsibility of the sharer, and placing primary blame on the victim;

Measures to address gender stereotyping should focus on boys, as this is where gender stereotyping was seen to have the strongest effect;

Targeted interventions should be delivered to heavy sharers (and heavy sexters); and

Laws should be framed as a tool to help victims to take control of their lives after having had a sext shared.

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 on-sharing of the images and associated consequences? It has been suggested that certain groups are more likely to experience harm from receiving sexual messages – girls, younger children, and those who face psychological difficulties; and that accordingly policy responses should be aimed at ameliorating harm to these groups (Livingstone & Görzig, 2014; p.13). 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 providing measures which can support young people when they are in fact harmed by an act of sexting, or effective preventative measures.

1.1.5. Legal responses to sextortion

Sextortion is a new type of exploitation of adolescents in the digital environment that is being identified by the media, law enforcement and policy makers. A number countries responding to the survey raised sextortion as a new and emerging risk. Latvia, for example, indicated that a rise in sextortion cases had been seen in the country. Whilst concerns regarding the naked images of adolescents may fall into other categories such as sexting, and/or the sharing of sexual images non-consensually (often for a bullying or 'revenge porn' purpose) may be seen as a separate risk, 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., 2017; p. 72, 73).

Interpol[36] defines sextortion as, "*blackmail in which sexual information or images are used to extort sexual favours and/or money from the victim*", often at the hands of organised gangs, who may use malware to hack webcams and obtain naked images of victims, or entice the sending of the initial images via fraudulent representation. These kinds of actions often occur across borders, adding another layer of complexity to identifying both the appropriate psychosocial and legal response (Dinh, et al., 2016; p. 52). The perpetrator is not however always unknown to the victim with one study (sample size of 1550) finding that in most cases (greater than 60%) the perpetrators knew the victims in person (with the remaining perpetrators having met the victims through the digital environment) (Wolak, et al., 2017; p. 77).

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., 2017; p 73).

Presently, there is a lack of empirical evidence on the prevalence of sextortion. Whilst a 2016 report by the US Department of Justice[37] (based on survey responses from more than 1,000 law enforcement investigators and related practitioners) found sextortion to be the most significantly increasing type of child exploitation in the digital environment, the report did not include estimates of numbers of cases or victims (Wolak, et al., 2017; p 73). This lack of evidence makes it difficult to comment on: whether or not current legislative responses that rely on applying the provisions of existing offences are effective; whether or not a specific legislative response is required; and to what extent the phenomena actually poses a significant risk to minors.

Nonetheless, anecdotal accounts and early research attempts clearly show sextortion to be a rising concern. The FBI identifies a number of cases where children have been victims of sextortion[38], and in 2017 a Scottish child protection expert made a public call for suicide prevention plans to be automatically put in place for young victims of webcam extortion[39]. In 2013, a 17-year-old UK teenager committed suicide after being the victim of sextortion[40]. In response to the OECD survey, a number of countries indicated that they considered sextortion to be a prominent issue or a new and emerging risk (*e.g.* Belgium, Italy, Mexico, Norway and the US), however no countries indicated that they have specific laws in this regard. Additionally, sextortion has been flagged by children's helplines as an emerging concern, with a number of helplines indicating that there has been a rise in reports received on this issue (Dinh, et al., 2016; p. 52). Belgium's helpline, Child Focus, has particularly noted a rise in sextortion cases, and has identified a need for appropriate tools to respond to this concern, such as guidelines or the identification of best practices (Dinh, et al., 2016; p. 18).

1.1.6. Liability of intermediaries

The extent to which intermediaries (*e.g.* the websites, or social media companies who may host harmful content) may be held liable for harm, has – in line with the increasing manner in which persons (including minors) live their lives in the digital environment – become an increasingly more visible issue. This is particularly demonstrated by the US Government's prosecution of the online classifieds website Backpage.com ('Backpage'), and the resulting legislative steps taken to ensure that legal frameworks relating to the responsibility of online intermediaries do not serve to shield providers of digital services from responsibility for harms related to online sex trafficking.

In 2018, the United States enacted the Allow States and Victims to Fight Online Sex Trafficking Act (FOSTA). This law gives state and local prosecutors the ability to bring charges against sites which have facilitated prostitution and sex trafficking, and also permits civil suits against such sites for facilitating sex trafficking. In this regard, the law removes the protections that section 230 of the CDA had given them against third party liability (see paragraph 57 for a discussion of this protection).

Since around 2011, significant public advocacy and public awareness actions began to occur regarding traffickers using online classified websites to place advertisements seeking customers for commercial sex. The children (and adults) appearing in the advertisements were often victims of sex trafficking. Backpage, was arguably the main target of such actions, and was the subject of a number of lawsuits and a senate enquiry (see Box 1). The legislation mentioned above was enacted subsequent to this enquiry, and in response to findings that Backpage, which actively facilitated sex trafficking - including trafficking of children, was shielded from liability.

Box 1. Backpage.com's facilitation of online sex trafficking

Operating in at least 97 countries across the globe, Backpage was once the world's second largest classified site, and became the subject of a US Senate investigation in 2016, due to sex ads hosted on its 'adult ads' section which depicted sex trafficking victims, including boys and girls. The report found that Backpage was involved in 73% of cases of suspected trafficking in the US, and was actively facilitating and profiting from online child sex trafficking. It was further found that in the Philippines the company was using a proxy company to seek out commercial sex advertisers, by contacting those people who posted sexually explicit ads on rival sites, and offering them free advertising on Backpage. A significant amount of Backpage's profits arose from this advertising. Although a number of their services were free, 'adult services' are paid ads. Accordingly, they were found to be profiting from child sex trafficking. Despite these findings, section 230 of the CDA had acted to shield Backpage from any liability before the courts.

Indeed, a number of legal cases had been brought in an attempt to hold the website liable. At the same time, Backpage itself had brought a number of actions against state legislatures who had sought to enact laws that would create a liability and act to force the shutdown of the website's adult services advertisements. In all cases backpage.com was successful.

In M.A. v Village Voice Media LLC, claims that Backpage had knowledge that advertisements were for prostitution and illegal sexual contact with minors, were dismissed as the requisite intent to assist others in committing a crime could not be established. In Backpage.com v. McKenna et al (2012) Backpage sought to overturn a Washington law which made advertising the commercial sexual abuse of a minor a felony offense. The relevant District Court, held that the law was unconstitutional (violating the commerce clause) and that escort ads were permissible free speech. A similar outcome was held in Backpage.com, LLC v. Cooper where a Texas law was likewise held incompatible with the freedom of speech and that imposing a presumption of illegality across all such ads, would impose an impossible burden on websites to review all ads, or shut down adult services entirely. A New Jersey law seeking to target third party advertising, and remove the immunity of websites, was similarly found to be unconstitutional and a violation of s230 of the CDA . In 2015, another attempt was made to pursue liability against Backpage, with specific allegations made that the design of the website was intended to promote the illicit sex trade, and the trafficking of children. Again, it was held that liability was precluded by s230 of the CDA.

A Senate investigation carried out over a period of 20 months eventually found in 2017 that Backpage knowingly concealed evidence of criminality by systematically editing its 'adult' ads, via instructing moderators to edit their text to conceal their true nature and that Backpage knew it was facilitating prostitution and child sex trafficking .

Ultimately, the result of this investigation was the passing of the FOSTA to amend the CDA. This law permits state criminal action against websites and tech platforms that intentionally facilitate prostitution or sex trafficking, as well as civil action against such entities for facilitating sex trafficking.

To some extent the aforementioned US laws have since triggered significant debate on how to address online sex trafficking. Some groups, namely the Electronic Frontier Foundation ('EFF') contend that the laws will do nothing to stop sex traffickers, but will instead force online platforms to restrict user content more forcefully, silencing legitimate voices.[41].

The EFF contends that by removing the protection found in s.230 of the CDA, the government is actually removing useful tools for finding and stopping traffickers; and that by creating a threat of civil litigation, website operators may in fact be less likely to try and identify and report traffickers[42]. A viewpoint to some extent reflected in the United Kingdom, where Cyber Crime police Units report strategic closing of websites, weighing the benefit of closing the website down, with what assistance they can obtain from the website in identifying the traffickers[43].

However, this viewpoint in itself is controversial. Contending that allowing the sex trafficking of children through intermediaries to persist, so as to catch the main perpetrators is arguably highly irresponsible. Lawmakers and policy makers have a responsibility to ensure the protection of all citizens. To allow this harm of the most abhorrent type against some of the most vulnerable members of society to continue in the name of prevention is arguably highly harmful in itself.

1.1.7. Sex trafficking of children through online means is a real and growing international concern

A recent US study into the domestic sex trafficking of minors, found that as of 2015, 55% of victims surveyed indicated that they used text, websites or apps to be in contact with the traffickers, and it was through this medium that a relationship was built between the traffickers and their victims. Advertising for services, are also progressively moving more and more onto the digital environment, with the same study finding that 75% of the advertising for the trafficked children's 'services' occurred online[44]. In testimony to the US Senate's permanent subcommittee on Investigations (Human Trafficking Investigation hearing), in November 2015, the Senior Vice President of the National Centre for Missing and Exploited Children ('NCMEC') indicated that between 2010 and 2015, the NCMEC saw an 846% increase in reports of suspected child sex trafficking to their Cyber TipLine, an increase which the NCMEC said was directly correlated to the use of the Internet to sell children for sex[45]. The Latin American Coordinator of the anti-child trafficking group ECPAT, has noted that trafficking often starts in the digital environment, as recruiters seek to interact with children where they interact with their peers[46].

At the European Level, in 2018 the European Commission noted that, "*Victims are exploited in the sex and entertainment industry, facilitated by the rapid technological development and the use of internet for advertising services and the recruitment of victims.*"[47] Similarly, the Council of Europe has noted that, "*the prevention of human trafficking is closely linked to the on-line security of children. Recruiting victims through the Internet, via websites advertising jobs, dating sites or social media is a growing trend*"[48].

In their 2018 Global Report on Trafficking in Persons (at 38), the United Nations Office on Drugs and Crimes ('UNODC'), identified that the online domain has opened new pathways for traffickers to identify, contact and entrap victims. In one relevant example, the Report details a case were two traffickers from an Eastern European nation, working with other traffickers within and outside of their region, used social networks and online groups to approach girls, and lure victims. Through fake profiles, the traffickers joined online groups and advertised lucrative jobs in order to contact victims who aspired to work as models. Recruiting 100 girls, the traffickers used images the girls shared to coerce them into coming to a specified destination, where they were then sold to another trafficker, and eventually through a third trafficker coerced into prostitution. Payments were made via a mobile payment application, and the traffickers never met the girls – facilitating the whole process through the digital environment.

It is evident that the sex trafficking of children through digital means is a real and growing concern. Despite this, whilst there is a number of national laws and international instruments and laws in place that deal directly with traffickers[49], globally the capacity to ensure that the companies that provide the platform for these crimes, do not profit from them and do not perpetuate them is limited. The protections that were contained in s.230 of the CDA meant that victims were unable to seek redress, and prosecutors were not in a position to take action. The legal position in a number of other jurisdictions, does not appear to have been tested, however, and it may be that in other jurisdictions a similar legal shield to the one that applied under the CDA would be available.

In fact, in jurisdictions other than the US, the liability of websites operators for the information transmitted / provided on their sites, also appears to be limited. For example, the EU E-Commerce Directive, provides that were a service provider acts as a mere conduit (does not initiate the transmission; does not select the recipient; and does not select or modify the information) then they cannot be liable for the information transmitted[50]. This directive, *prima facie,* would seemingly provide exactly a CDA kind of protection for website operators.

In some common law countries, the likely liability of websites can be gleaned through an analysis of defamation laws. Both Australian and Canadian Courts, for example, have considered the issue of Google's liability in defamation cases – where Google was used as the conduit for the defamatory content. In Australia, a 2017 case[51] of the highest appellate court in one Australian state, found that the search engine, as a secondary publisher of a data with knowledge of the defamatory material, was liable. In a second case heard in the High Court (the highest appellate in the country), Google was again found to be capable of liability in the defamatory space[52]. In 2015, in Canada, the British Columbia Supreme Court similarly found that a liability would exist should a search engine fail to act after being made aware of the defamatory material[53]. However, it is noted that these actions are grounded in both country's defamation laws, and it is unclear exactly how the principles here would apply in a case such as the Backpage one.

In the United Kingdom, as previously noted, a White Paper on Online Harms was published in April 2019. In 2019, media reports also indicated that the Government was considering a number of regulatory options, including a code of practice, a statutory duty of care, and a statutory regulatory body. In Germany, the NetzDG[54] legislation creates an obligation on social media platforms to remove or block access to manifestly unlawful content within 24 hours of receiving a complaint about the content – or face significant fines. Whilst this legislation creates a capacity for the countries regulatory body to sanction social-media companies, it is not clear that it would cover the Backpage scenario. The legislation explicitly references a number of unlawful offences under the criminal code, of which none, *prima facie*, cover child sex trafficking (although it is noted child pornography is covered)[55].

Lastly, as noted at the Zurich Conference, whilst this is a growing concern across OECD countries, in the developing world this is also an acute concern. An example can be taken from India and the experience of WhatsApp – which has reportedly also been used to facilitate sex trafficking; and in the rapid spread of false or misleading information which has caused harm (and in extreme cases) the killing of persons through social media fuelled mob violence.

A number of cases of teen girls being both groomed through unsolicited contact over WhatsApp, with Facebook being used to obtain information about them, have been reported[56]. This method of recruitment is reportedly used, as it can cast a wide net, with the same message (a proclamation of love, or an offer of a job) being sent to several girls at once. Like the eastern European case described above, the traffickers in India were able to wholly recruit the girls through electronic means (in this case WhatsApp) without ever meeting them in person. Like Backpage, classified websites in India reportedly host advertisements for the services of sex workers, who may turn out to be victims of child sex trafficking. In 2017, the Delhi police reportedly discovered a trafficking racket (with some girls as young as 14) operating over social media[57]. In January 2019, WhatsApp placed a limit on the number of recipients per message (allowing only 5 forwards)[58].

1.1.8. 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 (at p. 17). Broadly speaking, these three subcategories persist today, although advances in technology have altered both the potential volume of this material, and the methods by which children may become exposed to it.

Four issues stand out as either new issues, or ones that have been amplified or changed in nature due to the advance of technology since 2011. These are: *i)* hate speech, which was an issue in 2011, but may have been amplified due to broader publishing of such content on social media platforms; *ii)* offensive material and harmful content, which has been greater explored and defined through research; *iii)* traditional broadcasting regulation, which has had to adapt to new methods of content being published online (*e.g.* streaming services, YouTube); and *iv)* fake news, which is a new and emerging risk since 2011.

1.1.9. Hateful content and hate propaganda

Hate crime occurs where an offence is motivated by the victim's race, religion, disability, sexual orientation or transgender identity. In 2015/2016, the United Kingdom saw its highest number ever of hate crime prosecutions. It has been observed that this kind of crime is increasingly conducted in the digital environment, and to some extent, it can cross over with offences relating to cyberbullying when social media is involved (for example, through harassment or stalking online, or the distribution of written or visual material). More generally, the Internet has enabled people to offend, insult or abuse others outside of a specific hate crime context[59].

The number of minors affected by exposure to hate content in the digital environment appears to be rising. In 2010, 12% of 11-16 year old reported that they had been exposed to hate content, in 2013 this had increased to 23% of children in this age group[60]. The UK's Communications Regulator reports that in 2017, 45% of children aged 12-15 years who go online reported seeing hateful content online over the previous year (Ofcom, 2017; p. 5). Itself an increase from 2016, when 34% of children in this age group made this report (Ofcom, 2016, p. 117). It is however 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 this and how to make a report (as also noted in the following section).

From an industry perspective, all major social media platforms have their own statements of rights and responsibilities or Terms of Services that explicitly deal with, *inter alia,* hate speech (which is variously defined), and which can result in either the refusal to publish material or material being removed. What the impacts of these self-regulatory measures are, however, remains unclear and this is a space where a need for further research has been identified (Alava, et al, 2017; p. 17).

On the legislative level, this conduct may fall within a country's criminal legislation, including through laws that covers hate crime in an offline space. For example, in response to the OECD Survey a few countries indicated that they had specific laws designed to deal with hate crimes and hate speech, sometimes explicitly applicable to online behaviour. Both Canada and Luxembourg indicated that they have specific legislation on the distribution of hateful content. Whilst Luxembourg's laws do not specifically relate to digital contact, in Canada the prohibition on communicating hate propaganda extends explicitly to online content. In the United Kingdom, it was reported that the sending, or causing to be sent, by a public electronic communication a message or material which is grossly offensive or menacing is prohibited. In Germany, the new NetzDG Act (mentioned above under cyberbullying), provides fines of up to 50 million euros (USD 61.4 million) for social media companies that do not take quick steps to remove hate speech from their platforms.

On a regional level, the European Commission entered into an agreement with Facebook, Twitter, Microsoft and YouTube in 2016 in the form of the European Union Code of Conduct on Countering Illegal Hate Speech Online[61]. Through this code of conduct these platforms agree to review all reports of hate speech online within a 24-hour time frame. Recent EU figures indicate that the companies managed to review complaints within a day in 81% of cases over a six-week monitoring period in late 2017[62].

1.1.10. Preventing exposure to offensive material and harmful content

Current research provides a helpful overview of the kinds of material that children are exposed to in the digital environment, which they themselves identify causes distress. Children have noted being bothered by a wide range of issues: online scams, pop-up adverts that were pornographic, hurtful behaviour, unpleasant or scary news or pictures, harassment or sexual harassment by strangers, and people sharing too much personal information online (Byrne et al., 2016; p. 58, 59). Children have also indicated that they may be exposed to pornography and violent content, which causes them shock and disgust. Primarily, video sharing services such as YouTube are sources of this kind of content (Livingstone, et al., 2014b; p. 271).

