Organisation for Economic Co-operation and Development

DSTI/CDEP/DGP(2020)3/FINAL

Unclassified English - Or. English

12 January 2021

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INNOVATION
COMMITTEE ON DIGITAL ECONOMY POLICY

Working Party on Data Governance and Privacy in the Digital Economy

Children in the Digital Environment: Revised Typology of Risks

JT03470166

Foreword

The digital environment has become an integral part of children's everyday lives and interactions. The benefits can be tremendous, but there also risks. In 2011, the OECD adopted a Typology of Risks in an effort to broadly categorise those risks (OECD, 2011[1]). Since then the digital environment has changed significantly. Risks that previously existed have evolved in nature, and new ones have emerged.

This report examines these trends and presents an updated Typology of Risks, which provides a high-level overview of the risk landscape. It outlines four risk categories and their manifestations. The Typology also identifies and analyses risks that cut across these four risk categories, and as a result can have wide-ranging impacts on children's lives. The report informs the OECD's broader work on children in the digital environment.

The report was drafted by Andras Molnar under the supervision of Elettra Ronchi, of the OECD Secretariat. Lisa Robinson (OECD Secretariat) provided support throughout the drafting and editing process. The report was prepared under the aegis of the OECD Committee for Digital Economy Policy (CDEP), with input from delegates of the Working Party on Data Governance and Privacy in the Digital Economy (former Working Party on Security and Privacy in the Digital Economy). It was approved and declassified by CDEP on 30 November 2020. Delegates contributed significantly with their comments and amendments. The report greatly benefitted from consultations with the informal group of experts held in September, October and December 2019. The Secretariat of the Committee on Consumer Policy (Brigitte Acoca, Thyme Burdon, Reiko Odoko) also provided valuable feedback. The author would like to particularly acknowledge the contributions of Urs Gasser and Sandra Cortesi (Berkman Klein Center for Internet and Society at Harvard University), Baroness Beeban Kidron and Victoria Jaynes (5Rights Foundation), and Sonia Livingstone (London School of Economics and Political Science).

Note to Delegations:

This document is also available on ilibrary as:

OECD (2021), "Children in the digital environment: Revised typology of risks", *OECD Digital Economy Papers*, No. 302, OECD Publishing, Paris, https://doi.org/10.1787/9b8f222e-en.

Table of Contents

Children in the Digital Environment: Revised Typology of Risks

Executive Summary

The digital environment has become a part of children's everyday lives and interactions. It holds tremendous benefits for children, but there are also risks. Since the adoption of the OECD's 2011 Typology of Risks, the nature of existing risks have significantly changed, and a number of new risks have emerged. Technological developments and new business models have contributed to the change in digital devices and services, which in themselves have also contributed to the evolving risk landscape.

The revised Typology of Risks presented in this document provides a high-level and overarching overview of the different types of risks that children may face in the digital environment. It discusses four risk categories, namely: *i)* Content Risks; *ii)* Conduct Risks; *iii)* Contact Risks; and *iv)* Consumer Risks. The Typology also identifies risks that cut across these four risk categories and can have wide ranging impacts on children's lives. These are: *i)* privacy risks; *ii)* advanced technology risks; and *iii)* health and wellbeing risks. Whilst the revised Typology recognizes that some of the broad categories identified in 2011 (such as content and contact risks) are still relevant today, it highlights that the substantive acts underlying these risks have changed and evolved over time.

In particular, previously existing risks, such as cyberbullying or exposure to harmful content have changed in nature and still persist. Different types of exploitation may also pose risks for children in the digital environment (e.g. sextortion). A number of new concerns have also emerged, for example the spread of mis or disinformation ('fake news') or children acting in peer-to-peer exchanges where their own conduct can make them vulnerable (conduct risks).

Children today may face new types of misleading or fraudulent commercial practices. In addition, children may be exposed to potentially harmful marketing strategies blurring the line of what is commercial content and what is not. Children may also be targeted with advertising based on the personal data that is collected from them, which raises privacy as well as financial and security concerns. Furthermore, there are still instances of children being exposed to illegal and age-inappropriate products.

With the abundance of personal information collected, processed and shared through advanced technologies such as artificial intelligence and predictive analytics, children's data may also be used for the purpose of profiling, potentially affecting their fundamental legal rights and freedoms. The age and maturity of the child may affect their ability to understand the motivation behind this type of data collection and uses or the longer term privacy consequences. Widespread concerns are also emerging about the health and wellbeing effects of the digital

environment on children. Stronger evidence-base and good quality and comprehensive studies are however needed to further verify and address these concerns.

Background

The 2012 OECD Recommendation on the Protection of Children Online ('the 2012 Recommendation') [OECD/LEGAL/0389] aimed at assisting governments in setting policies to protect children from the risks they may face as Internet users without reducing their opportunities and benefits. The 2012 Recommendation was based on findings from an analysis of risks faced by children on the Internet and the "protection of children online" was defined as encompassing "content risks, contact risks, risks related to children as consumers as well as information security and privacy risks faced by children on the Internet" (OECD, 2011[1]).

The digital environment is now one of the spaces where children live their daily lives. It holds tremendous new opportunities for children, at the same time there are downsides and new risks. Because a significantly different risk landscape exists than that which initially gave rise to the 2012 Recommendation, this revised Typology of Risks examines emerging risks and how the nature of existing risks has changed.

Much of this evolution is due to children's increasing use of mobile and smart devices, rather than laptops or desktop computers (OECD, 2017[2]) (OECD, 2019[3]) (OECD, 2020[4])). In addition to the changing types of devices, the evolving risk landscape results from the changing nature of the use of these digital technologies. Compared with 2012, more and more children engage in the digital environment as part of their everyday lives and interactions. Internet connected digital devices are no longer simply tools (*i.e.* for research), but can enable children's education, help them acquire knowledge and information, and are an essential part of a child's communication, recreation, and social connection. The COVID-19 pandemic has accelerated these trends as school closures and social distancing measures have increased children's reliance on digital technologies for education and socialisation (OECD, 2020[5]).

Technological advances, which in themselves have contributed to the change in digital devices and services, have also contributed more broadly to this changing risk landscape. Online commercial practices have also changed since 2011. Today, children use a wide range of commercial online platforms, which have gained an increasingly prominent presence in children's lives. Many have specific features that make them particularly appealing to children and, yet, potentially harmful. Technological advances have also brought about significant changes in how personal information is collected, stored, shared and used. With the abundance of personal information processed and shared, children are exposed to increased and complex privacy risks.