In 2014, across the EU 12% of 9-16 year olds had reported seeing a sexual image in the digital environment, and about the same percentage had seen websites where people discuss ways of physically hurting themselves (Livingstone, et al., 2014a). In the United Kingdom at least, this number had significantly increased by 2016, with one UK report finding that 47% of 11-16 year olds had seen pornography online (Martellozzo, et al., 2016).

In 2017, the UK's Communications Regulator identified that 17% of 8-11 year olds and 29% of 12-15 year olds say that they have seen content online that they find worrying or nasty; and one in ten 12-15 year olds have seen something online or on their phone of a sexual nature that made them feel uncomfortable. Nonetheless, it was also seen that many children are taking action in response – either telling someone about what they have seen, or making a formal report (Ofcom, 2017; p. 5).

Whilst in the response to the survey, issues such as these were more likely to be covered by efforts to assist parents in self-regulation, and/or through increasing the digital literacy of children, some countries did have legislative responses covering this field. In New Zealand the Harmful Digital Communications Act deals with (among other matters) both the sending and the publishing of offensive material. 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[63].

Lithuania's Law on Minor's protection explicitly seeks to protect children from public material which could have a detrimental effect, with detrimental effect defined as, "*information which may be harmful to a minor's mental or physical health, or physical, mental, spiritual or moral growth*". A Lithuanian court has the power to order the removal of such material and its Communications Regulatory Authority ('RRT') has investigative and directive authority in regards to this Law. The RRT can take action regarding offensive or dangerous material on social networks, and has reported (to Facebook) several groups engaged in promoting suicidal behaviour – which resulted in the groups being removed[64]. These laws however have been criticised by some human rights advocates as they could potentially be used for censoring free speech and having a discriminatory effect[65].

1.1.11. Fake news

Increasingly, a need is being identified of the importance of teaching children and young people to be able to distinguish between what is fact and what is fiction in information distributed through digital means. This is a particularly critical skill given that predominantly children and young people 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[66].

In 2017, a public broadcaster in the United Kingdom undertook a survey on consumer's capacity to identify "fake news". Of the people surveyed, only 4% were able to correctly identify what was real and what was fake[67]. In the same year, the UK's Communications Regulator identified that 73% of 12–15 year olds were aware of the concept of fake news, whilst 39% said that they had ever seen something online that thought was a fake news story (Ofcom, 2017; p. 130).

Whilst presently legislative responses do not appear to exist, or are emerging, some countries have taken policy or programmatic steps to try and address the issue of fake news, identifying media and digital literacy, and critical thinking skills as essential needs in this regard. The United Kingdom has indicated a commitment to ensuring that minor's 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[68]. Australia's e-safety commissioner has publically available information designed to help minors identify what is real and what is not on the Internet[69]. In Hungary in March 2019 as part of the European Media Literacy week took place (an initiative of the European Commission) the Hungarian National Media and Infocommunications Authority provided information and lesson plans on how to identify fake news[70].

Whilst undoubtedly the role of legislative and policy responses are essential in this space, it is also worthwhile considering what is the role and responsibility of the media (including social media) in educating the public (including minors) on the issue of digital literacy and developing critical thinking skills regarding "fake news". It may be that policy makers need to consider how the media may be able to play a role in this, and whether or not the media themselves are in a position of conflict which can create a risk for minor's education / awareness raising on these issues.

1.1.12. On demand and online entertainment and traditional content regulation rules

The number of sources providing entertainment content that is accessible by minors has expanded well beyond broadcast and cable networks to include a wide-range of streaming services and games which are readily available online and therefore potentially difficult to both classify and monitor. A recent study by the European Commission concluded that not only were children spending more time online, but that the digital environment (notably streaming services) have to a large extent replaced television as a source of information and entertainment[71].

Whilst a number of countries did not indicate, in response to the OECD Survey, that their content regulation laws have been specifically adapted to new media, some jurisdictions have taken steps to strengthen protections and to try to prevent minors from being exposed to inappropriate media.

For example, in the United Kingdom the Digital Economy Act 2017, requires that any commercially available pornographic material be 'not normally accessible to persons under the age of 18'[72]. This law also allows the regulator to take action against those who are providing 'extreme pornographic material', regardless of whether or not age verification is in place. Additionally, in the United Kingdom, on-demand program services must not contain any 'specially restricted material' (*e.g.* pornography) unless the material is made available in a manner which ensures that persons under 18 will not normally see or hear it[73]. In France, a specific law has been introduced to address the protection of minors regarding on-demand digital media services. This law requires the classification of programs, age verification, and a prohibition on broadcasting content likely to harm children[74].

The Russian Federation has legislation on the protection of children from information that is harmful to their health and development. This law sets rules for the dissemination of information to children, including through the digital environment, according to age brackets (0+,6+, 12+, 16+, 18+), and provides for expert reviews and evidence based decision making regarding classification around age limits.[75] Whilst *prima facie* these laws are promising from the point of view that they are intended to be evidence based, human rights organisations have raised concerns regarding the potential that they could be exploited to increase censorship in the country[76].

In addition to the above examples, a number of other countries have specific policies or programs aimed at extending traditional classification and broadcasting policy/rules to new media. In response to the OECD Survey, the Russian Federation cited a joint initiative between the Communications and Telecom Ministry and the Education and Science Ministry, which provides recommendations on what information should be restricted in schools; what information might cause harm to the health of children; and recommendations on how to reduce access to such information types. Sweden's Media Council - a government agency tasked with the protection of minors from harmful media influences, and empowering them as conscious media users - has a content regulation role, as well as an educative and research function which extends to protecting children from harmful online content[77].

The above laws are an example of ones which specifically aim to protect minors from inappropriate content in on-demand video services, and where efforts have been made to extend traditional regulatory efforts to new technologies. Nonetheless, such attempts have not occurred across the board, with Canada for example, indicating that the country's Broadcasting Act does not extend to regulating content on the Internet or to new media services.

At the regional European level, on 14 November 2018 the Audiovisual Media Services Directive ('the revised AVMSD') was enacted. The revised AVMSD, recognises the dramatic shift in the media landscape in the past decade and the significant increase in the consumption of digital content, particularly by young people. It both specifically considers the need to protect minors; and changing viewing habits – moving from TV screens, to portable devices; and changing from traditional broadcasts to video on demand services, video sharing platforms, video clips and user generated content.[78]

The revised AVMSD, specifically notes that video-sharing platforms, and social media services act as a medium to share information, to educate, and to entertain – including user generated material. Accordingly, these services are now included in the scope of the directive. Therefore, where measures exist for the protection of minors that are applicable to television broadcasting services, the directive requires that they also extend to on demand services. Specifically, the AVMSD requires member States to ensure that media services do not impair the physical, mental, or moral development of minors, with gratuitous violence and pornography being subject to the strictest measures.[79]

Whilst the discussion above, when considering online games, deals with the risks that may be associated with their substantive content (*e.g.* inappropriately violent or sexual content that would not otherwise be approved for children in traditional media), online gaming and the 'apps' that they may be hosted on are often associated with pop-up or targeted advertising. These two issues should be distinguished from one another. Whilst the former has been discussed above, the latter is discussed below.

1.1.13. Consumer related risks

In 2011, the OECD identified 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)" (at p. 25). 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. This in turn has implications regarding what needs to be addressed when ensuring the digital literacy of children, and that of their parents (Livingstone, et al., 2016; p. 23).

As has been noted by researchers, the digital world is a highly commercial world, which is a main motivating factor behind increased datafication and hyperconnectivity (as will be discussed below under 'Privacy'). Primarily economic interests drive a desire to better understand potential consumers, as then they may be better targeted. Children can be considered important targets for the marketing industry for three main reasons: more and more, children have money to spend, they may influence their families spending, and they are future consumers. (Van Der Hoff, 2017; p. 415, 416)

Children may thus be exposed to targeted advertising online through various products such as banners, sponsored google search results, or advertising in YouTube videos. Online gaming is popular among children. For example, a 2018 Pew Research Center survey on the use of social media and technology in the US suggests that overall, 84% of teens say they have or have had access to a game console at home, and 90% say they play video games of any kind (whether on a computer, game console or cellphone)[80]. These percentages are even higher among boys, with roughly 97% of boys indicating that they play online video games in some form or fashion.

Most of these games also offer a platform for advertising[81]. In addition to advertising, apps and games may present a direct financial risk with in-app purchases often being offered to children (sometimes as an enticement to complete a game faster), or games themselves may be an advertisement – so called 'advergames' - which are specifically designed for advertising and for the marketing of a specific brand or product[82]. A 2016 EU Study of 25 of the most popular online games revealed that all advergames, all social media games, and half of all games available through application platforms contained embedded or contextual advertisements. A common feature was an ability to pay to remove advertising, or to accelerate the game[83].

A 2018 study that reviewed 135 Apps on the Google Play App store aimed at children aged between 12 months, and 5 years, found that 95% of the apps contained at least one advertisement. These included: the use of a known commercial character (42%); prompts to update to a full version of the app (67%); ad videos interrupting play (35% of all apps, 54% of free apps); in-app purchases (30% of all apps, 41% of free apps); prompts to rate the app (28%); share on social media (14%); distracting ads, *i.e.* banners (17%); or hidden ads with characters disguised as game play (7%). Overall the study found high rates of mobile advertising, using manipulative and disruptive methods. (Meyer, et. al., 2019) Despite these concerns there does not appear to be a prominent legislative response to these risks. In answer to the OECD survey, with some exceptions, 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. Nonetheless, some rules/guidance do exist regarding how existing consumer protection rules should apply to in-app purchasing. For example the UK in-app purchasing guide issued by the Office of Fair Trading[84], largely provides that existing rules apply to the app-environment; as does the International Chamber of Commerce's advertising code[85].

In Mexico, consumer protection laws prohibit marketing or publicity strategies that may mislead vulnerable members of the community, including children. In the US, a major purpose of the Children's Online Privacy Protection Act (COPPA) of 1998 is to limit advertising targeted to children (under 13 years) by prohibiting the collection, use, and dissemination of personal information from these children without informed, advance parental consent. COPPA places an obligation on the operators of websites to obtain verifiable parental consent prior to collecting personal information from children in this age group, as will be discussed below under privacy. The US Federal Trade Commission's ('FTC') enforcement efforts in regulating advertising to children has, however, been subject to some criticisms. COPPA applies only to websites and online services that are directed to children less than 13 years of age or where the operator has actual knowledge that the person using the service is younger than that age. Additionally, it can sometimes be difficult to tell whether a service is child-directed; children may lie about their birthdate; they frequently use websites or digital services that are intended for general audiences; and it is difficult to tell whether operators have "actual knowledge" that their users are child users (Campbell, A, 2017 pg. 26-27). These are however criticisms that the FTC has sought to address. Namely, a 2013 rule review (among other matters) specifically extended the definition of the operator of a website to modify the definition, and to make it clear that the rule equally applies to those child directed services which integrate outside services (such as plug-ins or advertising networks) that collect personal information from users[86].

Additionally, the FTC has had success through litigation in holding industry to account. The app Musical.ly (now known as Tik Tok), is an online music library featuring tracks popular with teens and younger children. Users create videos which they can then share publically, and other users can comment, and/or follow users to see more of their videos. To register for the app, users provided their email address, phone number, full name, user name, profile picture and a short bio. By default, profiles were public. For the first three years of operation the company did not ask for the users' name. They commenced doing so in July

2017 (and consequently then prevented persons who say they are under 13 years of age from creating an account), however they did not seek age information from existing users. Accordingly, the FTC posited that the app was acting in violation of COPPA, and succeeded in obtaining a $5.7 million civil penalty from the company, and agreement that they would change their practices to ensure COPPA compliance[87].

A March 2016 European Commission report found that the current regulatory regime is not providing children with sufficient protection from the adverse effects of online marketing. Two years later, a 2018 mapping of the Safer Internet Centres across the EU (see under 'Regional Policy Making' for further detail about the centres) found limited evidence of initiatives dealing with commercial risks associated with children's use of the Internet. In this study, only a third of the countries mapped (31 in total) said that their awareness centres had any activity related to compliance with national laws that covered profiling and behavioural advertising. Whilst 38% of countries said there was an activity to support the development of industry codes of conduct regarding inappropriate advertising online and self-regulatory bodies[88], only a quarter of them indicated that they monitored the implementation of such measures (O'Neill & Dinh, 2018; p. 62).

1.1.14. Privacy risks

Legal responses 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 comprehend these typologies in terms of their privacy. The following box, demonstrates the different types of data, adapted by researchers from the London School of Economics.

Box 2. The different types of data

- 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.

Source : Livingstone, et al., 2018a; p. 3.

Expanding upon the above, it can be said that 'data given' is that information given, or published consciously. For example, when opening an account for an online game, a child or young person may provide their email address, payment details, birth dates, etc. Data given also encompasses such things as sharing creative content online, *i.e.* pictures or videos that may be shared across various media. When sharing this data, the child or young person is likely to have thought about this data, and where it is going; and with whom they are choosing to share the data (family, friends, etc.) (Van Der Hoff, 2017; p. 412).

Data traces on the other hand, is personal data that is unknowingly, or unconsciously left behind, simply through the act of being online. When a person interacts in the digital environment, the simple act of moving from website to website, from search engines to online stores, to social media - leaves behind data traces. This is also known as behavioural data. Technologies - such as cookies, web beacons, device/browser fingerprinting, etc. – can be used to meticulously document how individuals behave in the digital environment. Apps and other online services cover a wide range of aspects of a person's life, and these apps may be sharing data both with the companies that own/distribute the app, and with third parties.

These data traces may consist of content (social media posts, pictures, videos, etc.) and also of metadata. Metadata includes such information as how much a phone is used, calling patterns, social connections and other location data (Van Der Hoff, 2017; p. 412, 413).

Inferred data, is therefore data that can be gleaned from these other forms of data. Both data given, and data traces may be captured, processed and analysed resulting in the acquisition of knowledge about a person, simply due to their behavioural patterns online. A 2014 Stanford study, found that analysing telephone metadata, had the capacity to produce extremely sensitive results about a person, for example: medical information; political and religious associations; and sexual interests (Van Der Hoff, 2017; p. 414).

Research has shown that whilst children are aware that they may have contributed data about themselves or about others as a result of their activities in the digital environment, the extent to which they understand the consequences for their privacy will depend upon the child's own understanding of interpersonal relationships, which in turn depends on the child's 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, et al., 2018a; p.3).

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 invent of 'smart connected toys' creates more opportunities for children's data to be collected and used – often in a manner contrary to the protections designed to safeguard the privacy of children in this regard. Two recent examples demonstrate this, and are discussed in the box below. The first is a Californian study which considered the collection of children personal identifiers by apps which are designed for children; and the second centres on concerns raised regarding the potential for serious privacy violations arising out of the use of smart toys.

Box 3. Emerging privacy and data protection challenges

Privacy risks of connected smart toys

Growth in hyper-connectivity, and the advent of the Internet of Things (IoT), has meant that increasingly, both people and objects are continuously connected. Whilst these smart devices are designed to make people's lives easier, they also come with the capacity, and the design, to track and predict the behaviour of users (Van Der Hoff, 2017; p. 414, 415). Connected devices, are increasingly meant specifically for children, such as smart toys. In 2015, Mattel launched 'Hello Barbie', which has the capacity to record and analyse children's conversations to find out about their preferences and interests. In response, the Campaign for a Commercial-Free Childhood launched a campaign against the toy, seeking to raise public awareness of risks associated with the toy[89].

Similarly, the Norwegian Consumer Council ('NCC') has highlighted the risks associated with internet connected toys, and smart watches[90] designed for children. Specifically, the NCC studied at the toys 'Cayla' and 'i-Que' –which are manufactured by a company in the US, paired with companion apps, and distributed across Europe, Asia, the Middle East, Australia and the United States. The NCC found that these devices: i) lacked simple security, allowing anyone to take control of the toy via a mobile phone and consequently listen and communicate through the toy; ii) that the user terms regarding the use of personal data for targeted advertisement were likely in breach of a number of EU Directives (data protection, unfair contract terms, and toy safety); iii) that anything the child tells the doll, is transferred to a US based, speech recognition company who reserves the right to share this information with third parties, and to otherwise use the data; and iv) hidden marketing is embedded in the toys.[91] Some guidance regarding connected toys is available for French parents and carers, through the website of the French data protection authority[92].

Mobile apps' compliance with the Children's Online Privacy Protection Act (COPPA)

In 2018, researchers at Berkeley analysed 5,855 Android apps, for compliance with the United States Children's Online Privacy Protection Act (COPPA). The Apps analysed were drawn from the ranks of popular free children's apps, and the majority were found to be potentially in violation of COPPA, through their software development platforms (SDPs). While a number of the platforms hosting the apps had configuration options in place to allow COPPA to be respected (through the disabling of tracking and behavioural advertising), the researchers found that a majority of the apps either did not make use of these tools, or used them incorrectly. 19% of the apps analysed were observed to collect identifiers or other personally identifiable information, in direct contravention of their terms of service with their SDPs (Reyes, et. al., 2018).

A 2017 report of the International Working Group on Data Protection in Telecommunications (of the International Conference of Data Protection & Privacy Commissioners - ICDPPC)[93] and the 2018 Resolution on eLearning Platforms of the ICDPPC's Digital Education Working Group[94] further highlight the above concerns. Generally, both of these reports highlight a lack of transparency in terms of use and privacy policies (using vague language around the use, scope, purpose, and length of retention of collected data). Policies were also found to reserve the right to change the terms at any time – hampering capacity for user control, and respect for basic principles of privacy and data protection. It is further highlighted that security flaws in smart devices for children (and/or in accompanying apps) have allowed for hackers to access sensitive information such as photos, videos and geolocation. Additionally, smart watches have been found to have the capacity to (and have been used to) eavesdrop on teachers during lessons[95].

1.1.15. Legal and policy responses

At the national level, almost all countries responded that their privacy laws act to protect children in some way, although issues relating to consent, to the processing of data, and the breaches of these laws may differ. As was the case in the 2011, information privacy and information security risks are for the most part covered by general data protection rules, and criminal laws as some information security risks are rendered as an offence.

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 in the digital environment. For example, the Office of the Australian Information Commissioner ('OAIC') is responsible for disseminating knowledge of the government's guidelines and principles regarding privacy awareness, has regulatory powers to investigate complaints, and to enforce compliance with Australia's privacy principles. Mexico's National Institute for Transparency, Access to Information and Personal Data Protection ('INAI') is tasked with the compliance of transparency and data protection laws and is active in the space of online protection. Mexico indicated that the INAI has entered into a number of partnerships and initiatives to specifically address the protection of children in the digital environment, including initiatives that extend beyond the privacy space. For example, the INAI collaborates with the Secretariat of Public Education to integrate digital technology into schools.

Across the EU, whilst most EU countries provided responses in the 2017 OECD Survey that gave details relating to their privacy regimes, it should be noted that these countries will now be subject to the provisions of the General Data Protection Regulation (EU) 2016/679 ('GDPR'), and so there may be some change in their legislative framework. Accordingly, the laws of European countries subject to the GDPR, 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[96]. Additionally, the GDPR places an obligation on data protection authorities to promote public awareness and understanding of the risks, rules, safeguards and rights relating to the processing of personal data, especially the processing of personal data relating to children[97]. In December 2018, the Irish Data Protection Commission launched a public consultation (including a child friendly version) on the processing of children's personal data and the rights of children as data subjects under the GDPR[98], with a view to publishing guidance material on the processing of data both for both organisations who process data and the children themselves[99].

It has been pointed out, that whilst the rationale behind this special protection for children is sound, in practice there remains a gap in the empirical evidence underlying it. Namely, there is an evidence gap in understanding the level of children's media literacy and the extent to which they are aware of the risks associated with the processing of personal data; of the potential harm; and of the ability of families to take a protective role (do parents have the requisite media literacy, children's need for privacy from their parents) (Livingstone, 2017; p. 19; 2018 Zurich workshop).

The UK's 2018 Data Protection Act (which implements the GDPR at the UK domestic level) includes a provision requiring the introduction of an Age Appropriate Design Code. This code was launched in April 2019 and after a period of consultation (which ran until 31 May 2019) is expected to become law after any consequent amendments are made and it is laid before parliament. This code provides requirements that online services must meet in order to make their services available for children; with compliance monitored by the Information Commissioners Office. Whilst it does not appear on the face of the code that non-compliance in itself will lead to a sanction, it is likely that non-compliance may hinder an online service's capacity to show that their processing is fair and complies with the GDPR, and the Information Commissioner's Office does have power to issue warnings, reprimands, stop-now orders and fines for GDPR breaches[100].

The provisions in the draft code require online services to: provide an age appropriate service; be transparent (*i.e.* allow children to understand the information presented to them); uphold community standards, and the providers own published terms of service; ensure geolocation tracking is off by default for children; and to ensure the safety, security and privacy of children where smart or connected devices are used in the home. The draft code also provides a number of negative obligations such as: prohibitions on using 'nudge techniques' which seek to lead or encourage children to provide unnecessary personal data or to weaken / turn off privacy protections; from promoting online behaviour that is detrimental to a child's health; and from using profiling to make recommendations to children based on their browsing history[101].

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 AVMSD, with its article 6a(2) providing that the personal data of minors collected or otherwise generated by media services is not to be processed for commercial purpose, such as direct marketing, profiling and behaviourally targeted advertising. Again, this is a relevantly new provision and it will take time to see its efficacy in practice.

The United States continues to operate the aforementioned COPPA law. This legislation was amended in 2013, creating a 'new Rule' designed to update terminology, strengthen consent provisions, change information provision requirements, and strengthen confidentiality and oversight. The previous provisions for obtaining parental consent had been criticised for being easy to circumvent (*i.e.* sending an email from the parents email address, providing the parents credit card details, a written consent, or a phone call from the parent) (OECD, 2011; p. 66). The amended methods for obtaining consent in the new Rule, seem to take advantage of technology, but not necessarily address the abovementioned issue, with the exception of allowing for videoconferencing. (Other new methods include: electronic scans of signed parental consent forms, use of government-issued ID, and alternative payment systems – assuming they meet the same stringent criteria as credit cards). The amendment expands the definition of a website or online service to include plug-ins or ad networks, and the definition of personal information, now includes geolocation information, photos, videos, and audio files. The amendment also strengthens rules around provisions of information to third parties, and monitoring.[102]

Outside of the European and US example, in Australia, consent for the sharing of personal information is required for children of less than 15 years. Canada, requires consent from the subject of the information themselves – a move designed to protect the rights of children and other vulnerable persons. Although the Canadian legislation does not specifically reference children, it does require that consent be fully informed– implying a need to use child friendly and appropriate language in seeking consent, and an implicit ban to obtaining consent from children of a very young age.

Mexico's privacy laws positively require that the best interests of the child be a primary consideration when processing the personal data of minors; provides that the general civil law rules of the country regarding capacity and legal tutorship/guardianship apply when obtaining consent; and mandates that a minors privacy will be considered violated if the treatment of their image by the media impairs their honour or reputation.

A few countries criminalise violations of a child's privacy. For example, Austria's penal code protects children from being recorded (audio or video) without their consent although arguably this is a protection geared towards preventing child pornography (and not necessarily the risks the focus of this report) as the offence is aggravated if it is sexual in nature. At the time of responding to the OECD Survey, Sweden indicated a plan to introduce legislation that will impose penalties for the violation of privacy when spreading images intended to cause tangible harm.

Internationally, The Digital Education Working Group of the International Conference of Data Protection & Privacy Commissioners (ICDPPC) conducted a survey in 2017, to identify what policies, safeguards and/or provisions were in place to protect the personal data of students by both data protection and educational authorities. This survey found that data being collected, used and disclosed on educational service platforms are both diverse and high in volume. Whilst the purposes for collecting data here, had clear linkages with an educational context, responses indicated that additional research was needed into the secondary uses of data (for example, advertising) and the varied mechanisms and frameworks for consent[103]. Following on from this 2017 survey, the Digital Education Working Group of the ICDPPC developed an International Resolution on eLearning platforms aimed at educators and service providers, which was adopted in 2018. The recommendations made seek to allow educational digital practices to be developed in schools, but also aim to guarantee effective data protection regarding the digital services offered to pupils and teachers, whilst also respecting the rights of pupils, parents and educators. At the time of publishing this report, it is understood that current work on this resolution is focussing on sharing experiences of national implementation of the Resolution on eLearning platforms, and creating an inventory of any recommendation guides or codes of practice which have been drawn up by authorities as a result of (or which address) the resolution.

It is, however, further recognised that poorly thought out or strictly applied laws may also have unintended consequences and detrimental effects, similar to the discussion on sexting. As an illustration, the Future of Privacy Forum in the US, points out that whilst 39 states and Washington DC, have passed 123 new privacy laws since 2013, this extensive legislative reform has been unaccompanied by the requisite funding and training needed to properly implement the laws. Additionally– it is reported that one state's laws by requiring that parents opt in to almost all data sharing, has resulted in schools being unable to share student artworks, announce the names of football players, or even pass on student details on the purpose of scholarships[104].

In the education space, further concerns around privacy arise out of the increasingly popular use of e-learning platforms. These platforms enable the creation of virtual classrooms where teachers can distribute materials and conduct tests – they also often allow pupils and teachers to communicate with each other. The use of these platforms, extends the range of data collected regarding minors from simply test results and attendance information to more nuanced information on how teaching materials are used tasks fulfilled – paving the way for personal data about learning behaviour to be gleaned.

1.1.16. Conclusions / observations

The legislative response is wide-ranging, largely made up of legislation which is pin pointed to specific risks, and leaves responsibility for meeting needs and addressing risks with the Ministries or departments who would be responsible for like acts in the offline space. This response, whilst seemingly intuitive, creates somewhat of a legal quagmire. Responsibility is siloed into different disciplines, whilst in reality this is a space that crosses traditional legislative boundaries – the issues of sexting and cyberbullying imply a response from Justice, Health and Education (at a minimum) and impact on children's privacy rights. Likewise, consumer risks for children, may straddle both traditional consumer responsibility issues (*e.g.* through enticements to spend on in-app purchases), and privacy issues (*e.g.* where data is mined from app-users).

In keeping legislative responses separate, countries risk: a duplication of efforts; matters not being covered by any relevant law; and, as in the case of sexting, the potential creation of new social issues arising out of a strict adherence to laws. Complementary policy actions and programs are necessary to fill gaps and address challenges and these responses will be discussed in the following section.

1.2. Policy Frameworks and complementary actions

In addition to a legislative response, countries national frameworks are evolving to include multiple policy actions that attempt to fill the gaps that laws cannot, and through their implementation, bolster the effectiveness of the legal framework. Often, policy is made up of a mix of strategies that revolve around multiple goals, which collectively contribute to a partial articulation of a national strategy. This often includes the involvement of multiple ministries, departments or statutory bodies.

The following table provides a snapshot of the types of policy mixes revolving around multiple goals that taken together contribute to this partial articulation of a national strategy.

Table 2. Examples of policy mixes and oversight bodies

Country	Policies	Oversight body(ies)
Belgium	*Je decide* – online privacy Digital Champion – promotes digital skills and opportunities Child Focus - combats child sexual exploitation	Data Protection Authority Private Professional, appointed by government mandate Publically funded interagency body
Canada	Canadian Centre for Cyber Security Innovation and Skills Plan, 'Technologies' – identify new technologies and develop skills	Multiple Departments (lead by Public Safety Canada) Innovation, Science and Economic Development Canada
Chile	ENLANCES – Integrates educational resources into the school system Asociación de Telefonia Móvil – Industry body, representing the mobile phone sector	Centre for Education and Technology (within Ministry of Education) Trade association, regulated by the Sub-secretariat of Telecommunications, under the Ministry of Transport and Telecommunications
Colombia	Under the framework of the Law Against Commercial Sexual Exploitation – multiple actions to prevent contact risks National Digital Security Policy ('CONPES No. 3854') – Privacy, digital security Various strategies on personal data, and protection against exploitation	Multiple government entities National Council for Economic and Social Policy Communications Regulatory Commission
France	Digital Education Unit and Policy Community of stakeholders *providing*	Data Protection Authority Educnum - Collective of 70 non-profit organisations and

Country	Policies	Oversight body(ies)
	awareness and education on educnum.fr E-enfance acting against cyberbullying and operating a national Safe line for children	NGOs E-enfance - association recognized as a public utility and approved by the Ministry of National Education
Hungary	Digital Child Protection Strategy - based on three pillars: awareness raising, digital literacy, and protection and safety.	Whole of government (part of the government's digital success programme)
Mexico	Niñ@s INAI – privacy / protecting personal data @Prende – community awareness and education	National Institute for Transparency, Access to Information and Personal Data Protection Secretariat of Public Education

In addition to the above examples, all countries indicated that their respective police forces have responsibility for the prosecution of offences (noting that some regulatory bodies also have quasi-criminal powers) and some countries have established specific cyber security strategies, and associated task forces within their police force. Whilst these kinds of initiatives may be strongly oriented towards the prevention of grooming and child pornography, their role can extend to issues such as cyber bullying or other technology facilitated abuse. For example, Australia's cyber security taskforce may be responsible for these matters as a result of the country's Cybercrime Protocol[105]. Likewise, Israel, Greece, and Norway all indicated that they have a dedicated cybercrime division in their police forces. In 2016, Israel announced it would establish a National Policy on cyber violence under the auspices of the newly created network mentioned above (see Table 2). Some countries have policies of aggravating cybercrimes when they relate to children (*e.g.* Spain, Belgium and Colombia). Of course, Interpol also has a significant role in investigating crimes against children in the digital environment and connecting national law enforcement agencies[106].

Furthermore, a few countries report the establishment of national multi-sectoral bodies to attempt to specifically and comprehensively address the protection of children in the digital environment. As an illustration, the UK Council for Internet Safety (UKCIS)[107] is a group of more than 200 organisations drawn from across government, industry, law, academia and charity sectors that work in partnership to help keep people safe online.

The important role that Safer Internet Centres ('SICs) play in countries who are member States of the European Union (as well as Iceland, Norway and the Russian Federation) should be flagged (SICs and the Strategy for a Better Internet for Children, is discussed in further detail below under 'Regional Policy Making'). This initiative, which is part of the European Commission's Strategy for a Better Internet for Children[108] ('BIK Strategy'), underlies several policy actions in these countries particularly in awareness-raising, and in the operation of helplines and hotlines. In answering the survey, a number of countries indicated that SICs are a central part of their policy response (*e.g.* Belgium; Latvia; Lithuania; Luxembourg; the Netherlands; and Portugal).

In March 2018, a mapping exercise was carried out on the implementation of the BIK Strategy. The results of this mapping found that[109]:

- All participating States have implemented BIK in some form, but no country had a single policy framework. The strategy was primarily addressed through separate policies based on singular BIK issues, or through broader policies.
- In most countries between four and six ministries are involved in the development and design of policies related to BIK.
- There was less focus on the area of positive content, with ten of the countries mapped having no national policy on positive online content for children.
- Coordination at the domestic level is often complicated by the large number of ministries involved.

- Only three of the countries surveyed had a multi-stakeholder body with responsibility for BIK, with most countries reporting more than one coordinating ministry, body or agency.

The above results reflect what has been observed in this report, namely: a spread of policy responsibility; complications in a coordinated response domestically, where there is a large number of ministries involved; and a lesser a focus on positive online content.

As well as the above in a number of countries policy is articulated through concrete actions such as awareness raising, technical measures, and consideration towards the role of parents and children. This is discussed below.

1.2.1. Awareness raising and education

Online practices are seen to be strongly linked with the acquisition of digital skills, which in turn, "*enable children to benefit from online opportunities and to manage or reduce the associated risks of internet use"* (Byrne, et al., 2016; p. 47). Some, although not all of the countries, responding to the survey indicated that media or digital literacy made up a part of their policy landscape. Estonia, Finland and Italy all reported having a specific policy focussed on media and digital literacy[110].

Across the board however even in the absence of a specific articulated policy, awareness raising and education are recognised as important policy tools, which can help to empower children, parents, caregivers, guardians and educators. Almost all countries responded with promising initiatives aimed at providing children in schools or the community at large awareness raising and educative tools designed to increase knowledge about the risks associated with the digital environment and children; and to promote safe and responsible online interactions. Whilst activities may be targeted towards children or adults, some take a specific focus (such as addressing the needs of women and girls). In a number of countries, awareness programs form part of a legislative response to protecting children in the digital environment. For example, awareness raising activities are a statutory activity of Australia's E-Safety Commissioner[111] and occur across the EU as part of the BIK Strategy. Additionally, initiatives can either be geared towards increasing the digital literacy of adults themselves, and/or increasing their capacity to support children to safely engage in the digital environment.

Both Denmark and Portugal provided examples of media and digital literacy being incorporated in wider policy documents or strategies. Portugal's Council of Ministers approved a resolution in 2015, which, *inter alia*, refers to the education and training of young people on the safe use of ICT's, with the specific aim of strengthening cyberspace safety training and creating skills and knowledge for the safe use of the internet in education. In Denmark, the Film Policy Accord (which is ostensibly a policy relating to the economic health of the film industry in Denmark) includes initiatives for film and media literacy for children and youth [112].

Finland, Lithuania and Luxembourg all provided examples of how media and digital literacy has been incorporated into the policy landscape on a program level. Lithuania's public library service has an initiative designed to actively promote media and digital literacy, and Luxembourg's SIC runs a twice-yearly workshop where children can learn to deal with new media and technologies in a responsible manner. Finland provided an example of a media literacy program designed to support those who support children, with its Media Literacy School initiative aimed at building competence and capacity in educators.[113] Hungary's campaigns in 2018 and 2019 (ostensibly to promote their Internet hotline and legal advisory service) focussed on digital literacy and raising awareness among minors regarding in what context commonly used emojis may be harmless, or threatening, abusive or offensive[114].

In France, a 2018 amendment to the Education Code, seeks to ensure that students and teachers are made aware of the responsible use of digital technology, and introduces data protection into schools and other educational establishments. Additionally, in 2015 the French ministry of education signed an agreement with the national data protection authority which aimed to ensure that both resources and training existed which acted to promote awareness among teachers and students of responsible and informed use of digital technology – including the development of training pathways for teachers and school directors on GDPR processes in school policies[115].

The Russian Federation indicated that the country's policy document on Information Security for Children is based on the presumption that minors are active participants in information processes. It identifies that State and familial efforts in this sphere, should be aimed at building the child or young persons sense of responsibility and independent existence in a hyper information society. The country reported a twofold increase in media literacy between 2013 and 2016.

1.2.2. Educational initiatives

At the school level activities include direct programs and activities geared towards children in the classroom, and also programs designed to support parents at home and teachers in delivering lessons and providing supports to students. Curricula to some extent focuses on digital literacy, however also has a strong protective orientation. Whilst a number of initiatives relate to developing curricula within the school, some countries have also developed information brochures, books, provided workshops, created dedicated media literacy centres[116], and held competitions. Importantly, some initiatives have focussed on increasing the digital literacy of the educators themselves.

In September 2018, the OECD published a report on New Technologies and the 21st Century[117.] In that report, schools (and parents) are specifically recognised as crucial to providing guidance to minors, and in turn that it is crucial that parents and teachers receive information on online safety and advice on how to help children manage online risks. Further, it was observed that whilst children nowadays seem to understand technology better than adults, they need guidance on how to use the technology in a responsible and positive way; including through stimulating children to be responsible content creators and not just content users (Hooft-Graafland, 2018: at 6.3).

1.2.3. Broader community awareness activities and engagement with parents

Across the wider community initiatives focus on the themes of digital literacy, but often take the form of addressing a particular risk. For example: fake information on the internet; online hate; cyber bullying; and privacy (including as to how this intersects with sexting and other use of a child's image). All countries participate in Safer Internet Day, which occurs each year in approximately 130 countries worldwide and aims to raise awareness of emerging online issues, choosing a topic each year that is reflective of a current concern[118].