At the same time, there have been changes to the capacity of parents, caregivers and guardians to supervise the activities of their children on mobile and smart devices, due to both the constantly connected nature of these devices and the activities undertaken on them (OECD, 2019[6]). For instance, in the absence of

payment authentication and parental control tools children may be able to make purchases without the knowledge or consent of their parents, caregivers and guardians (OECD, 2019[6]) (OECD, 2014[7]). Likewise, parents, caregivers and guardians may simply lack the skills necessary to be able to effectively understand and mitigate against the risks inherent in the digital environment, and often have less sophisticated digital literacy skills than those of their children (OECD, 2020[4]).

In light of these developments, it was recognised that the typology of risks developed by the OECD in 2011 (OECD, 2011[1]) no longer captures the current spectrum of risks. Whilst some of the broad categories identified in 2011 (such as contact and content risks) are still relevant today, the substantive acts underlying these risks have changed and evolved over time. Previously existing risks, such as exposure to harmful content or cyberbullying have changed in nature and still persist. Different types of exploitation may also pose risks for children in the digital environment (e.g. sextortion). A number of issues that did not exist (or were barely visible) in 2011 are emerging as new concerns, for example the spread of mis or disinformation ('fake news'), or children acting in peer-to-peer exchanges where their own conduct can make them vulnerable (conduct risks) (Hasebrink et al., 2018[8]). Advanced technologies (e.g. Artificial Intelligence, Internet of Things, predictive analytics, biometrics), are a further example of emerging digital technologies, which may also have some risk components, such as profiling, that may negatively affect children. At the same time, there are widespread concerns about the possible negative effects of the digital environment on children's health and wellbeing, even though there is a lack of robust research to support these concerns (OECD, 2020[5]). Taking all of this into account, it is crucial that children's comprehension of the digital environment, their digital skills, and capacity to provide full and informed consent are taken into account in designing services, policies and regulations (OECD, 2020[9]).

Four risk categories are described in the revised Typology of Risks ('the Typology' – see below Figure 1.) and presented in this document. Namely: *i)* Content Risks; *ii)* Conduct Risks; *iii)* Contact Risks; and *iv)* Consumer Risks. The Typology also identifies risks that cut across these four risk categories and can have wide ranging impacts on children's lives. These are: *i)* privacy risks; *ii)* advanced technology risks; and *iii)* health and wellbeing risks.

Figure 1. Typology of Risks

Risks for Children in the Digital Environment				
Risk Categories	**Content Risks**	**Conduct Risks**	**Contact Risks**	**Consumer Risks**
Cross-cutting Risks*	Privacy Risks (Interpersonal, Institutional & Commercial)			
	Advanced Technology Risks (e.g. AI, IoT, Predictive Analytics, Biometrics)			
	Risks on Health & Wellbeing			
Risk Manifestations	Hateful Content	Hateful Behaviour	Hateful Encounters	Marketing Risks
	Harmful Content	Harmful Behaviour	Harmful Encounters	Commercial Profiling Risks
	Illegal Content	Illegal Behaviour	Illegal Encounters	Financial Risks
	Disinformation	User-generated Problematic Behaviour	Other Problematic Encounters	Security Risks

*Note: The Typology acknowledges risks that cut across all risk categories ("Cross-cutting risks"). These risks are considered highly problematic as they may significantly affect children's lives in multiple ways.
Source: OECD and Berkman Klein Center for Internet and Society at Harvard University.

The Typology seeks to provide a high-level and overarching overview of the different types of risk category. Specific manifestations or examples of these risks are highlighted in this explanatory note. It is anticipated that these risk manifestations will be expanded on in more detail in a Companion Document to the OECD draft Recommendation on Children in the Digital Environment.

Additionally, as the focus of this document is the Typology of Risks, the multitude of opportunities brought about by the digital environment are not discussed. It is, however, anticipated that they will be addressed in the Companion Document.

Content Risks

In 2011, the OECD defined content risks to include circumstances where, "the child passively receives or is exposed to content available to all Internet users in a one-to-many relationship" (OECD, 2011[1]). At that time, the OECD identified three main subcategories of content risk: *i)* illegal content; *ii)* age-inappropriate or harmful content; and *iii)* harmful advice (OECD, 2011[1]). Whilst these three subcategories persist today, advances in technology have altered both the potential volume of this material, and the methods by which children may become exposed to it. Additionally, with the advances in technology new issues have arisen (e.g. fake news that uses technology to convincingly mirror legitimate news sources) that changed somewhat the nature of this risk. Accordingly, the Typology recognises four risk manifestations under content risks: *i)* hateful content; *ii)* harmful content; *iii)* illegal content; and *iv)* disinformation. Each of these are discussed briefly below.

Hateful content can take the form of pictures, words, videos, games, symbols and even songs (Livingstone, 2019[10]). It can be motivated, for instance, by the victim's

religion, race, gender, disability, sexual orientation or gender identity. This activity is increasingly conducted in the digital environment where this content can spread exponentially and often uncontrollably. The digital environment has more generally enabled people to insult, offend or abuse outside of the specific hate crime context (UK Government, 2017[11]), exacerbated by the anonymity and physical distance from the victim. It is especially important to recognise hateful content as a risk manifestation, because the number of children affected by exposure to hate content in the digital environment is rising. For instance, while in 2010, only 12% of 11-16 years old children in the United Kingdom reported that they had been exposed to hateful content online, by 2019 half of 12-15 years old declared seeing such content (Ofcom, 2020[12]).

Children can also be troubled by a wide variety of harmful content, such as online scams, pornographic pop-up advertisements, unpleasant or scary news or pictures (Byrne and Burton, 2017[13]). Violent and pornographic content can cause children shock and disgust. A study from 2020 revealed that in the European Union the most reported harmful content that children were exposed to (at least monthly) were hate messages[1] (average of 17%) followed by violent images (average of 13%) (Smahel et al., 2020[14]) (Council of Europe, 2018[15]) This report also found that exposure to different kinds of harmful content is interrelated. For instance, if a child sees one type of harmful content, it is more likely that the same child will also report seeing other types of harmful content (Smahel et al., 2020[14]).

Content that is illegal to publish (*i.e.* illegal content) can expose children to concepts that they are unable to manage and can also breach cultural and social norms. For example, images or videos of child sexual abuse, content that advocates terrorist acts, or promotes, instructs or incites crime or violence is considered illegal in many countries. However, the legislative response to these concerns varies across different jurisdictions (OECD, 2011[1]). For instance, in some OECD countries hate speech or racist online content may be illegal, whereas other countries might have a different response to tackling such issues.

There is also an increasing recognition that children need to be educated about disinformation so that they are able to distinguish between what is fact and what is false or a misrepresentation in the digital environment. This is an especially key skill given that children can have different interpretations of what makes a news outlet credible and they mostly obtain news and information from social media platforms, which can be unreliable (Babur, 2017[16]). Accordingly, children need strong digital literacy skills to be able to critically analyse the content that they are consuming, and to detect disinformation (Cortesi et al., 2020[17]) (UK Government, 2017[11]).

At the same time, it is important to ensure that a focus on ensuring strong digital literacy does not result in the responsibility to mitigate against this risk being placed squarely on the shoulders of children. Those who create and host content also play a vital role in tackling such disinformation. This has been most evident during the COVID-19 pandemic, where certain platforms and social media companies have reinforced their efforts to remove misleading, false and potentially harmful information related to COVID-19 (OECD, 2020[18]). In particular, Facebook, Twitter, YouTube, Google, LinkedIn, Microsoft, Reddit and Twitter have published a joint statement on their collaboration with government health agencies to prevent disinformation related to COVID-19 (OECD, 2020[18]). However, in spite of these

efforts, obtaining digital literacy skills to detect disinformation can still be particularly challenging for children. For instance, a Parliamentary report found that only two percent of children and young people in the United Kingdom have the digital literacy skills necessary to assess whether a news story is real or fake (National Literacy Trust, 2018[19]).

Conduct Risks

Whilst in its previous typology, the OECD specifically excluded activities in the digital environment whereby children were creating risks for other children (OECD, 2011[1]), it has become increasingly clear that this is a significant and growing concern for children. A 'conduct risk' is now recognised by the United Kingdom's Safer Internet Centre, who refers to this specific category of risk (United Kingdom Safer Internet Centre, n.d.[20]). During the October 2018 OECD Workshop in Zurich on the 'Protection of Children in a Connected World' the issue of a conduct risk was also recognised as a distinct category of risk (OECD, 2019[3]) (Hasebrink et al., 2018[8]).

Accordingly, the concept of a 'conduct risk' is included in the Typology. This is a risk where children are actors in a peer-to-peer exchange, including when their own conduct can make them vulnerable (for instance in the case of sexting, or cyberbullying) (O'Neill, Livingstone and McLaughlin, 2011[21]). This concern is distinguishable from a contact risk where a child is a victim of an interactive situation.

Under conduct risks, the following risk manifestations are recognised in the Typology: *i)* hateful behaviour; *ii)* harmful behaviour; *iii)* illegal behaviour; and *iv)* user-generated problematic behaviour. As highlighted in the OECD review of legal and policy practices, it is undoubtable that such risks manifestations not only pose a risk towards those children who are on the receiving end of such behaviour in the digital environment, but also to those whose behaviour created the risk (OECD, 2020[4]). Concretely, a conduct risk occurs where a child behaves in a way that contributes to risky digital content or contact (UNICEF, 2017[22]).

Hateful behaviour can, for instance, be motivated by the victim's religion, race, gender, disability, sexual orientation, gender identity (Hasse et al., 2019[23]), or even seemingly benign personal characteristics such as accent, language skills, personal appearance, hobbies, taste in music, fashion sense, etc. Its primary aim is to offend, abuse or insult the victim. In the case of harmful behavior a child (or children) can use the digital environment to aggress another child, in many cases repeatedly, leading to cyberbullying.

A lack of agreement across policy actors and research as to what actually constitutes cyberbullying has resulted in countries addressing this concern in different ways – in many cases by criminal justice responses. However, where children are the perpetrators, a criminal justice response can be highly controversial and disproportionate as it can lead to the criminalisation of children unaware of the impact of their actions.

Sexting, the exchange of sexual messages, on the other hand, provides an example of user-generated problematic behaviour. It can cause a multitude of problems (both social and legal) for the creator(s) of the content. 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 (even in those cases when their 'sext' is shared consensually), they may be self-producing child pornography material that can quickly spread and remain in the digital environment permanently. Sexting not only has implications on a child's privacy, health and wellbeing, but there is also a significant risk that a child could be criminalised as a result of 'self-producing' child pornographic material.

Contact Risks

Contact risks occur when children interact in the digital environment. Risk manifestations in this category are further distinguished according to whether: *i)* children are exposed to hateful encounters in the digital environment; *ii)* the encounter takes place with the intention to harm the child; *iii)* the encounter is prosecutable under criminal law; and *iv)* the encounter is problematic but cannot be placed under the three previous risk manifestations.

Just like with previously identified risks manifestations, the motivations for such behaviours can overlap, and it may be that the very actions which, for example, gave rise to a conduct risk, can also give rise to a contact risk. The difference here is that the child is the victim (or recipient of) such actions, as opposed to the actor. For example, a victim of cyberbullying, or a victim of a shared sext can lead to negative consequences for the victim's personal development, safety and wellbeing and can even culminate in suicide (OECD, 2020[4]).

Under this risk category, other manifestations are also relevant. For example, sextortion refers to a type of exploitation, whereby the perpetrator threatens to expose or share a sexual image to blackmail the victim into doing something (this can range from sharing more images to paying money or engaging in sexual activity) (OECD, 2020[4]).

Additionally, sex trafficking and cyber grooming are clear contact risks. Whilst the 2012 Recommendation did not seek to cover such offences, these issues have been identified as a growing concern across OECD countries and are also acute concerns in the developing world. The OECD provided a detailed analysis of these concerns in its review of legal and policy practices (OECD, 2020[4]).

Consumer Risks

Children can also face risks as consumers in the digital economy. As with other categories, this risk category includes new and emerging types of risks that were not part of the previous typology.

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)" (OECD, 2011[1]).

This statement remains true today; however, a host of emerging commercial practices may pose additional risks to children (Cortesi et al., 2020[24]). The digital environment is a highly commercialised world that is characterised by

hyperconnectivity and datafication (as will be further examined under 'Cross-cutting Risks'). Since children depending on their age, maturity and circumstances may be more susceptible to misleading or fraudulent market practices, they are likely to be targeted in the digital environment based on the personal data that is collected from them (OECD, 2019[25]). Indeed, children are an important audience for marketers as they may influence family spending, directly engage in transactions, and are future consumers (Van Der Hof, 2017[26]).