Engagement with parents was noted to be key throughout the responses to the OECD Survey. Often, community awareness activities aim to accompany parents in their support for their children (*e.g.* Canada 'Media Smarts' program[119], or Belgium's 'Click Safe' program[120] the latter being aimed at both parents and teachers). Costa Rica in their response to the survey flagged a need to place more emphasis on the digital literacy of the adults themselves. It has separately been seen that parents may have higher digital literacy skills then their children aged 9-11, about the same skills as their children aged 12-14, and weaker skills then their children aged 15-17. This results in parents not necessarily being able to appropriately guide their older children in their online experience (Byrne, et al., 2016; p55).

The observation made in 2011 that, other than *"integrating Internet literacy in schools' curricula, little or no information is available on effective strategies for identifying and reaching out to categories of children who are more at risk than others, such as those whose parents cannot play the role expected of them in a policy model based on shared responsibility"* (OECD, 2011; p. 37) rings true today - at least on an operational level. Largely awareness raising activities outside of direct education for children, relate to empowering parents to protect their children in the digital environment[121]. However, it remains unclear what initiatives address the needs of children without a responsible parental figure, particularly where a heavy policy reliance is placed on voluntary measures by parents to protect children online.

Further, it has been observed that the most effective strategies to promote digital citizenship and child online safety are those that involve a multi-stakeholder, multi-sectoral approach, *plus engagement from parents* and children themselves (Byrne, et al., 2016; p83) (emphasis added). Where children have a trusting relationship offline and are able to turn to their parents for support generally, this needs to be able to be translated into a capacity on behalf of parents to positively mediate and encourage their children's activities in the digital environment. Promoting awareness among parents and caregivers is noted as being key to achieving this (Byrne, et al., 2016; p83). Not all children, however, are able to turn to their parents, and a gap in response in this space (for example, by increasing the capacity of teachers to respond or promoting children's agency) has been identified (Byrne, et al., 2016; p83, 84).

1.2.4. Recognising the role of children

In 2011, the OECD noted that where policies existed to protect children online there was a wide recognition that children differ in age, degree of vulnerability and/or resilience, with some more at risk than others. At that time, a common understanding existed that policies to protect children in the digital environment must be tailored to their needs, risks and stages of development. Additionally, policies should respect children's right to a freedom of expression as laid down in Article 13 of the UN Convention on the Rights of the Child ('CRC') and in countries' constitutions (OECD, 2011; p. 37).

Children's rights and the online environment should not be considered in a mutually exclusive manner. As has been noted throughout this report, the digital environment is more and more part of the environment where children live their lives, rather than merely a tool used for communication, research, etc. Accordingly, children's fundamental rights need to be protected online, just as they are offline and the four guiding principles of the Convention of the Rights of the Child (the best interests principle, the right to be heard, freedom from discrimination, and the right to life, survival and development) should be respected and upheld in any policy making consideration. Since 2011, it is clear that a greater recognition has been given to considering the rights of children in their online interactions, and the need for a child-centred approach that respects and upholds these rights when engaging in policy making. Whilst the following paragraphs consider this issue in the light of a child's right to a freedom of expression, and their right to participation it is noted that in the international space a large amount of work is being done to take a rights-based approach to policy making, and this is further discussed below (at 2.3.) Whilst a rights-based approach can only be lauded for ensuring personal agency in policy making and that any measures act to protect rights, it cannot be approached in a silo, and must be at the same time supported by evidence-based policy making.

A child's right to a freedom of expression includes the seeking, receiving and imparting of information. Where policy rests heavily on protecting children's privacy through parental consent, there is a possibility that this right could be curtailed should a parent be either unwilling, or incapable of providing reasonable consent (Nyst, 2017: p. 9). At least one country raised a concern that parents themselves may present a risk to children (predominantly in a privacy space) when using their child as content[122]. Likewise, it is has elsewhere been noted that threats to children's privacy can come not only from governments and the private industry, but from parents themselves through the sharing of information about their children online (Viola de Azevedo Cunha, 2017; p. 14-15).

Policies which existed in 2011, that adapted responses to certain age groups (*e.g.* through filtering tools, educational curricula) continue to exist today. In response to the survey at least one country[123] indicated that any review of the OECD Recommendation should include consideration of the use of the digital environment by toddlers. This does appear to be a gap in the policy and research space. For example, whilst the 2017 observation by the UK's Communications Regulator saw an increase in children going online, and more children owning their own tablet (including those belonging to the youngest age group measured), the report does not measure the online use of any children under the age of 3 years (Ofcom, 2017; p. 7). There may be some movement in this space, however, with the UK Information Commissioner publishing a consultation draft of an Age Appropriate design code of conduct in April 2019. This draft code recognises the age group 0-3 as well as a lack of evidence and awareness of the potential risks posed to children in this age group[124].

A number of countries continue to recognise minors as active stakeholders in the formulation of policy and its implementation process, for example the EU and some individual countries (*e.g.* Australia, the Russian Federation). It is known that involving children more actively in developing policies can contribute to better policy measures. Children are also more likely to be engaged in peer education strategies and can help relay information about risks in the digital environment and risk mitigation strategies[125]. Despite this, the recent mapping of EU States involved in the Better Internet for Kids Strategy, found that whilst most countries consulted with children, only a third indicated that children had an opportunity to be actively involved in policy design (O'Neill & Dinh, 2018; p. 10).

1.2.5. Helplines and hotlines

Almost all countries indicated that they ran (or supported via an NGO or SIC) a helpline, a hotline, or a 24/7 online space to field complaints and offer support to children and young people regarding online behaviour. Helplines are likely to offer support, whereas hotlines can be used to receive tips relating to possible criminal activity / illegal online content. Some helplines / hotlines are broad in nature, relating to both online and offline behaviour (*e.g.* 'line 147' Chile); some are geared towards sexual abuse responses (*e.g.* Belgium, the United Kingdom); and others provide broader assistance including psychological support, counselling and advice for both minors and their parents (*e.g.* Colombia, Estonia, Latvia, Spain). A few countries indicated that they operated both a hotline and a helpline (*e.g.* Lithuania, Luxembourg, Portugal, Turkey).

1.2.6. Technical measures: Filtering tools

In a range of countries, filtering schemes operate as part of the commitment by Internet Service Providers ('ISP') to block access to illegal content, and in particular, images of sexual abuse of children. Additionally, in response to the survey a number of countries indicated a reliance on voluntary parental filter use, or the availability of such tools (*e.g.* Hungary, Italy, Japan, Lithuania, Norway, the United Kingdom, and the United States).

Whilst often these filters are promoted through government initiatives, they are likely to be voluntary and a service provided by the ISP rather than a government action (*e.g.* Australia, Italy, the Russian Federation, and Turkey). Some governments indicated that they arrange for the testing of filtering tools, and subsequently provide recommendations (*e.g.* Lithuania, Spain). Both the United Kingdom and Norway (to a lesser extent) indicated cooperation with industry with regards to the provision of filtering tools. One of Norway's mobile phone companies has developed various applications to protect children when on their mobile phones, including a tool to block bullies and a child pornography filter. In the United Kingdom, the four major ISP's have delivered on a commitment to present an unavoidable choice to consumers on whether or not they wish to switch on a family friendly network filter. In Costa Rica, legislation obligates private owners of public internet access spaces (i.e. cyber cafes), to install programs and filters which block access to websites and communications which have harmful content that is directed towards teenagers. In February 2018, Japan introduced a revised 'Act on Development of an environment that provides safe and secure Internet use for young people'. The previous version of the Act had imposed on telecom operators an obligation to ask parents to embed filtering software in mobiles owned by children under the age of 18 years, and the new version extends the scope of this Act, by placing this obligation on selling agents, and on manufacturers of mobiles, PC's and operating system developers[126].

Data on the use of filtering tools, is available from the UK's Communications Regulator, who noted that between 2016 and 2017 nearly two in five parents of children aged 3-4 and 5-15 years who have broadband, and whose child goes online, used home network filters (an increase from the year before); and one in five parents of children aged 5-15 years had changed the settings of their child's tablet or mobile to prevent downloads or in-app purchases (also an increase from the year before). It is however flagged, that at the same time, one in five parents of 5 to 15 year olds who use network-level filters felt that their child may be able to by-pass home network settings (Ofcom, 2017; p. 7).

1.2.7. Conclusions / Observations

In many ways, the policy landscape today is not significantly different to what was identified in 2011. At that time, a multi-layered policy approach encompassing legislative, self- and co-regulatory, technical, awareness, and educational measures, as well as positive content provision and child safety zones was identified (OECD, 2011; p. 33). Today, whilst some countries have made some moves towards centralising their responses, divergent policies and those that are spread across sectors remain in place. As noted by other researchers, a lack of overarching policy on children in the digital environment creates a scattered response across departments, resulting in ministries responding in accordance with their own traditional responsibilities, which may not be the appropriate response and/or may mean that the appropriate measures are overlooked (Byrne & Burton, 2017; p. 47).

In 2011, the effectiveness of high-level policies was unclear owing to a lack of comparable evidence (OECD, 2011; p. 33). To a certain extent that gap in evidence persists today. It has elsewhere been noted that policy making to protect children and young people in the digital environment is impeded by both inadequate measuring of the impact of existing policies, and partial evidence being used to justify a response or that serves a particular political goal (Byrne & Burton, 2017; p48). There is a clear need for a comprehensive and cross-national knowledge base to support policymaking. Below, (under 2.2.11-2.2.12) this report will consider how countries responded to the survey with regards to how measuring and monitoring is occurring at the national level. The role of multi-stakeholders in policy making, is however addressed first.

1.2.8. Multi-stakeholder engagement

As was the case in 2011, the common understanding that policy for the protection of children in the digital environment rests on the commitment and shared responsibilities of all stakeholders persists today. 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[127].

Whilst a number of initiatives which meet this definition are discussed under international policy making below, on the national level, a number of countries have sought to enter into partnerships with industry and civil society to address risks to children in the digital environment. In some countries specific bodies have been created to coordinate the activities of private and public stakeholders.

The United Kingdom's Council for Internet Safety (UKCIS) is a multi-stakeholder forum representing over 200 organisations with an interest in Internet safety. Prior to November 2018, this body was the United Kingdom's Council for Child Internet Safety (UKCCIS), and focussed solely on children's issues. Since November 2018, its remit has expanded to cover adults.

This council brings together Government, industry, law enforcement, academia, charities and parenting groups to work in partnership to help keep people safe online, albeit on a non-statutory basis. UKCIS is recognised by the UK Government to have played a pioneering role in promoting and championing improvements to child online safety[128]. This body has introduced a number of positive initiatives, such as: friendly Wi-Fi logos, which enable the identification of public Wi-Fi spots that have filtered inappropriate websites; collating internet safety research; creating guides for parents with practical safety and privacy tips; and creating guides for industry which include examples of good practice and advice from online child safety experts[129].

1.2.9. Civil society engagement

Across the board engagement with Civil Society is high. Governments partner with civil society to offer services, develop policy, and to contribute to expert subject matter groups.

Australia, Costa Rica and the United Kingdom have multidisciplinary advisory bodies made up of academics, industry, child protection groups, Non-Government Organisations ('NGOs'), and telecommunication providers.[130] Likewise, even though Finland did not indicate that a representative body exists, it did report that a large variety of stakeholders implement governmental policies, including NGOs and the business sector. Latvia reported that NGO's advise policy makers on trends, key problems and areas for action.

Austria, Greece, the Netherlands, Lithuania and Norway, all run their SICs (see the discussion below under 'Regional Policy Making') through NGO's or proactively engage with NGO's in service delivery. Belgium actively engages with NGO's, but cannot enforce policy through these organisations. On the other hand, Estonia, indicated that NGO's have the main role in implementing policies.

A number of countries rely on NGO's to work on awareness raising activities, resource development, research, and education. This is the case for the Czech Republic, Italy, Norway, and Poland. The US indicated that NGO's are instrumental in operating their COPPA initiative. Mexico has partnered with NGO's on specific campaigns, including a campaign on sexting.

At the Zurich Workshop, a number of initiatives (both national and international and) led by the Commission nationale de l'informatique et des libertés (CNIL) were presented by the French privacy and data protection enforcement authority. This included partnerships with young ambassadors on children's rights who act as trainers on data protection issues, on NGO's working with children in an offline space (i.e. sports clubs), the development of peer privacy competitions, and the use of this space to promote awareness on the good use of social networks. At the educational level a number of initiatives were highlighted, including importantly an initiative to integrate the International Competency Framework on Personal Data Protection within school curricula, which will be adapted to different age groups. At the international level it was reported that a common digital education web platform has been created which allows for the sharing of pedagogical resources and best practices.

1.2.10. Engagement with industry

Some countries reported active engagement with industry, with a few governments specifying an active policy strategy to work with telecommunication companies and other private industry to promote cooperation on online safety. This may take the form of direct policy input, joint initiatives, and representation on larger multi-stakeholder forums.

Examples of direct policy input include the Austrian government's collaboration with telecom operators, whose input was indicated as being important in policy development. The Russian Federation indicated that the government works with the operator of one of its most popular social networks (and the shareholder of this service) and regularly plans work to restrict access to inappropriate content on an age appropriate basis. Chile's *Asociación de Telefonía Móvil* a representative body for the country's mobile phone industry which, *inter alia*, seeks to integrate advancements in the telecommunications sector with the work of public and private bodies.

Some countries provided examples of successful joint partnerships, often through the country's SIC. For example, the Greek SIC successfully partnered with Facebook to develop an information booklet. In the Netherlands, the SIC has partnered with private industry on initiatives such as their Media Literacy Network. Norway, in their response to the survey, highlighted an initiative between government and a telecommunications company to develop applications designed to protect children on their phones (i.e. an anti-bullying filter and a child pornography filter).

From the industry perspective, a number of organisations and companies take an active stance in relation to ensuring the protection of children in the digital environment. In particular major social media and websites have policies regarding child protection, with varying efficacy.

For example, YouTube has community guidelines[131] for their users. The guidelines include such things as prohibitions on nudity or sexual content; harmful or dangerous content; and hateful content. The language of the guidelines is strongly angled towards the protection of children. YouTube reports that if any of their users obtain three strikes for violating the community guidelines, their account will be terminated. The site maintains a public register of the channels terminated and the reasons. It indicates that 4.5% of removals are for child protection reasons[132]. The website's child protection page indicates that should child sexual abuse imagery be uploaded on the site, a report will be made to the National Centre for Missing and Exploited Children, who will then work with law enforcement. It also provides information on how to report bullying and harassment.[133]

Google, of which YouTube is a part, has taken steps to enforce COPPA compliance. It's 'Designed for Families' program, provides app developers with information on COPPA and requires that they certify they are in compliance. However, as reported at the Zurich workshop, it has been found that there is in practice limited enforcement of this (Reyes, et. al., 2018; p. 77).

Likewise, Facebook has community guidelines, which purport to provide protections for children, banning any material that depicts or advocates for the sexual exploitation of children; and removing images which have the potential for abuse (for example, a nude image of a child which is innocently posted by a parent, and not sexual in nature). The guidelines provide parameters and measures regarding material that may be bullying or harassment[134].

Snapchat, also has community guidelines which prohibit sexually explicit content, harassment and bullying, threats violence and harm, and hate speech. Snapchat provides for in-app reporting, whereby a user can press a 'white flag' button directly on the snap, which acts as a report[135]. TikTok's community guidelines prohibit a number of items, such as illegal activities, violent and graphic content, suicide self-harm and dangerous acts, adult nudity and sexual activities, hate speech, and harassment and bullying. The platform has specific guidelines on minor safety prohibiting the posting of: nudity and sexual exploitation involving minors; underage delinquent behaviour (i.e. minors consuming or possessing alcohol, drugs or tobacco); child abuse; grooming behaviour; and content which sexualises minors. It is indicated that any content depicting or disseminating child abuse, nudity or sexual exploitation will be reported to legal authorities[136].

Instagram similarly has community guidelines which includes information for parents (including on protecting their child's privacy); on how to address abuse; and on eating disorders[137]. Instagram also maintains a list of unsearchable terms which are designed to avoid users navigating directly to harmful images. In 2018, Instagram updated this list to include a number of hashtags which could promote eating disorders, following a BBC investigation into hashtags promoting eating disorders[138].

The enforcement of these community guidelines are largely self-regulatory based on the actions of the sites themselves, the users, or the parents of the users. Arguably therefore, shifting responsibility to the consumer. For example, whilst all of these sites provide that any person under the age 13 cannot join their site, in reality children under that age often do sign up for these services. In the United Kingdom, as of 2018, 12% of nine year olds, 21% of 10 year olds, and 34% of 11 year olds had a social media profile (OFCOM, 2018; p. 17).

A number of companies are also members of multi-agency initiatives designed to promote the safety of children in the digital environment, often in cooperation with government. The role that the UKCIS plays in promoting online safety has already been highlighted above. The EU Alliance to better protect minors online, is a self-regulatory multi stakeholder platform facilitated by the European Commission, and strives to tackle harmful online behaviour and content. The Alliance's Statement of Purpose focuses on three categories of risk: content; conduct; and contact; and includes such organisations as Disney, Twitter, the Lego Group, Spotify, Snap (Snapchat), Microsoft, Google, and Facebook139. There are however rising doubts about the effectiveness of self-regulation, and that it can lead to un-equal protection depending on the child's situation (Livingstone, et. al., 2018b: p. 8, 9).

Finally, it is noted that positive engagement with industry may be one way to address concerns regarding the lack of focus on positive and beneficial online content in that is identified throughout this report. Whilst ensuring good digital literacy is clearly necessary, it is also necessary to create an enabling environment for the development of quality content that is appropriate for different age groups. Governments may need to consider ensuring that sustainable business models exist which promote the development of content specifically designed for children with respect to both privacy, and ensuring safety by design.

1.2.11. Monitoring and evaluation

There are a number of gaps and significant differences in the manner in which countries monitor the effectiveness of their laws and policies. Some countries undertake regular targeted reviews, some monitor individual programs, some carry out a number of different monitoring activities (*e.g*. through government, service providers, CSO's and academia), at least one country monitors via case studies, and some reported no monitoring at all.