The typology identifies four risk manifestations under consumer risks for children, namely: *i)* marketing risks; *ii)* commercial profiling risks; *iii)* financial risks; and *iv)* security risks. These risk manifestations can for instance affect children's privacy, may amount to commercial pressure, and can expose children to inappropriate messages or products (Livingstone, Carr and Byrne, 2016[27]).

Marketing risks include techniques that can expose children to illegal and age-inappropriate products and potentially harmful marketing strategies such as native advertising, non-transparent "influencer" marketing, prize-winning activities and "advergames" (i.e. advertisements featuring gaming content) that may make it more difficult for children to distinguish between commercial and non-commercial content (ICPEN, 2020[28]) (as discussed in Box 1. below).

Box 1. Examples of common marketing strategies that may affect children

- Native or in-stream advertising - advertising that aims to mimic the tone and format of the online platform on which it appears (Amazeen, 2019[29]) (OECD, 2019[29]). In particular, children may not notice that the content they are viewing is an ad and as a result may be more easily persuaded by the message (ICPEN, 2020[28]).
- Influencer marketing – advertising that is integrated into user-generated content generally on social media platforms. Influencers can be beauty bloggers, gamers, travel experts, and fitness gurus among others and have a large social media following. Influencers may have an impact on consumer trends and can partner with companies to promote their services and products to their "followers" (i.e. social media audiences) (OECD, 2019[29]). Influencers may be viewed by children as role models and can increase the persuasiveness of the message, magnifying the potential for harm (ICPEN, 2020[28]).
- Prize-winning activities – children may be incentivised to buy a product or use a service through the use of prizes or competitions as well as "like and share" activities, which makes children part of a business's marketing strategy and obscures the commercial nature of posts for other children who receive the posts from a friend and not a business. (OECD, 2019[29]) (ICPEN, 2020[28]).
- Advergames – video games that feature advertisements and commercial messages (OECD, 2019[29]).

Children may not have the capacity to fully understand the information presented in commercial transactions such as disclosures about negative options marketing or subscription traps in apps and online games (OECD, 2019[6]) (see below in Box 2.). They may not, for example, fully understand disclosures about in-game "microtransactions" (in-game purchase usually for a small fee) or "loot boxes" ("video game microtransactions in which the consumer purchases a reward containing one or more virtual items of differing value or rarity assigned at random") (FTC, 2020[30]). Children may also not understand the relationship between real currency and game currency and calculate the "exchange rate" for every transaction (FTC, 2020[30]).

Box 2. Problematic marketing practices

- Negative options or subscription trap – services or products advertised for "free", which enrol consumers in a subscription that after a trial period automatically generate charges (OECD, 2019[25]).

Commercial profiling risks may arise when advertisers use data created through children's use of social media and other digital platforms without informed consent and/or in violation of consumer or data protection laws (UNICEF, 2017[22]). To this end, many children do not have sufficient digital literacy skills to understand the disclosures they encounter in the digital environment, especially in respect to the use of their personal data (as discussed under 'Privacy Risks') (OECD, 2019[6]). In relation to commercial profiling, in the European Union, the GDPR states (under Recital 71) that "such measure should not concern a child" - a clear indication that such processing of children's personal data should not be the norm (ICO, 2018[32]) (ICPEN, 2020[28]). However, currently there is no commonly accepted global approach to regulate the practice of commercial profiling of children (ICPEN, 2020[28]).

It is worth noting that apart from its commercial aspects, profiling can also be used for other wide ranging purposes. It can be used to suggest content to children, to encourage them towards particular behaviours, and to determine where, when and how often that content should be served (ICO, 2020[33]). However, content feeds that gradually take children away from their original area of interest into content that is not suitable for them raise much more significant concerns (ICO, 2020[33]). Such content feeds can encompass not just commercial content, but also possibly harmful content generated by other internet users or provided by downloads and other websites (ICO, 2020[33]).

Risks to children's finances or those of their parents, caregivers or guardians may occur when the marketing practices discussed above influence children to unknowingly order products through digital assistants, sign up for services that require recurring payments, or spend large amounts of money on products or services without the knowledge or consent of their parents, caregivers or guardians.

Consumer risks also encompass a number of security risks that children may face in the digital environment: for instance, free games, ring tones, or other downloads that contain malware, social networking apps that give the app's developers impermissible access to personal information, and "phishing" text, email, or pop-up messages that may facilitate identity theft.

While in the physical world, practices and regulations are in place to protect children from consumer risks, including age-inappropriate advertising and false, misleading or deceptive conduct, in a number of cases these practices and regulations are still to be satisfactorily developed for the digital environment (Livingstone, Carr and Byrne, 2016[27]). In response to an OECD survey, with some exceptions, only a few countries reported that their laws specifically addressed consumer risks to children (OECD, 2020[4]). There have, nonetheless, been a number of enforcement initiatives that have addressed unauthorized purchases in online games in OECD countries as well as self-regulatory developments that provide parents with parental controls and information to prevent and mitigate such risks, e.g., spending limits on digital games (OECD, 2018[34]).

Cross-cutting risks

The Typology also acknowledges risks that cut across all risk categories and are considered highly problematic as they may significantly affect children's lives in multiple ways. These are: *i)* privacy risks; *ii)* advanced technology risks; and *iii)* health and wellbeing risks.

Privacy risks

The privacy space has significantly evolved since the adoption of the 2011 typology of risks. Today, children's personal information and their data is not simply the information that they knowingly share, but involves information that can be gained from their activities in the digital environment or even from disclosures that parents and friends may make (and these actions can follow children into their adulthood – see below in Box 3.).

Box 3. Concerns around sharenting

The term 'sharenting' refers to when parents share information about themselves and their children in the digital environment (Blum-Ross and Livingstone, 2017[35]). Sharenting is a widely popular practice among parents, as they may get a lot of gratification for posting stories, images and videos about their children online (Kamenetz, 2019[36]). A study conducted in the United Kingdom found that, on average, nearly 1500 photos of a child will have been posted in the digital environment before they reached the age of five (Nominet, 2016[37]). Another study found that among parents of children aged up to four, three-quarters reported that they know of another parent, who they consider to be sharing too much information about their child on social media (Mott Poll Report, 2015[38])

The practice of sharenting may lead to a number of serious concerns for children. Notably, it can infringe on a child's privacy. According to recent academic research, whilst parents are supposed to protect children's personal data and privacy,

narrating children's lives through sharenting may undermine this protective role (Steinberg, 2017[39]). This desire to share moments of their child's upbringing, conflicting with a parent's protective role, can create problems outside of just privacy concerns. For instance, some children's advocates have argued that as children grow they might disagree with the disclosures made by their parents years earlier (Steinberg, 2017[39]). To this end, a French law allows adult children to sue their parents for privacy infringements that they had to experience when they were younger (Staufenberg, 2016[40]) (Blum-Ross and Livingstone, 2017[35]), concerning both children's privacy and impacting their interpersonal relationships.

Additionally, sharenting may also expose children to other risks, including contact risks such as online grooming and paedophiles (Blum-Ross and Livingstone, 2017[35]) and consumer financial and security risks such as child identity theft. In the United States, a new law, in effect since 2018, allows parents and child welfare representatives of people under 16, as well as legal guardians, to request a security freeze, also called a credit freeze, to help protect a young person from identity theft and fraud (FTC, 2019[41]).

In relation to privacy concerns, the GDPR introduced an array of protective measures supporting the rights of the child to safety and privacy, including special protection with regard to children's personal data and the right to be forgotten. However, despite these safeguards the GDPR does not specifically address the right to privacy of those children who are the subjects of sharenting (Donovan, 2020[42]). Furthermore, the GDPR also does not acknowledge that parents may not always act in their children's best interest or may not be sufficiently technologically savvy to safeguard their children's privacy (Donovan, 2020[42]).

To examine how children of different ages understand data typologies in terms of their privacy, it is important to distinguish between three types of data:

- 'Data given' – the data provided by individuals (about themselves or about others), usually knowingly though not necessarily intentionally while they are online;
- 'Data traces' – the data left by participation online (usually without the knowledge of the user) and captured via data-tracking technologies such as web, beacons or device browser fingerprinting, cookies, location data and other metadata; and
- 'Inferred data' – the data derived from analysing data traces and data given, frequently by algorithms (also referred to as 'profiling'). This can also be combined with other data sources (Livingstone, Stoilova and Nandagiri, 2018[43]).

The Typology recognises that data can be placed under interpersonal, institutional and commercial privacy risks. Primarily, children are aware of data given in an interpersonal context (e.g. either they provide data themselves or they may be aware that their friends or family do too). In such cases, children most likely consciously decide whether and with whom they are choosing to share data with (Hof, 2017[44]). Research reveals that children are aware that they possibly

contributed data about themselves or about others as a result of their activities in the digital environment. The extent to which they will comprehend the consequences for their privacy will depend on the child's age, maturity and circumstances.

Institutional privacy mainly depends on data given. Here, risks can originate from necessary or routine data collection, for example by hospitals or schools. Concerns in this area are also increasingly linked to inferred data, in the form of health or learning analytics (Livingstone, Stoilova and Nandagiri, 2018[43]). Furthermore, the COVID-19 pandemic has also highlighted increased privacy risks for children in educational settings (see below in Box 4.).

Commercial privacy depends on all three types of data and it is also becoming a more visible concern. Children – at least older children - are increasingly aware of the commercial uses of 'data traces' but their understanding of 'inferred data' and its value to businesses relies on their comprehension of business models operating in institutional and commercial contexts (Livingstone, Stoilova and Nandagiri, 2018[43]). These are issues that children are rarely educated about, and parents and caregivers may also lack knowledge about how data is collected and used (OECD, 2020[45]). In addition, many children, especially younger ones, do not have sufficient literacy and/or comprehension skills to understand many of the disclosures they encounter in the digital environment, especially in respect of privacy and the use of personal data (Livingstone, Stoilova and Nandagiri, 2019[46]). The dynamic and complex nature of the information and communication ecosystem (i.e. rapid emergence of new products and services, multitude of actors involved in data lifecycle) may also act as a barrier to awareness of privacy risks. Increased data collection by companies to determine a user's age and verify their identities may also lead to privacy risks. The privacy and data security risks of connected smart toys and apps that are being designed and targeted towards children as well as child-directed video sites create more opportunities for the collection and use of children's data. In many cases, this happens in a manner contrary to measures designed to protect the privacy of children (Norwegian Consumer Council, 2017[47]; Irwin Reyes et al., 2018[48]) (McReynolds et al., 2017[49]). Some authorities in OECD countries have taken enforcement action when such measures have been breached (FTC, 2018[50]) (Hessel and Rebmann, 2020[51]).

Box 4. The effects of COVID-19 on the privacy of children

There has been an abundance of personal data processed and shared as a result of the COVID-19 pandemic, notably in educational settings. This situation has the capacity to lead to increased privacy risks for children (OECD, 2020[5]).

In the absence of clear regulation and protections, the mass recourse to E-learning platforms (often privately run platforms) may undermine children's privacy due to the collection, use, reuse and disclosure of personal data (Han, 2020[52]). Online platforms that contain video conferencing services and are used more frequently for educational purposes may also conduct inappropriate personal data collection and can lead to privacy violations (OECD, 2020[5]). Whilst it is often the case that

these platforms are presented to children, parents, carers, and teachers as 'transformational', the merging of public education with for-profit platforms and business models raises serious concerns for the protection of children's privacy (Livingstone, Stoilova and Nandagiri, 2019[46]). At the same time, the COVID-19 crisis may mean that not only do lessons occur through dedicated E-learning platforms, but that student-teacher interactions might be conducted on social networking platforms and apps that may not have sufficient personal data protection and privacy safeguards (World Childhood Foundation et al., 2020[53]).

Furthermore, many governments have taken extraordinary measures to contain the spread of the COVID-19 pandemic, by using digital technologies and advanced analytics to collect, process and share personal data for front-line responses (OECD, 2020[54]). Whilst these exceptional measures may prove effective in containing the virus, some of these responses may pose a risk to the protection of children's personal data and privacy. Such violations for instance can include the public sharing of an infected child's personal information, or information sufficient to lead to their personal identification (United Nations, 2020[55]).