Most of the countries engaged in the EU's Better Internet for Kids Strategy reported that they undertook their monitoring through this process. This is the case for Denmark, Greece, and Luxembourg. Monitoring in this space seems to take the form of analysing: the number of contacts with a service; demographic data; feedback on training; as well as reviewing annual reports. In Luxembourg it was indicated that this data helps shape future policy.

A number of countries monitor through public surveys. Israel indicated that it conducts surveys on the themes of online risk: threats; shaming; harassment; extortion; humiliation; and reports made to schools, parents or helplines. There was not however any indication of the outcome/findings of these surveys. Lithuania also monitors via public survey using questions separately targeted to youths and adults. The surveys focus on operational issues such as the visibility and usability of the hotline and awareness centre. In Hungary, a survey of both parents and their children focussed on media use patterns, rules applied in-family regarding children's media use, and on specific risks and harms children may be exposed to.

Some countries monitor through their statutory or regulatory bodies, or as a product of their guiding policy document. For example, Latvia indicated that it must regularly review its policy guidelines on information society. Likewise, the Australian *Enhancing Online Safety Act* is statutorily required to be reviewed every three years, with the Commissioner having key policy targets to meet[140]. The Norwegian Media Authority conducts a bi-annual national reference survey as part of its National Action Plan. The results of this survey are used to target actions and develop better resources.

There may be separate monitoring by individual government bodies or authorities in their respective areas of work. In Australia, quantitative and qualitative research is used to monitor the effectiveness of content regulation measures. In the US the Federal Trade Commission oversees the work of COPPA. Poland indicated that their monitoring occurs through each department monitoring their own program or policy. Sweden's National Education Agency, monitors online progress in schools every three years and the country's Ministry of Culture, and its Media Council undertake constant monitoring of trends, and use this data to propose new policies, or amendments to exiting policies. In Canada, the Office of the Privacy

Commissioner of Canada oversees compliance with the Privacy Act[141] (which covers the practices of government departments and agencies on handling personal information); and the Personal Information Protection and Electronic Documents Act[142] (Canada's federal private sector privacy law).

Some countries take feedback from a wide variety of stakeholders, and use that feedback to help develop future policy. Greece consults with academia, the private sector, civil society, the mass media and the public. Portugal's public sector and government bodies work together with civil society to define and develop policy, and to implement this policy. In Portugal, industry and civil society are key stakeholders in identifying risks and trends, and use collaboration and self-regulatory methods to minimise risks and implement security measures.

In Italy it was noted that the effectiveness of policy is measured on a case-by-case basis, with the results used to guide future awareness and accountability campaigns.

Norway identified that only resources and projects are evaluated, not overall policies. For Norway, a lack of robust evaluation of processes was identified. A report from the country's National Institute of Public Health concluded that the two main awareness campaigns against bullying lacked a robust evaluation methodology, highlighting a need to strengthen evaluation methods and ensure the sharing of best practices[143].

1.2.12. Measuring

A number of countries identified that there was no systemic measuring of risks, or of the effectiveness of preventative measures. As it is illustrated below, some countries measure their activities through data obtained via helplines and SIC's.

As can be seen from the table below, even from within the collaborative and coordinated EU space, mechanisms for measuring risks are varied, both from the standpoint of the actual method employed, and with regards to how that data is used. Additionally, the terminology and definitions used in measuring (both in and outside of the EU) are seemingly widely varied.

Likewise, outside of the EU, responses to the survey on how risks were measured varied however surveys remained a common measure. Costa Rica reported measuring this way, and a nationwide telephone survey was taken in 2013. The results of this survey showed adult carers needed education and training on how best to guide and accompany minors in their interactions in the digital environment. This finding resulted in the development of a website to address this gap[144]. Costa Rica also reported relying on the work of academics and universities to measure outcomes and analyse issues.

Table 3. Measuring of Safer Internet Centre Activities

	Greece	Latvia	Lithuania	Norway	Portugal
Data Collection Method	Helpline & Safeline Statistics	SIC conducted survey – separately targeted at parents / children	Measures numbers of events held, tools developed and reports received	SIC conducts an annual survey – separately targeted at parents / children	Number and quality of calls.
Data Use	Project deliverables	Identify risks, strengths and trends in online behaviour.	Used to improve service delivery and increase impact of service/	Compares trends over time, allows for targeted actions and improved resources	Inform future public policy.

Source: OECD

Both Japan and Sweden reported measuring the effectiveness of their policies through the digital literacy of children. Japan's Ministry of Internal Affairs and Communications has, since 2012, conducted annual tests on young persons' Internet literacy. The assessment targets children in their first year of high school, and includes both the rates of Internet usage and the prevalence of filtering services. In response to the survey, Japan reported that between 2012 and 2014, Internet literacy for 15 year olds (on appropriate online communication capability) increased 9.16%. The Swedish Media Council has developed indicators to measure children's level of media and information literacy. These indicators are based on a child's ability to find, analyse, critically evaluate, create, and handle information in different media and contexts.

This lack, or mismatch, of evidence can lead to inappropriate or disproportionate responses in the offline world – leading to a public discourse which is in fact disengaged from reality. In recent years, two high profile cases of apparent serious risk to children has caused a storm online, and provide an example of the concern and panic which can spread across communities of concerned parents; when in fact both such cases were themselves declared to be a hoax. The first example of this is the 'Blue Whale Challenge', an apparent suicide game which emerged in Russia in 2017, and told of a story where young people were given a series of challenges over 50 days, eventually culminating in a suicide. More recently, the 'Momo Challenge' told of a social media challenge spreading over Facebook and WhatsApp, whereby a user named Momo was enticing children to perform a serious of dangerous tasks including violent attacks, self-harm and suicide. Again, it was concluded that this so called online challenge was a hoax, and the spreading of warnings about it, had in themselves the potential to cause harm – creating panic, or encouraging children to look up violent or disturbing material[145].

Improvements in defining and measuring risk and the exact nature of minor's engagement in the digital environment, is needed to address this mismatch between actually identified and evidence based risks for minors online, and those which are perceived risks. This in turn, should support measures which encourage both minors, their parents (and other key stakeholders – educators, policy makers) to engage in critical thinking around what are actual and what are perceived risks and ensure that efforts to minimise or mitigate risks are appropriately directed.

1.2.13. Conclusions / Observations

In 2011, the OECD noted that, "The policy-making process would benefit from official statistics on children's use of the Internet and the prevalence of risk. This would require a more consistent approach to definitions, methodologies and indicators. Impact assessments would help address conflicting policy objectives and place greater emphasis on the quantification of benefits and costs" (at p5). This is not happening across the board. A lack of common definitions and methodologies appear to persist. Whilst survey taking appears to be a common monitoring / measuring mechanism, there is a lack of consistency regarding what is measured from the surveys and how those results are used. The need for a systemic approach to evidence based policy making continues to be essential in determining policy priorities and in maximising protections that may be afforded by national policies (OECD, 2011; p.5).

1.3. International policy making

As previously concluded by the OECD, 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 medium. Intergovernmental organisations at international and regional level (APEC, CoE, ITU, OECD, WSIS/IGF, etc.), and in particular the European Union, have continued work in this space within their remit. Whilst at their core the initiatives remain somewhat consistent with what was identified in the 2011 Report, the work that is undertaken in this space has evolved to include some useful moves towards increasing efficiency in measuring and monitoring, and attempts at harmonising research and responses.

Table 4. Initiatives for international co-operation by intergovernmental organisations

Organisation	International / Regional co-operation activities
APEC	On 8 August 2012 at its Telecommunication and Information Ministerial Meeting, APEC Ministers acknowledged the particular susceptibility of vulnerable groups (including children) to online risks and called on members to implement strategies. The APEC Cross-border Privacy Enforcement Arrangement (CPEA) creates a framework for regional cooperation in the enforcement of privacy laws. 27 bodies participate in this framework.
Council of Europe	The COE has a number of initiatives aimed at protecting children in an online environment, including: the work of the Lanzarote Committee; that of the Cybercrime Committee; the Guidelines to respect, protect and fulfil the rights of children in the digital environment; and a project aimed at ending online child sexual exploitation and abuse. The *Lanzarote Convention*[146] is the first regional treaty specifically dedicated to the protection of children from sexual violence. The Lanzarote Committee monitors the implementation of the Convention, and the second monitoring round (underway at the time of drafting this report) is focussing on the protection of children from sexual exploitation and sexual abuse facilitated by information and communication technologies[147]. The Cybercrime Convention Committee aims to facilitate the effective use and implementation of the COE Convention on Cybercrime[148], and the exchange of information between State parties. The Convention itself provides minimum standards regarding criminal and procedural law reform, covering *inter alia,* offences related to child pornography and international co-operation. On 4 July 2018, *Guidelines to respect, protect and fulfil the rights of children in the digital environment*[149] were adopted. These Guidelines provide a set of ground rules to assist States in providing the necessary basis for ensuring the best interests of children in a digital environment. The COE project to end online child sexual exploitation and abuse[150], seeks to strengthen regional and national cooperation, develop capacity building and training tools to enhance effective investigation and prosecution, and to raise awareness of prevention activities. This project will be implemented at a regional level until December 2020.
European Union	The EU's *Better Internet for Children Strategy* aims to ensure children have the necessary skills and tools to fully and safely benefit from the Internet. It includes actions on: Promoting quality content for children, and positive online experiences; Digital and media literacy; Simplifying and strengthening reporting tools to deal with risks such as cyber bullying and grooming;

	Improving age rating tools, and the use and availability of parental controls; Online advertising, overspending and online gambling; and Child sexual abuse and sexual exploitation Better Internet for Kids Website – core service platform for sharing resources, services and practices between service providers and service users. Safer Internet Centres Annual Safer Internet Forum
Internet Governance Forum	The IGF's *Dynamic Coalition on Child Online Safety* aims to protect children from potentially harmful content, conduct or contact (with a focus on child sexual abuse images, and other forms of sexual abuse) IGF provides an annual international and multi-stakeholder platform to exchange views on children and young people, among others. (For example, the 2018 agenda includes workshops on, 'Technology, Suicide and the Mental Health of Youth and Preventing Youth from Online Violent Radicalisation')
ITU	ITU pursues its work on Child Online Protection at policy and operational level: The Child Online Protection (COP) Initiative is a multi-stakeholder effort of ITU membership to create awareness and to develop practical tools and resources to help mitigate risks The Council Working Group on Child Online Protection (CWG-CP) is a platform for member states, sector members and external experts to exchange views and advance the work on child online protection Guidelines have been developed which are targeted separately at: children; parents, guardians and educators; policy makers; and industry
OECD	Developed a Recommendation of the OECD Council on the Protection of Children online (2012) Published a report on the risks faced by children online and the policies to protect them (2011). Holding a workshop in Zurich in October 2018, on the protection of children online to review: new opportunities and online risks; regulatory frameworks, policies and educational approaches, digital literacy needs, and the role of technological developments in building a protective environment.
UNICEF	UNICEF focuses on the protection of children from violence, exploitation and abuse. The UNICEF Innocenti Research Centre, has prepared a number of reports on the safety on 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. Separately, UNICEF partnered with ITU to develop guidelines for industry on online child protection.

1.4. Regional policy making

As highlighted in the 2011 Report, both the Council of Europe (COE) and the European Union have policy frameworks to protect children in the digital environment. The work of the COE is discussed below when considering the rights based approaches emerging in this space. The EU's activities are centralised in the *Better Internet for Children Strategy* ('the BIK Strategy') and its associated activities.

The BIK Strategy arises out of the European Commission's 2012 Communication, which recognised that the variations in Member States' policy approaches, either regulatory or self-regulatory, to protect children in the digital environment and EU policies had not been combined in a coherent framework. The BIK Strategy aims to ensure that children have appropriate digital skills and tools to fully and safely benefit from the Internet. The Strategy includes actions on: *i)* promoting quality content for children, and positive online experiences; *ii)* digital and media literacy; *iii*) simplifying and strengthening reporting tools to deal with risks such as cyber bullying and grooming; *iv*) improving age rating tools, and the use and availability of parental controls; *v)* online advertising, overspending and online gambling; and *vi)* child sexual abuse and sexual exploitation. The Strategy obligates the Commission to take certain actions, and places suggested actions on member States and industry for supporting its implementation.

A number of concrete actions accompany the BIK Strategy. This includes an online portal which brings together resources, services, information about awareness raising activities and provides a space to share research and good practices[151]. Safer Internet Centres (SICs)[152] operate as part of the BIK strategy in each of the EU member States as well as in Iceland, Norway and the Russian Federation. SICs are made up of awareness centres, helplines (part of the INSAFE network), and hotlines (part of the INHOPE network). The main activities of awareness centres focus on awareness raising, advice and the provision of information. With regards to the survey, those countries party to the OECD Recommendation who are also part of the BIK strategy strongly indicated that SICs were a large part of their policy framework on the protection of children in the digital environment. As would be expected, this was particularly the case with regards to awareness raising activities and in the provision of community education and information. In addition to the above activities, as part of the BIK agenda, the European Commission and SICS engage in industry partnerships[153] carry out research activities[154], and ensure youth participation[155]. As was the case in 2011, BIK continues to run an annual Safer Internet Forum where multi-disciplinary stakeholders can discuss issues related to children's safety online.[156]

The other regional body somewhat active in this space is APEC, although APEC's specific actions in this regard are less recent and less comprehensive. At its 2012 Telecommunications and Information Ministerial Meeting, the APEC Ministers acknowledged that vulnerable groups, especially children, are particularly susceptible to risk in an online environment and called upon members to implement counter active strategies and promote cyber safety and cyber security.[157]

1.5. International policy frameworks

The protection of children online remains on the international policy agenda, and is part of the work programme of several intergovernmental organisations and international non-governmental organisations. As was noted in 2011, international co-operation takes place at policy and operational levels. The work of the International Telecommunication Union ('ITU'), the International Conference of Data Protection and Privacy Commissioners, and the Internet Governance Forum are examples of policy level work. The INSAFE and INHOPE networks continue to work on an operational level, and the Global Kids Online partnership between UNICEF, the London School of Economics and Political Science, and the EU Kids Online Network seeks to fill a gap that previously existed regarding comprehensive global research.

1.5.1. Policy level

Since November 2008, ITU's *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. The COP takes a holistic approach to promoting online safety for children, by developing strategies in five key areas: *i)* Legal Measures; *ii)* Technical and Procedural Measures; *iii*) Organisational Structures; *iv)* Capacity building; and *v)* International Cooperation.

As part of COP, ITU has released Guidelines for Child Online Protection, targeted separately at: children; parents, guardians and educators; policy makers; and industry[158]. The latter was developed in partnership with UNICEF and provides advice on how the ICT industry can help promote safety for children using the Internet or any technologies or devices that can connect to it. Finally, as part of COP the *Council Working Group on Child Online Protection* holds annual meetings where views can be exchanged, and reports made on the activities of the members[159].

The International Conference of Data Protection and Privacy Commissioners (ICDPPC) is a grouping of accredited data protection and privacy authorities (122 at the time of writing this report)[160]. Through its working group on digital education a number of resolutions have been passed on key issues regarding and education and children's rights (in particular privacy rights). For example, on e-learning platforms[161] and on privacy in education[162]. The working group seeks to address the extent to which minors can independently exercise their rights over their personal data by sharing information on, and experience from, national initiatives focussed on children's online rights.

Global Kids Online, is a collaborative initiative between the UNICEF Office of Research-Innocenti, the London School of Economics and Political Science, and the EU Kids Online Network. This research seeks to fill a knowledge gap which had existed with regards to comparable evidence from lower and middle income countries across different continents on topics such as skills digital literacy and civic engagement, as well as risk and hurtful behaviour (Bryne & Burton, 2017: p.39). It aims to provide tools and guidelines to national researchers and comparative analysis of country specific research findings. A comprehensive research synthesis covering 2015-2016 (Byrne, et al., 2016) has been completed, and overall the projects aims to create a researchers toolkit, which can enable longitudinal and cross-national comparisons so as to create a global knowledge base around children's use of the internet and its associated risks (Byrne, et al., 2016: p. 8).

1.5.2. A child's rights perspective

Whilst this report largely focuses on policy responses, it is worth noting that efforts to improve the responses to the needs of children in the digital environment, is concurrently occurring in a rights space. UNICEF has noted that children's rights are largely absent from Internet governance (Livingstone, et al., 2016: p 12) and notably the Council of Europe ('COE') and the Committee on the Rights of the Child ('the CRC Committee') have taken steps to seek to ensure that children's rights are appropriately protected and upheld in any legislative or policy response. Whilst 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 digital 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 & Burton, 2017, p. 40, 42).

The CRC Committee held a general day of discussion in 2014 on Digital Media and Children's Rights. The recommendations from that day included, *inter alia,* that:

- States should recognise the importance of children's access to, and use of, digital media and information and communication technologies in the promotion of their rights;
- States should undertake on-going research, data collection, and analysis to better understand how children access and use digital and social media, and how it impacts on their lives;
- States should carry out awareness raising activities, and support digital and social literacy skills for children;
- Children's right to privacy in relation to digital media and information needs to be effectively safeguarded;
- States need to address risks posed by digital media and information and communications technologies to the safety of children, including online harassment, access to violent and sexual content, and self-generated sexual content;
- States should provide effective remedies for child victims of online harm;
- States should implement policies to ensure accessibility of online content to children with disabilities; and
- Information on digital media should be included in periodic reports to the Committee.

Since the day of General discussion, it is noted that the English Children's Commissioner has made a formal case for the CRC Committee to release a General Comment on Children's Rights and Digital Media (Livingstone, et al., 2017). In March 2019, the CRC Committee announced that it would be making a general comment on children's rights in the digital environment. The general comment will, *inter alia*, aim to clarify how the rapidly evolving digital environment impacts on the full range of children's rights in positive and negative ways. The Committee will specifically consider a number of issues that have been raised throughout this report, such as: taking children's views and experience into account in policy making; how businesses operating in the digital environment should support the realisation of children's rights; and the extent of the role of parents and other caregivers[163].