Advanced Technology Risks

Whilst advanced technology (e.g. Artificial Intelligence, Internet of Things, predictive analytics, biometrics) has a number of benefits, it can also carry new risks. As an illustration automated systems (European Parliament, 2019[56]) (Rieke, Bogen and Robinson, 2018[57]) can significantly impact and shape children's lives, including their education; health and well-being; privacy and safety; freedom of expression among others. Advanced technology risks can create inequalities; exclusion; discrimination; bias and manipulation among others (Hasse et al., 2019[58]).

For instance, the use of AI-based technologies (and their reliance on big data) may pose risks to children's safety, security, and privacy (Hasse et al., 2019[58]). In relation to privacy, significant concerns exist regarding how ed-tech applications collect and store children's personal data (Hasse et al., 2019[58]). Companies that use AI-based technologies can also undermine children's privacy if they are not ethical and clear about how they collect, use and store children's personal data (Hasse et al., 2019[58]). Big data collected by AI technologies could also lead to data breaches and may culminate in the illegal use of children's personal data. Among other concerns, AI-based technologies may also negatively affect children with disabilities and their rights to education and protection from abuse (UNICEF and Human Rights Center, 2019[59]). Recent research shows that algorithms may amplify and replicate existing biases such as social attitudes which may portray disabilities as negative (Whittaker et al., 2019[60]) (Hutchinson et al., 2019[61]).

Furthermore, in education AI can be considered trustworthy not just when the system successfully implements what it is supposed to do, but also when one can trust humans will use it in an appropriate and fair way (OECD, 2020[62]). For instance, early warning systems that are supported by AI have the capacity to profile students and identify those who are at risk of dropping out. The effectiveness of these systems in identifying the right students may be too limited, or another possibility is that they are accurate but misused (OECD, 2020[62]). In

particular, due to identifying those students who are at risk of dropping out, interventions might result in an exclusion of those 'at risk' students from school because of potential loss of reputation, rather than targeted support (OECD, 2020[62]).

The Internet of Things (IoT) has meant that smart devices, such as smart toys, may also pose privacy, security and safety risks for children (OECD, 2018[63]). For instance, "connected" toys often come with the capacity to film children, communicate with them remotely, reveal their location, or record and analyse their conversations to investigate their preferences and interests (Hof, 2017[44]). These toys may also possess software vulnerabilities allowing them to be hacked by third parties.

The use of predictive analytics may raise serious ethical concerns, because predictive models rely on historical patterns, which may be inadvertently biased against certain subgroups of children (Teixeira and Boyas, 2017[64]). Additionally, the accuracy of predictive tools raises concerns, and classification errors are possible. To this end, for instance, in child welfare where predictive tools may be used to assess whether or not a child is at risk classification errors can culminate in poor targeting of agency resources (due to false positives, identifying some cases as high risk when they are in fact low risk) and can even be directly dangerous to the child (due to false negatives, failing to accurately identify a high risk child) (Teixeira and Boyas, 2017[64]) (D'Andrade, Austin and Benton, 2008[65]). Additionally, in this context, whilst parents and caregivers may be aware that predictive analytics shares their and their children's personal data with social support and health systems, they may not know that this can lead to an algorithmic scoring of their families for 'risk' (Teixeira and Boyas, 2017[64]).

Lastly, the use of biometric technologies (i.e. the use of fingerprints, facial recognition and iris scans, etc.) may pose specific risks to children. Biometric systems have been primarily designed to work with adults, and they may not be suitable to appropriately recognise children, and therefore to be used for children. As of mid-2019, there were no biometric technologies capable of consistently providing high levels of accuracy in very young children (less than 5 years), and weak evidence in support of the use of biometrics from children aged 5 to 15 years (UNICEF, 2019[66]). Specific risks include data protection and privacy risks. Other misuse of children's biometric data include theft, abuse and identity fraud that can harm children and may have serious or even permanent consequences (UNICEF, 2019[66]). The use of biometric technologies can also lead to exclusion, for instance where this technology is mandatory for access to a service, but design and technology limitations may cause errors in the biometric registration service, the child is unable to have their biometric trait captured, or the child's parent does not consent to this (UNICEF, 2019[66]). Biometric systems also have the risk of scope creep, namely when the data is used for motives outside the scope of its original collection, and in a manner for which informed consent was not given (UNICEF, 2019[66]). To this end, the use of children's biometric data may raise social and ethical concerns as children often lack the knowledge and understanding to make informed decisions on this matter. Furthermore, parents, caregivers and guardians may also lack the capacity to comprehend the risks related to the use of children's biometric data (UNICEF, 2019[66]).

In general, there is still very little empirical evidence on the impacts of advanced technology risks, mirroring gaps in policy documents. For instance, in most cases national AI strategies and AI ethical guidelines do not specifically mention children.

Businesses have a responsibility to develop inclusive design, safety and privacy by design, as well as ethical technologies and solutions for children to meet the potential risks posed by these advanced technologies (OECD, 2020[67]). The development of related practices and standards could also involve additional stakeholders – including government and civil society - when appropriate. This will better enable the beneficial deployment of these technologies for children.

Health and wellbeing risks

The possible negative impacts of the digital environment on children's health and wellbeing has raised widespread public concern. In some specific contexts (*i.e.* the impact of excessive screen time) this is an emerging field of research, with a limited evidence base.

Nonetheless, there are areas where a health and well-being risk may cut across other risks. For example, whilst cyberbullying has been discussed above (as both a contact and a conduct risk), a clear concern of cyberbullying is the effect on the child victim's mental health. It has been recognised that cyberbullying can have a more negative effect on children's mental health than traditional bullying. Those who have been cyberbullied reported higher levels of depression, anxiety and social difficulties compared to those who were 'traditionally bullied' (Perren et al., 2010[68]).

The dangers of screen media and social media use is also receiving increased attention. In relation to screen media use, a literature review conducted by the UK Royal College and Paediatrics and Child Health revealed the following associations:

- Children with higher screen time tend to have a higher energy intake, a less healthy diet and more pronounced indicators of obesity – Noting that this association could also be explained by causality in either direction (e.g. more obese children are likely to have higher screen time) or by underlying causes (e.g. poverty); and
- Children with over two hours screen time per day, tend to have more depressive symptoms. However, it was also revealed that some screen time is better for mental health than none at all (Royal College of Paediatrics and Child Health, 2019[69]).

Another study also indicated that moderate use of digital technologies and screen time allows children to enjoy the benefits of the digital environment, whilst no activity or too much use may have negative impacts on children (OECD, 2020[5]) (Burns and Gottschalk, 2019[70]) (Przybylski and Weinstein, 2017[71]).

It is worth noting, that there seems to be a consensus among policymakers that screen time and the types and duration of online activities should be distinguished and measured separately. Calling some of the different concerns on children's health and wellbeing simply screen time and not clearly distinguishing between the different actions (such as blue light on children's sleeping patterns, or vulnerable teenagers on Instagram) may lead to inconsistent findings (OECD, 2020[67]). Thus,

in order to understand possible risks it is essential to examine the child's age, circumstances and maturity as well as the context and content rather than just time spent in front of a screen.

Furthermore, whilst research on the impacts of social media on clinically diagnosed depressed children supports the notion that social media may exacerbate depressive symptoms (OECD, 2019[3]), it is also important to point out that children who are vulnerable offline are more likely to be vulnerable in the digital environment (Livingstone and Bulger, 2013[72]) (UNICEF, 2017[73]) (Burns and Gottschalk, 2019[70]) (OECD, 2020[5]). Thus, it is difficult to establish clear causality, as those children who already suffer from depression or anxiety may be likely to be more prone to digital overdependence (OECD, 2019[3]).

It is also worth briefly noting that there is significant mismatch between the public discourse and the evidence available when it comes to the effects of the digital environment on children's health and wellbeing (OECD, 2019[3]). The evidence base in this area is still emerging, and currently there is a need for good quality, comprehensive, large-scale studies on the health and wellbeing effects of digital technology use (Kardefelt-Winther, 2017[74]) (Burns and Gottschalk, 2019[70]) (Royal College of Psychiatrists, 2020[75]). Despite a seemingly widespread concern about the effects of social media and the increased use of smartphones on the mental health of children, currently, we do not have enough evidence to support these concerns, with the underlying data in many existing studies not sufficiently well developed (OECD, 2019[3]).

Bibliography

Amazeen, M. (2019), *News in an Era of Content Confusion: Effects of News Use Motivations and Context on Native Advertising and Digital News Perceptions*, https://journals.sagepub.com/doi/10.1177/1077699019886589. [62]

Babur, O. (2017), "We've Heard All about Fake News—Now What?", *Harvard Magazine*, https://harvardmagazine.com/2017/03/fake-news-solutions-berkman-klein. [7]

Blum-Ross, A. and S. Livingstone (2017), *Sharenting: parent blogging and the boundaries of the digital self*, http://eprints.lse.ac.uk/67380/1/Blum-Ross_Sharenting_revised_2nd%20version_2017.pdf. [52]

Burns, T. and F. Gottschalk (2019), *Educating 21st Century Children: Emotional Well-Being in the Digital Age*, https://www.oecd-ilibrary.org/docserver/b7f33425-en.pdf?expires=1591092438&id=id&accname=ocid84004878&checksum=0BABCD10B674FC095A55E3D6631D50AA. [43]

Byrne, J. and P. Burton (2017), "Children as Internet Users: How can evidence better inform policy debate?", https://www.tandfonline.com/doi/pdf/10.1080/23738871.2017.1291698?needAccess=true. [5]

Cortesi, S. et al. (2020), *Youth and Digital Citizenship+ (Plus): Understanding Skills for a Digital World*, https://cyber.harvard.edu/publication/2020/youth-and-digital-citizenship-plus. [22]

Cortesi, S. et al. (2020), *Youth and the digital economy: Exploring youth practices, motivations, skills, pathways, and value creation*. [24]

Council of Europe (2018), *Hate Speech*, https://www.coe.int/en/web/freedom-expression/hate-speech. [79]

D'Andrade, A., M. Austin and A. Benton (2008), *Risk and Safety Assessment in Child Welfare: Instrument Comparisons*, https://www.contracosta.ca.gov/DocumentCenter/View/31214/TOC-CW-B2?bidId=. [40]

Donovan, S. (2020), *'Sharenting': The Forgotten Children of the GDPR*, https://phrg.padovauniversitypress.it/system/files/papers/PHRG-2020-1-2.pdf. [63]

European Parliament (2019), *A governance framework for algorithmic accountability and transparency*, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf. [60]

Federal Register (2019), *Rule Concerning the Use of Prenotification Negative Option Plans*, https://www.federalregister.gov/documents/2019/10/02/2019-21265/rule-concerning-the-use-of-prenotification-negative-option-plans. [80]

FTC (2020), *Video Game Loot Box Workshop: Staff Perspective*, https://www.ftc.gov/system/files/documents/reports/staff-perspective-paper-loot-box-workshop/loot_box_workshop_staff_perspective.pdf. [84]

FTC (2019), *New protections available for minors under 16*, https://www.consumer.ftc.gov/blog/2019/03/new-protections-available-minors-under-16. [82]

FTC (2018), *Electronic Toy Maker VTech Settles FTC Allegations That it Violated Children's Privacy Law and the FTC Act*, https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated. [85]

FTC (2009), *Negative Options: A Report by the staff of the FTC's Division of Enforcement*, https://www.ftc.gov/sites/default/files/documents/reports/negative-options-federal-trade-commission-workshop-analyzing-negative-option-marketing-report-staff/p064202negativeoptionreport.pdf. [77]

Han, H. (2020), *As Schools Close Over Coronavirus, Protect Kids' Privacy in Online Learning*, https://www.hrw.org/news/2020/03/27/schools-close-over-coronavirus-protect-kids-privacy-online-learning. [29]

Hasebrink, U. et al. (2018), *What are you concerned about? Classifying children's and parents' concerns regarding online communication*, https://leibniz-hbi.de/uploads/media/default/cms/media/hl9lir5_2018-11-01_ECREA_Hasebrink%20et%20al_What%20are%20you%20concerned%20about.pdf. [42]

Hasse, A. et al. (2019), *Youth and Cyberbullying: Another Look*, https://cyber.harvard.edu/publication/2019/youth-and-cyberbullying/another-look. [23]

Hasse, A. et al. (2019), *Youth and Artificial Intelligence: Where We Stand*, https://dash.harvard.edu/bitstream/handle/1/40268058/2019-05_YouthAndAI.pdf?sequence=5&isAllowed=y. [36]

Hessel, S. and A. Rebmann (2020), *Regulation of Internet-of-Things cybersecurity in Europe and Germany as exemplified by devices for children*, https://link.springer.com/article/10.1365/s43439-020-00006-3. [86]