The work of the Council of Europe ('COE') was highlighted in the 2011 Report, and since that time the COE has continued to work in this space. In its 2016-2021 Strategy for the Rights of the child, the challenge '*Growing up in a Digital World*' has been identified as a specific target issue to be addressed, and is recognised as a priority area for protecting and promoting the rights of the child. In 2016, under the authority of the Ad hoc Committee for the Rights of the Child, a 'Drafting Group of Specialists on Children and the Digital Environment' (CAHENF-IT) was established. This group had a "*mandate to develop comprehensive Guidelines for member States to empower, protect and support children's safe access to their rights on the Internet*" (Council of Europe, 2016a). The Committee of Ministers recommendation on *Guidelines to respect, protect and fulfil the rights of the Child* (CM/Rec (2018)7) was adopted on 4 July 2018, and work is continuing on developing a handbook setting out concrete measures to implement the Guidelines.

The guidelines provide concrete solutions and aim to stimulate co-operation at the national and international level. The guidelines apply fundamental rights standards and principles to the digital environment, namely those rights and principles contained in the UNCRC, and the European Convention on Human Rights. In addition, the Guidelines set out concrete measures to strengthen the implementation of the Lanzarote Convention and the Cybercrime Convention. Conventions which provide a comprehensive benchmark for criminal and procedural law standards relating to the sexual exploitation and abuse of children facilitated by ICTs. The Guidelines emphasise the importance of prevention strategies, and in ensuring that all actors carry out the necessary due diligence for protecting children in the digital environment, further recognising that upholding the rights of the child in the digital environment is a shared responsibility, requiring both public and private actions; legal and voluntary measures; and the participation of children. Specifically, the guidelines cover, *inter alia*, the following rights / principles: participation; non-discrimination; access to the digital environment; freedom of expression and information; privacy and data protection; the right to education; the right to protection and safety; and the right to an effective remedy. The Guidelines also provide concrete guidance for national legal and policy frameworks; and international frameworks.

In addition to the above, the Protocol amending the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (CETS No. 223) [164] was opened for signature on 10 October 2018. At time of drafting this report it had not yet entered into force[165]. The modernised Data Protection Convention will provide that member States must give special attention to the data protection rights of children and other vulnerable individuals.[166]

2. Conclusions

This report 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 an analysis of the laws and policies in place as of mid-2019, and consideration of whether or not they have kept pace with the changing environment. Whilst some promising practices are seen – such as the creation of some (although few) single oversight bodies and a continued common understanding of the importance of international and regional cooperation - a number of issues remain. This includes:

- The wide-ranging nature of the legislative responses and the drawbacks of this (*i.e.* duplicating efforts; overlooking issues; and in some cases the creation of new social issues).
- Fragmented policy responses; and
- A lack of consistent measuring, and reporting – including varied definitions and terminology; and consequently, a lack of evidence based policy making.

Additionally, whilst both the importance of multi stakeholder bodies, and of promoting digital and media literacy are recognised, these matters are not always adequately addressed in countries' legislative or policy responses. It may be, that the development of National Strategies would be an appropriate measure to address these concerns, notably the fragmentation of responses.

As has been stated above (see executive summary), the 2012 Recommendation focuses on three main challenges that were (at that time) faced by governments, and which underline the emerging nature of the protection of children online as a public policy area. These were: *1)* the need for an evidence-based policy making approach; *2)* the need to manage policy complexity through enhanced policy co-ordination, consistency and coherence; and *3)* the need to take advantage of international co-operation to improve the efficiency of national policy frameworks and to foster capacity building.

Whilst these needs still persist today, this report has shown that the online landscape has significantly changed since 2011. The changing nature of the risks, the patterns of use by minors online, and the complexity of digital technologies call for new responses and tend to indicate that the Recommendation in its present form does not wholly act to ensure the protection of children in the online environment. Indeed, even the terminology itself has changed significantly since 2011 – today, the digital environment is recognised as being symbiotic with people's lives, rather than simply the 'Internet' being a tool for communication, research, etc.

In addition to changing terminology, a number of broad areas stand out as needing to be clearly addressed – both in any changes to the OECD recommendation, and consequently by policy makers and legislators. These are the concept of a conduct risk; the rapidly changing nature of the privacy space; the role of parents and educators; and the extent to which intermediaries can hold a liability.

The concept of a conduct risk, which was previously not recognised as a risk by the OECD, is a clear risk today. Issues such as sexting and cyberbullying, cannot be quarantined and considered to pose a risk only towards those children who are the recipients of such online abuse or material (i.e. a contact risk), but also to those children whose behaviour itself arguably creates the risk. Whilst issues such as sexting, and the exact nature of the risk continue to need a better evidence base, it is undeniable that this is a circumstance where the child's own conduct makes them vulnerable, and that laws and policies should act to protect and support children and young people (rather than act to criminalise them, which is often the case today).

The relation between privacy and data in the digital environment is becoming highly complex. Children's online activities are the focus of commercial interests, a multitude of monitoring and data-generating processes, and it is vital that children's understandings of the digital environment, their digital skills and their capacity to consent are taken into account in designing services, regulation and policy.

At the same time, parents, carers and children's teachers are being asked to address these risks with little recognition of the fact that they themselves are ill equipped to understand them. Whilst it is not disputed that in principle parents hold a primary protection role, the changing and rapidly evolving nature of technology leaves parents in a space where they may not comprehend the technology or the risk, and therefore may not have the capacity to fulfill this role.

Lastly, greater attention is being paid to the capacity to hold intermediaries (*e.g.* websites, social media companies) liable for harm. A number of countries have explored the possibility of introducing a statutory liability. The drawbacks of allowing an exemption for hosting harmful content is most clearly seen through the example of Backpage.com whereby intermediaries who facilitated the sex trafficking of children were able to avoid a liability and this led to a change in the US legislation in 2017.

References

APEC (2012) Telecommunications and Information Ministerial Meeting, 'Declaration'. Available at: https://www.apec.org/Meeting-Papers/Sectoral-Ministerial-Meetings/Telecommunications-and-Information/2012_tel

38th International Conference of Data Protection and Privacy Commissioners, "Resolution for the adoption of an International Competency Framework on Privacy Education", October 18–21, 2016, Marrakesh, Morocco. Available at https://icdppc.org/wp-content/uploads/2015/02/Resolution-2016-on-Privacy-education.pdf .

Alava, S., Frau-Meigs, D., and Hassan, G. (2017), 'Youth And Violent Extremism On Social Media: Mapping The Research' UNESCO. Available at: https://en.unesco.org/news/unesco-releases-new-research-youth-and-violent-extremism-social-media

APEC (2009), "APEC Cooperation Agreement Arrangement for Cross-Border Privacy Enforcement". Available at: https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx

Arthur, R. (2017), 'Sending a naked selfie can be a criminal offence — but not many teenagers know this' The Conversation. Published on 27 September 2017. Available at: https://theconversation.com/sending-a-naked-selfie-can-be-a-criminal-offence-but-not-many-teenagers-know-this-84149

Asociación de Telefonia Móvil (n.d.). Available at: https://atelmo.cl

Australia, *Enhancing Online Safety Act 2015* (Cth) Available at: *https://www.legislation.gov.au/Details/C2017C00187*

Australian Government (2013), 'National Plan to Combat Cybercrime'. Available at: *https://www.homeaffairs.gov.au/crime/Documents/national-plan-combat-cybercrime.pdf*

Australian Government, Office of the E-Safety Commissioner (n.d), "About the Office". Available at: *https://www.esafety.gov.au/about-the-office*

Australian Government (2018), 'Online Safety Consultative Working Group'. Available at: *https://www.directory.gov.au/portfolios/communications-and-arts/australian-communications-and-media-authority/esafety-commissioner/online-safety-consultative-working-group*

Australian Senate, Legal and Constitutional Affairs References Committee (2018), "Adequacy of existing offences in the Commonwealth Criminal Code and of state and territory criminal laws to capture cyberbullying". Available at: *https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Cyberbullying/Report*

Austrian Federal Ministry for Digital and Economic Affairs (2017) "Digital Road Map Austria". Available at: *https://www.digitalroadmap.gv.at/en/*

BBC Trending. (2018), 'Instagram tightens eating disorder filters after investigation' BBC News. Published on 12 December 2018. Available at: *https://www.bbc.com/news/blogs-trending-46505704*

Belgian Data Protection Authority (n.d.) "Je decide". Available at: *https://www.jedecide.be*

Better Internet for Kids, (n.d.). Available at: https://www.betterinternetforkids.eu/web/portal

Bonanno, R. A., & Hymel, S. (2013). Cyber bullying and internalizing difficulties: Above and beyond the impact of traditional forms of bullying. Journal of Youth and Adolescence, 42, 685–697. Available at: https://doi.org/10.1007/s10964-013-9937-1

Brooks, L. (2017), 'Suicide prevention plan needed for child victims of 'sextortion' – expert says'. The Guardian. Published on 29 November 2017. Available at: https://www.theguardian.com/society/2017/nov/29/suicide-prevention-plan-needed-for-child-victims-of-sextortion-expert-says

Byrne, J. and Burton, P. (2017), "Children as Internet Users: how can evidence better inform policy debate", Journal of Cyber Policy, 2(1), 39-52

Byrne, J., Kardefelt-Winther, D., Livingstone, S., Stoilova, M. (2016). Global Kids Online Research Synthesis, 2015-2016. UNICEF Office of Research Innocenti and London School of Economics and Political Science. Available at: https://www.unicef-irc.org/publications/pdf/IRR_2016_01.pdf

Campbell M., and Bauman S., (2017), 'Cyberbullying: Definition, consequences and prevalence', in Reducing Cyberbulling in Schools: International Evidence-Based Best Practices, Elsevier Science & Technology

Campbell, M. A., Slee, P. T., Spears, B., Butler, D., & Kift, S. (2013). Do cyberbullies suffer too? Cyberbullies' perceptions of the harm they cause to others and to their own mental health. School Psychology International, 34, 613–629. Available at: https://doi. org/10.1177/0143034313479698.

Campbell, A (2017) Rethinking Children's advertising policies for the digital age. https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=2969&context=facpub

Canadian Government, Innovation, Science and Economic Development Canada, (2016) "Innovation and Skills Plan: Technology". Available at: https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00051.html

Canadian Government, Public Safety Canada (2018), "National Cyber Security Strategy". Available at: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx#s14

Chan, P. (2009) Psychosocial implications of homophobic bullying in schools: a review and directions for legal research and the legal process, The International Journal of Human Rights, 13(2-3), 143-175

Chanel 4, (2017), 'C4 study reveals only 4% surveyed can identify true or fake news'. Published on 6 February 2017. Available at: http://www.channel4.com/info/press/news/c4-study-reveals-only-4-surveyed-can-identify-true-or-fake-news

Child Focus (n.d.). Available at: http://www.childfocus.be/fr

Children's Rights International Network (n.d.) 'Minimum Ages of Criminal Responsibility Around the World'. Available at: https://www.crin.org/en/home/ages

Chilean Government, Centre for Education and Technology (n.d.), "ENLANCES". Available at: http://www.enlaces.cl

Committee on the Rights of the Child (2014), "Annex III: Recommendations from the 2014 day of general discussion on children's rights and digital media". Available at: https://www.ohchr.org/en/hrbodies/crc/pages/discussion2014.aspx

Committee on the Rights of the Child (2014), "Day of General Discussion: Digital Media and Children's Rights". Available at: https://www.ohchr.org/en/hrbodies/crc/pages/discussion2014.aspx

Council of Europe (2009), Recommendation **CM/REC(2009)5** of the Committee of Ministers to member states on measures to protect children against harmful content and behaviour and to promote their active participation in the new information and communications environment (Adopted by the Committee of Ministers on 8 July 2009 at the 1063rd meeting of the Ministers' Deputies). Available at https://wcd.coe.int/ViewDoc.jsp?id=1470045&Site=CM

Council of Europe (2016a), 'Drafting Group of Specialists on Children and the Digital Environment'.

Available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806cbf8e

Council of Europe (2016b), 'Strategy for the Rights of the Child (2016 -2021)'. Available at: https://rm.coe.int/168066cff8

Council of Europe (2017a), "Ad hoc Committee on the Rights of the Child, Children with Disabilities and Digital Media The Case for Research" Available at: https://rm.coe.int/09000016806fe6bb

Council of Europe (2017b), "Ad hoc Committee on the Rights of the Child, Drafting Group of Specialists on Children and the Digital Environment: Participation of Children in the development of Guidelines for member States to empower, protect and support children in the digital environment.". Available at: https://rm.coe.int/09000016806ff44d

Council of Europe (2018), Recommendation of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment CM/Rec (2018)7 available at: https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a

Crawford, A. (2014), ''Sextortion' Suspects deny involvement in Daniel Perry Case'. BBC News. Published on 19 December 2014. Available at: https://www.bbc.com/news/technology-30494566

Cross, D., Shaw, T., Hearn, L., Epstein, M., Monks, H., Lester, L., & Thomas, L. (2009). 'Australian covert bullying prevalence study (ACBPS)'. Western Australia: Report prepared for the Department of Education, Employment and Workplace Relations (DEEWR). Available at: https://docs.education.gov.au/system/files/doc/other/australian_covert_bullying_prevalence_study_executive_summary.pdf

Dean, M (2012), "The Story of Amanda Todd", The New Yorker, Published 18 October 2012. Available at: https://www.newyorker.com/culture/culture-desk/the-story-of-amanda-todd

DeNardis, L., & Hackl, A. M. (2015). Internet governance by social media platforms. Telecommunications Policy, 39(9), 761–770.

De La Pava, B., Chernyavskaya, A. and Livingstone S. (2015) 'Children, Advertising and the Internet'. Available at: http://blogs.lse.ac.uk/mediapolicyproject/topic-guides/children-advertising-and-the-internet/

Dinh, T., Farrugia, L., O'Neill, B., Vandoninck, S., & Velico, A. (2016) "INSAFE Helplines: Operations, effectiveness and emerging issues for internet safety helplines". Available at: https://www.lse.ac.uk/media@lse/research/EUKidsOnline/EUKidsIV/PDF/Helpline-insafe-report.pdf

Digital Champions Belgium (2018). Available at: https://www.digitalchampions.be/digitalchampions/

Dooley, J., Pyżalski, J., & Cross, D. (2009), 'Cyberbullying versus face-to-face bullying: A theoretical and conceptual review' Journal of Psychology, 217, 182–188. Available at: https://doi. org/10.1027/0044-3409.217.4.182

European Commission, (2016), 'Study on the impact of marketing through social media, online games and mobile applications on children's behaviour'. Available at: https://ec.europa.eu/info/publications/study-impact-marketing-through-social-media-online-games-and-mobile-applications-childrens-behaviour_en

European Commission (2018), "A European Strategy for a Better Internet for Children". Available at: https://ec.europa.eu/digital-single-market/node/286

European Commission (2018) "Safer Internet Centres". Available at: https://ec.europa.eu/digital-single-market/en/safer-internet-centres

European Commission, (3 December 2018), 'Second report on the progress made in the fight against trafficking in human beings (2018) as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims'. Available at:

https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20181204_com-2018-777-report_en.pdf

European Parliament and Council (2006), Communication 2012/0196 of the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the European Strategy for a Better Internet for Children Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2012%3A0196%3AFIN

Francisco Lupiáñez-Villanueva et al., Study on the impact of marketing through social media, online games and mobile applications on children's behaviour, EUROPEAN COMM'N 151-56 (Mar. 2016), available at http://ec.europa.eu/consumers/consumer_evidence/behavioural_research/docs/final_report_impact_marketing_children_final_version_approved_en.pdf

German Government, (2017), Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act). Available at: https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf;jsessionid=829D39DBDAC5DE294A686E374126D04E.1_cid289?__blob=publicationFile&v=2

Gillespie, A. (2013) 'Adolescents, Sexting and Human Rights', Human Rights Law Review, 13(4), 623-643

Global Privacy Enforcement Network (n.d.). Available at: https://www.privacyenforcement.net

Görzig, A., and Machackova, H. (2015), 'Cyberbullying from a socio-ecological perspective: A contemporary synthesis of findings from EU Kids Online' MEDIA@LSE Working Paper Series. Available at: http://www.lse.ac.uk/media-and-communications/assets/documents/research/working-paper-series/EWP36.pdf

GRETA, (7 October 2016) 'Report concerning the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings by the United Kingdom'. Available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806abcdc

GRETA (May 2018), 'Trafficking in Children: Thematic Report of the 6th General Report on GRETA's Activities'. Available at: https://rm.coe.int/1680706a42

Grigonis, H. (2017). Cyberbullying happens more often on Instagram, a new survey suggests. Digital trends (July 20). https://www.digitaltrends.com/social-media/cyberbullying-statistics-2017-ditch-the-label/ .

Hooft Graafland, J. (2018), "New technologies and 21st century children: Recent trends and outcomes", OECD Education Working Papers, No. 179, OECD Publishing, Paris, http://dx.doi.org/10.1787/e071a505-en

Hungarian Government (2016), "Digital Child Protection Strategy". Available at: https://digitalisjoletprogram.hu/files/c2/61/c2610c5560ef56425860d4d7bdd68b3d.pdf

INHOPE (2017), "Annual Report". Available at: http://www.inhope.org/Libraries/Annual_reports/INHOPE_Annual_Report_2017.sflb.ashx

International Conference on Data Protection and Privacy Commissioners, International Working Group on Digital Education (2017), 'Report of the International Working Group Concerning Digital Education September 2017'. Available at: https://icdppc.org/wp-content/uploads/2017/12/DEWG-Research-Paper-Canada-eplatforms_Sept-2017.pdf

Internet Governance Forum (n.d.) "Dynamic Coalition on Child Online Safety". Available at: https://www.intgovforum.org/multilingual/content/dynamic-coalition-on-child-online-safety

Interpol (n.d.) 'Online Safety – Sextortion'. Available at: https://www.interpol.int/Crime-areas/Cybercrime/Online-safety/Sextortion

Japanese Government (2015), "The Third Basic Plan on Measures for Providing Safe and Secure Internet Use for Young People". Available at: http://www8.cao.go.jp/youth/youth-harm/suisin/pdf/dai3ji_keikaku_eng.pdf

Jha, M. (2019), 'The Dark Hand of Tech That Strokes Sex Trafficking in India' Factor Daily. Published on 25 February 2019. Available at: https://factordaily.com/tech-phone-calls-whatsapp-facebook-sex-trafficking-india/

Johnson, M., Mishna, F., Okumu, M., Daciuk, J. Non-Consensual Sharing of Sexts: Behaviours and Attitudes of Canadian Youth, Ottawa: MediaSmarts 2018. Available at: http://mediasmarts.ca/digital-media-literacy/digital-issues/sexting/sharing-sexts

Klomek, A. B., Sourander, A., & Gould, M. S. (2011). Bullying and suicide: Detection and intervention. Psychiatric Times, 28(2), 27–31.

Lansdown, Gerison, (2001), 'Promoting Children's Participation in Democratic Decision-Making', UNICEF Office of Research, Florence. Available at: https://www.unicef-irc.org/publications/pdf/insight6.pdf

Lanzarotte Committee (2019), 'Opinion of the Lanzarote Committee on child sexually suggestive or explicit images and/or videos generated, shared and received by children'. Available at: https://rm.coe.int/opinion-of-the-lanzarote-committee-on-child-sexually-suggestive-or-exp/168094e72c

Latvian Government (2014), "National Cyber Security Strategy 2014-2018". Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/latvian-national-cyber-security-strategy

Latvian Government (2014), "Policy Guidelines on the Information Society 2014-2020". Available at: http://www.varam.gov.lv/eng/darbibas_veidi/e_gov/?doc=13058

Levin, S (2016), 'New Mexico teens can now legally sext each other and exchange nude photos', The Guardian. Published on 26 February 2016. Available at: https://www.theguardian.com/us-news/2016/feb/26/new-mexico-legalizes-teen-sexting

Livingstone, S. (2017) "Children: a special case for privacy?" Intermedia, 46 (2) pp. 18-23. Available at http://eprints.lse.ac.uk/89706/

Livingstone, S., and Haddon, L. (2009), "EU Kids Online: Final report". LSE, London: EU Kids Online. (EC Safer Internet Plus Programme Deliverable D6.5). Available at www.lse.ac.uk/collections/EUKidsOnline/Reports/EUKidsOnlineFinalReport.pdf

Livingstone, S., O'Neill, B., and Mclaughlin, S (2011) 'Final recommendations for policy, methodology and research'. EU Kids Online network, London, UK. Available at: http://eprints.lse.ac.uk/39410/

Livingstone, S. and Görzig, A., (2014) 'When adolescents receive sexual messages on the internet: explaining experiences of risk and harm'. Computers in Human Behavior, 33. pp. 8-15. Available at: http://eprints.lse.ac.uk/55630/

Livingstone, S., Haddon, L., Vincent, J., Mascheroni, G. and Ólafsson, K. (2014a). 'Net Children Go Mobile: The UK Report'. London: London School of Economics and Political Science. Available at: http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20III/Reports/EUKidsOnline-NetChildrenGoMobile.pdf

Livingstone, S, Kirwall, L., Ponte, C. and Staksrud, E. (2014b), 'In their own words: what bothers children online?' European Journal of Communication, 29(3), 271-288. Available at: http://eprints.lse.ac.uk/62093/1/In_their_own.pdf

Livingstone, S., Carr, J. and Byrne, J. (2016a). "One in Three: Internet Governance and Children's Rights." Innocenti Discussion Paper No.2016-01, UNICEF Office of Research, Florence. Available at: https://www.unicef-irc.org/publications/pdf/idp_2016_01.pdf

Livingstone, S., Stoilova, M., and Kelly A. (2016b) 'Cyberbullying: incidence, trends and consequence', in Ending the Torment: Tackling Bullying from the Schoolyard to Cyberspace. United Nations Office of the Special Representative of the Secretary-General on Violence against Children, New York, USA, pp. 115- 120. Available at:

http://eprints.lse.ac.uk/68079/1/Livingstone_Cyberbullying%20incidence%20trends_2016.pdf

Livingstone, S., Lansdown, G., & Third, A. (2017) 'The Case for a UNCRC General Comment on Children's Rights and Digital Media: A report prepared for Children's Commissioner for England". Available at: https://www.childrenscommissioner.gov.uk/wp-content/uploads/2017/06/Case-for-general-comment-on-digital-media.pdf

Livingstone, S., Stoilova, M., and Nandagiri, R., (2018) Conceptualising privacy online: what do, and what should, children understand? Parenting for a Digital Future (06 Sep 2018), pp. 1-4. Blog Entry. Available at: http://eprints.lse.ac.uk/90228/

Livingstone, S., Tambini, D., Belakova, N., Goodman, E., (2018). Protection of children online, does current regulation deliver? Media Policy Brief 21. London: Media Policy Project, London School of Economics and Political Science. Available at: http://eprints.lse.ac.uk/90731/1/Livingstone_Protection-of-children_Author.pdf

Martellozzo, E., Monaghan, A., Adler, J.R., Davidson, J., Leyva, R. and Horvath, M.A.H. (2016) I wasn't sure it was normal to watch it. London: NSPCC. Available at: https://learning.nspcc.org.uk/research-resources/2016/i-wasn-t-sure-it-was-normal-to-watch-it/

Meyer, M., Adkins, V., Yuan, Y., Weeks, H.M., Chang, Y., Radesky, P. (2019), "Advertising in Young Children's Apps: A Content Analysis", Journal of Developmental and Behavioural Pediatrics 40, 32-39

Milosevic T (2016) Social Media Companies' Cyberbullying Policies, International Journal of Communication 10(2016), 5164–5185

Muthanna, S. Burbridge, V, El Asam, A. Foody, M. Smith, P.K., and Morsi, H., (2017) 'Bullying and Cyberbullying : Their legal status and Use in Psychological Assessment' Int J Environ Res Public Health. 2017 Dec; 14(12): 1449. Available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5750868/pdf/ijerph-14-01449.pdf Select Committee on Communications HoL. Social Media and Criminal Offences; HL 37, First Report of Session 2014–2015; TSO (The Stationery Office): London, UK, 2014.

New Zealand Government, Consumer Protection (n.d.) 'Harmful Digital Communications Act'. Available at: https://www.consumerprotection.govt.nz/general-help/laws-policies/online-safety/harmful-digital-communications-act/

New Zealand Government, (n.d.), "Netsafe". Available at: https://www.Netsafe.org.nz

Norwegian Consumer Council, (6 December 2016), 'Connected toys violate European consumer laws. Available at: https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/

Norwegian Consumer Council, (18 October 2017), 'Significant Security Flaws in Smartwatches for Children'. Available at: https://www.forbrukerradet.no/side/significant-security-flaws-in-smartwatches-for-children/

Nyst, C. (2017), 'Privacy, protection of personal information and reputation rights,' Children's Rights and Business in a Digital World Discussion Paper Series, United Nations Children's Fund. Available at: https://www.unicef.org/csr/css/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf

OECD (2011), "The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them", OECD Digital Economy Papers, No. 179, OECD, Paris. Available at: https://doi.org/10.1787/5kgcjf71pl28-en

OECD (2019), OECD – University of Zurich Expert Consultation "Protection of Children in a Connected World" - 15-16 October, University of Zurich, Zurich, Switzerland. Available at: DSTI/CDEP/SPDE(2019)3

Ofcom (2017), "Children and Parents: Media Use and Attitudes Report". Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0034/93976/Children-Parents-Media-Use-Attitudes-Report-2016.pdf

Ofcom (2017), "Children and Parents: Media Use and Attitudes Report". Available at:

https://www.ofcom.org.uk/__data/assets/pdf_file/0020/108182/children-parents-media-use-attitudes-2017.pdf

Ofcom (2018), "Children and Parents: Media Use and Attitudes Report". Available at: https://www.ofcom.org.uk/__data/assets/pdf_file/0024/134907/Children-and-Parents-Media-Use-and-Attitudes-2018.pdf

Office of the Privacy Commissioner of Canada (2017), “2017 Global Privacy Enforcement Network Sweep”. Available at: https://www.priv.gc.ca/en/about-the-opc/what-we-do/international-collaboration/international-privacy-sweep/2017_result/

Oltermann, P. (2018) “Tough new German law puts tech firms and free speech in spotlight” The Guardian. Published on 5 January 2018. Available at: https://www.theguardian.com/world/2018/jan/05/tough-new-german-law-puts-tech-firms-and-free-speech-in-spotlight

O’Neill, B., Dinh, T. (2018). “The Better Internet for Kids Policy Map: Implementing the European Strategy for a Better Internet for Children in European Member States”. Available at: https://www.betterinternetforkids.eu/bikmap

Perren, S., Dooley, J., Shaw, T., & Cross, D. (2010). Bullying in school and cyber-space: Associations with depressive symptoms in Swiss and Australian adolescents. Child and Adolescent Psychiatry and Mental Health, 4(1), 1–10. Available at: https://doi. org/10.1186/1753-2000-4-28.

PREVNet (2018), ‘Legal Consequences of Cyberbullying’. Available at: https://www.prevnet.ca/bullying/cyber-bullying/legal-consequences

Privacy International (2016), “Discussion about Cyber Security in Colombia”. Available at: https://privacyinternational.org/feature/1145/discussion-about-cyber-security-colombia

Republic of Poland (2013), “Cyberspace Protection Policy of the Republic of Poland”. Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf

Republic of Slovenia (2016), “Digital Slovenia 2020 – Development Strategy for the Information Society until 2020”. Available at: http://www.mju.gov.si/fileadmin/mju.gov.si/pageuploads/DID/Informacijska_druzba/pdf/DSI_2020_3-2016_pic1.pdf

Reyes, I., Wijesekera, P., Reardon J., Elazari Bar On, A., Razaghpanah, A., Vallina-Rodriguez, N., and Egelman, S. "Won't Somebody Think of the Children" Examining Coppa Compliance at Scale” Proceedings of the Privacy Enhancing Technologies Symposium (PETS'18), 2018, pp. 63-83. Available at: https://www.appcensus.mobi/documents/pets18.pdf

Reuters, ‘Grooming is Gateway to child sex trafficking as predators go online’ The Strait Times. Published on 17 June 2018. Available at: https://www.straitstimes.com/world/americas/grooming-is-gateway-to-child-sex-trafficking-as-predators-go-online

Spanish Government (2013), “National Cyber Security Strategy”. Available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/the-national-security-strategy

Spears, B., Taddeo, C., Swirski, T., Keeley, M., Katz, I., Collin, P., Daly, T., & Bates, S. (2014). ‘Research on youth exposure to, and management of, cyberbullying incidents in Australia: Part C–An evidence-based assessment of deterrents to youth cyberbullying - Appendix A (SPRC Report 12/2014)’. Sydney: Social Policy Research Centre, UNSW Australia. Available at: https://www.sprc.unsw.edu.au/media/SPRCFile/Youth_exposure_to_and_management_of_cyberbullying_in_Australia_Part_C_Appendix_A.pdf

Sticca, F., & Perren, S. (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, 42, 739–750. Available at: https://doi.org/10.1007/ s10964-012-9867-3.

Strohmaier, H., Murphy, M. & DeMatteo, D. (2014), 'Youth Sexting: Prevalence Rates, Driving Motivations, and the Deterrent Effect of Legal Consequences' Sexual Research and Social Policy, 11 (3), 245-255

Thompson, S. (2014), 'Sexting Prosecutions: Minors as a Protected Class from Child Pornography Charges' University of Michigan Journal of Law Reform Caveat, 48(1), 11-19. Available at: https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1039&context=mjlr_caveat

THORN, (January 2018) 'Survivor Insights: The Role of Technology in Domestic Minor Sex Trafficking'. Available at: https://www.thorn.org/wp-content/uploads/2018/06/Thorn_Survivor_Insights_061118.pdf

UK Council for Child Internet Safety (UKCCIS). Available at: https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

UK Council for Child Internet Safety (2015), 'Child Safety Online: A Practical Guide for Providers of Social Media and Interactive Services'. Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/487973/ukccis_guide-final__3_.pdf

UK Government (2017), "Internet Safety Strategy – Green Paper". Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/650949/Internet_Safety_Strategy_green_paper.pdf

UK Government (2019), 'Age-Appropriate Design Code – Version 1.0 for Public Consultation (15/04/2019 – 31/05/2019)' at p. 93. Available at: https://ico.org.uk/media/about-the-ico/consultations/2614762/age-appropriate-design-code-for-public-consultation.pdf

UK Government (2019), "Online Harms White Paper". Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf

UK Government, Select Committee on Communications HoL. Social Media and Criminal Offences; HL 37, First Report of Session 2014–2015; TSO (The Stationery Office): London, UK, 2014. Available at: https://publications.parliament.uk/pa/ld201415/ldselect/ldcomuni/37/3702.html

UNICEF (2018) 'Children and Digital Marketing: Rights, risks and responsibilities'. Available at: https://www.unicef.org/csr/css/Children_and_Digital_Marketing_-_Rights_Risks_and_Responsibilities(2).pdf

UNICEF Innocenti. (2012) 'Child Safety Online: Global Challenges and Strategies. Technical report.' United Nations Children's Fund. UNICEF. http://www.unicef-irc.org/publications/pdf/ict_techreport3_eng.pdf.

UNICEF (USA) (11 January 2018), 'Innocent Victims: The Fight Against Child Sex Trafficking'. Available at: https://www.unicefusa.org/stories/innocent-victims-fight-against-online-child-sex-trafficking/33866

UNODC, (2018) Global Report on Trafficking in Persons (at 38), the United Nations Office on Drugs and Crimes. Available at: https://www.unodc.org/documents/data-and-analysis/glotip/2018/GLOTiP_2018_BOOK_web_small.pdf

US Department of Justice (2016), 'The National Strategy for Child Exploitation Prevention and Interdiction'. Available at: https://www.justice.gov/psc/file/842411/download

U.S. Department of Justice, Federal Bureau of Investigation, '(2015) Sextortion of Children in the United States: A Fact Sheet for Parents and Children'. Available at: https://www.fbi.gov/file-repository/stop-sextortion-brochure.pdf

US Government, Federal Trade Commission (2015), 'Complying with COPPA: Frequently Asked Questions'. Available at: https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

US Government, Federal Trade Commission (2012), 'FTC's revised COPPA Rule: Five need-to-know changes for your business'. Available at: https://www.ftc.gov/news-events/blogs/business-blog/2012/12/ftcs-revised-coppa-rule-five-need-know-changes-your-business

United States Senate, 'Backpage.com's knowing facilitation of online sex trafficking'. Available at: https://www.portman.senate.gov/public/index.cfm/files/serve?File_id=5D0C71AE-A090-4F30-A5F5-7CFFC08AFD48

Van Der Hof, S. (2017) "I Agree… Or Do I? – A Rights Based Analysis of the Law on Children's Consent in the Digital World" Wisconsin International Law Journal. Available at: http://hosted.law.wisc.edu/wordpress/wilj/files/2017/12/van-der-Hof_Final.pdf

Viola de Azevedo Cunha, M. (2017) "Child Privacy in the Age of Web 2.0 and 3.0: Challenges and Opportunities for Policy" Innocenti Discussion Paper 2017-03. UNICEF Office of Research – Innocenti. Available at: https://www.unicef-irc.org/publications/pdf/Child_privacy_challenges_opportunities.pdf

Wakefield, J. (2017). Instagram tops cyber-bullying study. BBC (July 19). http://www.bbc.co.uk/news/technology-40643904

Waterson, J. (1 March 2019). Momo hoax: schools, police and media told to stop promoting viral challenge. The Guardian. https://www.theguardian.com/technology/2019/feb/28/schools-police-and-media-told-to-stop-promoting-momo-hoax

Wittes, B (2017), 'Cyber Sextortion and International Justice' Georgetown Journal of International Law 48 (3), 941- 948

Wolak, J., Finkelhor, D., Walsh, W., & Treitman, L. (2017) 'Sextortion of Minors: Characteristics and Dynamics' Journal of Adolescent Health, 62(1), 72-79

Notes

[1] The OECD in 2020 has revised the Typology of Risks. For further information see 'OECD Draft Recommendation on Children in the Digital Environment: Revised Typology of Risks', available at: https://one.oecd.org/document/DSTI/CDEP/DGP(2020)3/en/pdf

[2] As per paragraph I(i) of the 2012 Recommendation, the term 'Children' encompasses all persons aged under the age of 18. This report recognizes the differing needs of children at the different stages of their development, and specifically notes this where necessary. As the recommendation and this report covers both young children and adolescents, as far as possible the term 'minors' will be used throughout. Where the discussion relates specifically to a certain age group (*i.e.* very young children, adolescents) this is specified. Where a particular report / document uses the term children, or young people or both, that has largely been maintained throughout.

[3] Australia, Austria, Belgium, Canada, Chile, Colombia, Costa Rica, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Israel, Italy, Japan, Latvia, Lithuania, Luxembourg, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Russian Federation, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom , and the United States.

[4] Available at, *https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/copy_of_PO_NCSS.pdf*

[5] Available at, *https://embamex.sre.gob.mx/italia/images/pdf/national%20digital%20strategy.pdf*

[6] Available at, *https://www.digitalroadmap.gv.at/fileadmin/downloads/digital_road_map_broschuere.pdf*

[7] It is noted that at the time of writing this report, the United Kingdom had released a Green Paper on developing an Internet Safety Strategy (October 2017) envisaging the creation of a Digital Charter and a number of measures designed to centralize and streamline legal and policy responses.

[8] This mapping covered all countries participating in the EU's "Strategy for a Better Internet for Children", which includes all member States of the EU as well as Iceland, Norway and the Russian Federation.

[9] Austria's explanatory memorandum to the draft Government Bill before amending their law specifically referenced the suicide of Canadian teen Amanda Todd. In their response to the survey, Italy noted an upswing in suicide attempts due to cyber bullying.

[10] See also OECD Education Working Paper No. 179, 'New Technologies and 21st Century Children: Recent Trends and Outcomes' at part 2, outlining the findings of a 2015 OECD survey. Notably, 95% of 15 year olds were found to have access to Internet at home, an increase from 75% in 2006 (at page 8).

[11] See for example, the UK Safer Internet Centre, at: https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues.

[12] Ibid, at 94(a)

[13] See, https://www.lawcom.gov.uk/abusive-and-offensive-online-communications/

[14] See, https://rm.coe.int/norway-nationalreporting-en/pdf/16808a38de at page 3

[15] A regularly updated list of state level cyberbullying laws is available at, *www.laws.cyberbullying.org/bullying-laws*

[16]See, the *Megan Meier Cyberbullying Prevention Act,* available at: *www.govtrack.us/congress/bills/111/hr1966/text*

[17] See, *https://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000037289658&cidTexte=LEGITEXT000006070719&dateTexte=20180806*

[18] Information provided by CNIL (June 2019)

[19] See Harmful Digital Communications Act 2015, s22

[20] See Harmful Digital Communications Act 2015, s19

[21] For further information see, *https://www.prevnet.ca/bullying/cyber-bullying/legal-consequences* Whilst the exams given here relate to Canada's federal laws, several provinces and territories also have laws dealing with online and offline bullying.

[22] See, *https://www.esafety.gov.au/complaints-and-reporting/cyberbullying-complaints*

[23] *Enhancing Online Safety Act* 2015 (Cth), s42.

[24]Available in English at, *https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf;jsessionid=829D39DBDAC5DE294A686E374126D04E.1_cid289?__blob=publicationFile&v=2*

[25] See, Australian Senate (2018) at 5.23-5.31

[26] See, UK Government Online Harms White Paper (April 2019), at p. 53. Available at: *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf*

[27] See, *https://www.theguardian.com/politics/2019/jan/26/matt-hancock-facebook-social-media-suicide-self-harm-young-people* Letter available at: *https://twitter.com/MattHancock/status/1089864139835670528*

[28]See, UK Government Online Harms White Paper (April 2019). Available at: *https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf*

[29] For example, in England and Wales children may be held liable for criminal offences from the age of 10 years (Children and Young Persons Act 1933, s50); and Turkey places the age of criminal responsibility at 12 (Criminal Code, art. 31(1)(2). Comprehensive global information on the minimum age of criminal responsibility is available at: *https://www.crin.org/en/home/ages*

[30] Livingstone, S., M. Stoilova and A. Kelly (2016), "Cyberbullying: incidence, trends and consequence", in *Ending the Torment: Tackling Bullying from the Schoolyard to Cyberspace.*, United Nations Office of the Special Representative of the Secretary-General on Violence against Children, New York, http://eprints.lse.ac.uk/68079/

[31] See for example, discussion in the Amicus brief filed by the Juvenile Law Centre in the *State of Washington v. E.G.* from p14, available at: *https://jlc.org/sites/default/files/case_files/2015.11.30%20Gray%20Amicus%20Brief.pdf*

[32] See, *https://theconversation.com/sending-a-naked-selfie-can-be-a-criminal-offence-but-not-many-teenagers-know-this-84149*

[33] See, *https://www.theguardian.com/us-news/2016/feb/26/new-mexico-legalizes-teen-sexting*

[34] See, *https://rm.coe.int/opinion-of-the-lanzarote-committee-on-child-sexually-suggestive-or-exp/168094e72c*

[35] Spanish Penal Code, at art. 197.7

[36] See, *https://www.interpol.int/Crime-areas/Cybercrime/Online-safety/Sextortion*

[37] See, https://www.justice.gov/psc/file/842411/download

[38] See, *https://www.fbi.gov/file-repository/stop-sextortion-brochure.pdf*

[39] See, *https://www.theguardian.com/society/2017/nov/29/suicide-prevention-plan-needed-for-child-victims-of-sextortion-expert-says*

[40] See, *https://www.bbc.com/news/technology-30494566*

[41] For further information, see: *https://www.eff.org/deeplinks/2018/12/congress-censors-internet-eff-continues-fight-fosta-2018-review*; and *https://www.eff.org/deeplinks/2019/02/fosta-already-leading-censorship-we-are-seeking-reinstatement-our-lawsuit*

[42] Further information available at, *https://www.eff.org/deeplinks/2018/12/congress-censors-internet-eff-continues-fight-fosta-2018-review*

[43] GRETA, 'Report concerning the implementation of the Council of Europe Convention on Action against Trafficking in Human Beings by the United Kingdom' at 302

[44] THORN, 'Survivor Insights: The Role of Technology in Domestic Minor Sex Trafficking', at p 23-27, 39-41

[45] United States Senate, Hearing Before the Permanent Subcommittee on Investigations of the Committee on Homeland Security and Governmental Affairs, First Session, November 19, 2015, at p. 2. Available at: *https://www.govinfo.gov/content/pkg/CHRG-114shrg98445/pdf/CHRG-114shrg98445.pdf*

[46] Reuters, 'Grooming is Gateway to child sex trafficking as predators go online' *The Strait Times*. Published on 17 June 2018

[47] European Commission, (3 December 2018), 'Second report on the progress made in the fight against trafficking in human beings (2018) as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims' at p. 3

[48] GRETA, 'Trafficking in Children: Thematic Report of the 6th General Report on GRETA's Activities' at p. 13

[49] For example, the Palermo Protocol, the 2nd optional protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution, and Child Pornography, and the Lanzarote Convention, the EU Anti-Trafficking Directive (2011/36/EU).

[50] E-Commerce Directive, 2001/31/EC, at Art. 12(1)

[51] *Google Inc. V Duffy [*2017] SASCFC 130

[52] *Trkuija v. Google LLC* [2018] HCA 25

[53] *Weaver v. Corcoran* 2015 BSCS 165; See also, *Baglow v Smith* 2015 ONSC 1175, where a similar conclusion was reached.

[54]Available in English at, https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf;jsessionid=829D39DBDAC5DE294A686E374126D04E.1_cid289?__blob=publicationFile&v=2

[55] Ibid, at s1(3); German Criminal Code, s184b

[56] See, https://factordaily.com/tech-phone-calls-whatsapp-facebook-sex-trafficking-india/

[57] See, https://factordaily.com/tech-phone-calls-whatsapp-facebook-sex-trafficking-india/

[58] See, https://www.theguardian.com/technology/2019/jan/21/whatsapp-limits-message-forwarding-fight-fake-news

[59] See, UK Government, Internet Safety Strategy – Green Paper (2017) at 48.

[60] See, UK Government, Internet Safety Strategy – Green Paper (2017) at 49.

[61] See, http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54300

[62] See, https://ec.europa.eu/information_society/newsroom/image/document/2016-50/factsheet-code-conduct-8_40573.pdf

[63] See Harmful Digital Communications Act 2015, ss 19, 22

[64] Lithuania response to the OECD survey.

[65] See for example, http://www.lgl.lt/en/?p=8646

[66] See, UK Government, Internet Safety Strategy – Green Paper (2017) at 48

[67] See, http://www.channel4.com/info/press/news/c4-study-reveals-only-4-surveyed-can-identify-true-or-fake-news

[68] See, UK Government, Internet Safety Strategy – Green Paper (2017) at 48

[69] See, https://esafety.gov.au/youngandesafe/question

[70] See, http://english.nmhh.hu/article/202183/What_is_fake_news_Educational_materials_have_been_prepared_by_National_Media_and_Infocommunications_Authority_NMHH_for_the_European_Media_Literacy_Week

[71] See, Věra Jourová, Fact Sheet on The impact of online marketing on children's behavior, (May 2016), available at http://ec.europa.eu/consumers/consumer_evidence/behavioural_research/docs/online_marketing_factsheet_2016_en.pdf

[72] See, Digital Economy Act 2017, s14

[73] See, Digital Economy Act 2017, s94

[74] See, Deliberation n° 2011-64 of 20 December 2011 and Law n° 30/091 of 1986, art. 2

[75] See, http://www.loc.gov/law/foreign-news/article/russia-protection-of-children-from-harmful-information/

[76] See, https://www.bbc.com/news/technology-20096274

[77]Further information, available at: https://www.statensmedierad.se/ovrigt/inenglish.579.html

[78] Audiovisual Media Services Directive (EU) 2018/1808, preamble at (1)

[79] Ibid at Arts. 6a, 9, 28b

[80] See, http://www.pewinternet.org/2018/05/31/teens-social-media-technology-2018/

[81] See, UK Government, Internet Safety Strategy – Green Paper (2017) at 47.

[82] See, http://blogs.lse.ac.uk/mediapolicyproject/topic-guides/children-advertising-and-the-internet/

[83] See, European Commission, (2016), 'Study on the impact of marketing through social media, online games and mobile applications on children's behaviour'

[84] See, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/288360/oft1519.pdf

[85] See, https://iccwbo.org/publication/icc-advertising-and-marketing-communications-code/

[86] See, Federal Trade Commission (2013), Children's Online Privacy Protection Rule; Final Rule. Available at: https://www.ftc.gov/system/files/2012-31341.pdf

[87] See, https://www.ftc.gov/news-events/blogs/business-blog/2019/02/largest-ftc-coppa-settlement-requires-musically-change-its

[88] An example of a self-regulatory body is the US based Children's Advertising Review Unit which specifically recognizes that Advertisers have special responsibilities when advertising to children or collecting data from children online in their core principles. Information available at:

http://www.caru.org/guidelines/index.aspx

[89] See, https://commercialfreechildhood.org/action/hell-no-barbie-8-reasons-leave-hello-barbie-shelf

[90] See, https://www.forbrukerradet.no/side/significant-security-flaws-in-smartwatches-for-children/

[91] See, https://www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws/

[92] See, https://www.cnil.fr/fr/jouets-connectes-quels-conseils-pour-les-securiser

[93] See, https://www.dataprotectionauthority.be/berlin-group

[94] See, https://icdppc.org/wp-content/uploads/2019/03/dewg-resolution-adopted-20180918.pdf

[95] See, https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2017/17112017_Verbraucherschutz.html

[96] General Data Protection Regulation (EU) 2016/679, arts. 8, 38

[97] General Data Protection Regulation (EU) 2016/679, art. 57

[98] See, https://www.dataprotection.ie/en/news-media/latest-news/public-consultation-processing-childrens-personal-data-and-rights-children

[99] See, https://www.dataprotection.ie/sites/default/files/uploads/2018-12/DPC_ChildrensRights_2019_English.pdf at p. 9

[100] UK Government (2019), 'Age-Appropriate Design Code – Version 1.0 for Public Consultation (15/04/2019 – 31/05/2019)' at p. 93. Available at: https://ico.org.uk/media/about-the-ico/consultations/2614762/age-appropriate-design-code-for-public-consultation.pdf

[101] See, https://5rightsfoundation.com/uploads/5rightsaadcbriefing.pdf

[102] For further information see, *https://www.ftc.gov/news-events/blogs/business-blog/2012/12/ftcs-revised-coppa-rule-five-need-know-changes-your-business* and https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

[103] See the Report of the International Working Group Concerning Digital Education September 2017, at p 11

[104] For further information see, https://fpf.org/2019/01/23/keeping-students-safe-how-education-privacy-will-affect-the-next-decade-and-beyond/

[105] Australian Government, National Plan to Combat Cybercrime, at p. 5

[106] See, https://www.interpol.int/Crime-areas/Crimes-against-children/Crimes-against-children

[107] See, https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

[108] See, https://ec.europa.eu/digital-single-market/en/european-strategy-better-internet-children

[109] O'Neill and Dinh, 2018, p. 9, 10.

[110] Information provided in from the survey responses of Estonia, Finland and Italy. However see also Estonia's Digital Focus Policy, available at: *https://www.hm.ee/en/activities/digital-focus*; and Finland's Good Media Literacy National Policy Guidelines, available at: *http://julkaisut.valtioneuvosto.fi/handle/10024/75280*

[111] See, *Enhancing Online Safety Act 2015* (Cth) s(1)(b)(f)

[112] See, *https://www.dfi.dk/en/english/danish-film-agreement-place-2015-18*

[113]Information provided in from the survey responses of Finland, Lithuania and Luxembourg, however see also O'Neill & Dinh (2018) at p65, 66.

[114] See, *http://english.nmhh.hu/article/197197/Yes_awkward_the_new_campaign_of_the_NMHH_explains_online_infringements_using_emojis*

http://english.nmhh.hu/article/200672/Yes_awkward_campaign_reloaded_a_microsite_to_provide_guidance_and_vloggers_to_offer_advice_in_support_of_safer_internet_use_for_kids

[115] See, *https://magistere.education.fr*

[116] See for example, Hungary Magic Valley Media Education Centres. Information available at: *http://magicvalley.hu/*

[117] See, Hooft Graafland, J. (2018), "New technologies and 21st century children: Recent trends and outcomes", OECD Education Working Papers, No. 179, OECD Publishing, Paris, http://dx.doi.org/10.1787/e071a505-en

[118] See, *https://www.saferinternetday.org*

[119] See, *http://mediasmarts.ca/parents*

[120] See, *http://www.childfocus.be/fr/prevention/securite-en-ligne/parents*

[121] See for example Hungary's online guide, 'Understand your Kids!' available at: *http://english.nmhh.hu/article/194574/Understand_your_kids*

[122] Luxembourg response to the OECD Survey.

[123] Austria response to the OECD Survey.

[124] See, *https://ico.org.uk/media/about-the-ico/consultations/2614762/age-appropriate-design-code-for-public-consultation.pdf* at p. 98

[125] *E.g.* youth ambassadors from Egypt's youth Internet safety focus group "net-aman" (Livingston and Haddon, 2009, p. 23); Landsown (2001), at p. 4-8

[126] Information provided by Japan Delegation, May 2019.

[127] See, The OECD Privacy Framework, page 4. Available at: *http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf*

[128] See, UK Government, Internet Safety Strategy – Green Paper (2017) at 11. It is noted that at the time of writing this report, the UK Government is considering a change to the structure and remit of the UKCCIS to, *inter alia,* increase its work to cover all users of the internet.

[129] See, https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis#ukccis-achievements-include

[130] In Australia, the Online Safety Consultative Working Group; in the UK, the UK Council for Child Internet Safety (UKCCIS); and in Costa Rica, the National Council of Childhood and Adolescence and the National Commission on Online Safety.

[131] Further information available at: https://www.youtube.com/yt/about/policies/#community-guidelines

[132] Further information available at: https://transparencyreport.google.com/youtube-policy/removals

[133]Further information available at, https://support.google.com/youtube/answer/2801999?hl=en&ref_topic=2803176

[134] Further information available at: https://www.facebook.com/communitystandards/introduction

[135] Further information available at: https://www.snap.com/en-US/safety/safety-center/

[136] Further information available at: https://www.tiktok.com/community-guidelines?lang=en

[137] Further information available at: https://help.instagram.com/154475974694511

[138] BBC Trending. (2018), ‘Instagram tightens eating disorder filters after investigation’ *BBC News.* Published on 12 December 2018

[139] Further information available at: https://ec.europa.eu/digital-single-market/en/news/individual-company-statements-alliance-better-protect-minors-online

[140] See, *Enhancing Online Safety Act 2015* (Cth) Ss 15, 107

[141] See, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/

[142] See, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

[143] Norway response to OECD Survey.

[144] See, crianzatecnologica.org (Technological Upbringing).

[145] See, *https://www.betterinternetforkids.eu/fr/web/portal/home/-/asset_publisher/UkbOS3dmMlyU/content/id/1746696;jsessionid=EF7EA6CB608A40FA0BC44F85504C2B2A*; and https://www.theguardian.com/technology/2019/feb/28/schools-police-and-media-told-to-stop-promoting-momo-hoax

[146] *The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse* CETS 201 (2007)

[147] Further information available at: https://www.coe.int/en/web/children/2nd-monitoring-round

[148] The *Council of Europe Convention on Cybercrime* (ETS No. 185) (2004)

[149] Available at: https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a

[150] Further information available at:

[151] Available at: https://www.betterinternetforkids.eu

[152] Links to each country's SIC is available on the BIK website. The European Commission's policy page on SICs is available at: https://ec.europa.eu/digital-single-market/en/safer-internet-centres

[153] Further information available at: https://www.betterinternetforkids.eu/web/portal/practice/industry

[154] Further information available at: https://www.betterinternetforkids.eu/web/portal/practice/research

[155] Further information available at: https://www.betterinternetforkids.eu/web/portal/practice/youth

[156] Further information available at: https://www.betterinternetforkids.eu/web/portal/policy/safer-internet-forum

[157] Declaration of the 2012 APEC Telecommunications and Information Ministerial Meeting, at 29

[158] Available at: https://www.itu.int/en/cop/Pages/guidelines.aspx

[159] Further information on the work of the council is available at: https://www.itu.int/en/council/cwg-cop/Pages/default.aspx

[160] See, https://icdppc.org

[161] See, https://icdppc.org/wp-content/uploads/2019/03/dewg-resolution-adopted-20180918.pdf

[162] See, https://icdppc.org/wp-content/uploads/2015/02/Resolution-2016-on-Privacy-education.pdf

[163] See, Concept Note, available at:
https://www.ohchr.org/Documents/HRBodies/CRC/GCChildrensDigitalEnvironment/CN.docx and
https://www.ohchr.org/EN/HRBodies/CRC/Pages/GCChildrensRightsRelationDigitalEnvironment.aspx

[164] See: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223/signatures

[165] *The Convention for the protection of individuals with regard to automatic processing of personal data* (ETS No. 108) (1981)

[166] For further information see*:* https://rm.coe.int/16808ade9d which provides a copy of the text as it will be once amended, specifically art. 15(2)(e); and https://rm.coe.int/16808accf8