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*, https://openaccess.leidenuniv.nl/bitstream/handle/1887/58542/S_van_der_Hof_-_I_AGREE._._._OR_DO_Ioe1oe.pdf?sequence=1. [15]

Hutchinson, B. et al. (2019), *Unintended Machine Learning Biases as Social Barriers for Persons with Disabilities*, http://www.sigaccess.org/newsletter/2019-10/hutchinson.html. [65]

ICO (2020), *Profiling*, https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/12-profiling/. [78]

ICO (2018), *The General Data Protection Regulation Applications: Children and the GDPR*, https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr-1-0.pdf. [71]

ICPEN (2020), *Best Practice Principles: Marketing Practices Directed Towards Children Online*, https://icpen.org/sites/default/files/2020-06/ICPEN%20-%20Best%20Practice%20Principles%20for%20Marketing%20Practices%20Directed%20Towards%20Children%20Online%202020.pdf. [70]

Irwin Reyes et al. (2018), "'Won't Somebody Think of the Children?'': Examining COPPA complaince at scale'"", *Proceedings on Privacy Enhancing Technologies*, https://petsymposium.org/2018/files/papers/issue3/popets-2018-0021.pdf. [17]

Kamenetz, A. (2019), *The Problem With 'Sharenting'*, https://www.nytimes.com/2019/06/05/opinion/children-internet-privacy.html. [53]

Kardefelt-Winther, D. (2017), *How does the time children spend using digital technology impact their mental well-being, social relationships and physical activity? An evidence focused literature review*, https://www.unicef-irc.org/publications/pdf/Children-digital-technology-wellbeing.pdf. [47]

Livingstone, S. (2019), *Revenge pornography and online hate content: the evidence underpinning calls for regulating online harms in the UK*, https://blogs.lse.ac.uk/medialse/2019/06/27/revenge-pornography-and-online-hate-content-the-evidence-underpinning-calls-for-regulating-online-harms-in-the-uk/. [2]

Livingstone, S. and M. Bulger (2013), *A Global Agenda for Children's Rights in the Digital Age: Recommendations for Developing UNICEF's Research Strategy*, https://www.unicef-irc.org/publications/pdf/lse%20olol%20final3.pdf. [45]

Livingstone, S., J. Carr and J. Byrne (2016), "One in Three: Internet Governance and Children's Rights", *Office of Research-Innocenti*. [13]

Livingstone, S., M. Stoilova and R. Nandagiri (2019), *Children's data and privacy online: Growing up in a digital age*, http://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review.pdf. [30]

Livingstone, S., M. Stoilova and R. Nandagiri (2018), *Conceptualising privacy online: What do, and what should, children understand?*, https://blogs.lse.ac.uk/medialse/2018/09/07/conceptualising-privacy-online-what-do-and-what-should-children-understand/. [14]

McReynolds, E. et al. (2017), *Toys that Listen: A Study of Parents, Children, and Internet-Connected Toys*, https://www.ftc.gov/system/files/documents/public_comments/2017/11/00038-141895.pdf. [35]

Mincy, R., D. Miller and E. De la Cruz Toledo (2016), "Child support compliance during economic downturns", *Children and Youth Services Review*, Vol. 65, pp. 127-139, http://dx.doi.org/10.1016/j.childyouth.2016.03.018. [26]

Mott Poll Report (2015), *Parents on social media: Likes and dislikes of sharenting*, https://mottpoll.org/reports-surveys/parents-social-media-likes-and-dislikes-sharenting. [58]

National Literacy Trust (2018), *Commission on Fake News and the Teaching of Critical Literacy Skills in Schools*, https://literacytrust.org.uk/policy-and-campaigns/all-party-parliamentary-group-literacy/fakenews/. [8]

Nominet (2016), *Parents 'oversharing' family photos online, but lack basic privacy know-how*, https://www.nominet.uk/parents-oversharing-family-photos-online-lack-basic-privacy-know/. [54]

Norwegian Consumer Council (2017), "Significant security flaws in smartwatches for children", *Forbrukerradet*, https://www.forbrukerradet.no/side/significant-security-flaws-in-smartwatches-for-children/. [16]

OECD (2020), *CO2.2: Child poverty*, OECD Family Database, http://www.oecd.org/els/family/database.htm (accessed on 16 April 2020). [25]

OECD (2020), *Combatting COVID-19 disinformation on online platforms*, http://www.oecd.org/coronavirus/policy-responses/combatting-covid-19-disinformation-on-online-platforms-d854ec48/. [68]

OECD (2020), *Combatting COVID-19's effect on children*, https://read.oecd-ilibrary.org/view/?ref=132_132643-m91j2scsyh&title=Combatting-COVID-19-s-effect-on-children. [21]

OECD (2020), *Draft Recommendation of the Council on Children in the Digital Environment*, https://one.oecd.org/document/DSTI/CDEP/DGP(2020)4/en/pdf. [51]

OECD (2020), *Ensuring data privacy as we battle COVID-19*, http://www.oecd.org/coronavirus/policy-responses/ensuring-data-privacy-as-we-battle-covid-19-36c2f31e/. [32]

OECD (2020), *Good Practice Guide on Consumer Data*, https://www.oecd-ilibrary.org/docserver/e0040128-en.pdf?expires=1590750306&id=id&accname=guest&checksum=300CC687BD4C64AECDB8A35A72E56B3F. [34]

OECD (2020), *Protecting Children Online: An Overview of Recent Developments in Legal Frameworks and Policies*, https://www.oecd-ilibrary.org/docserver/9e0e49a9-en.pdf?expires=1591134238&id=id&accname=ocid84004878&checksum=7F6435BE313D41CA23AADD97145727D3. [59]

OECD (2020), *Review of the 2012 Recommendation of the OECD Council on the Protection of Children Online - Second Consultation of the Informal Group of Experts, 30 September - 1 October 2019, OECD Headquarters: Summary of Main Points*, https://one.oecd.org/document/DSTI/CDEP/DGP(2020)9/en/pdf. [67]

OECD (2020), *Trustworthy artificial intelligence (AI) in education: promises and challenges*, http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=EDU/WKP(2020)6&docLanguage=En. [66]

OECD (2019), *Challenges to Consumer Policy in the Digital Age*, https://www.oecd.org/sti/consumer/challenges-to-consumer-policy-in-the-digital-age.pdf. [72]

OECD (2019), *Good Practice Guide on Online Advertising: Protecting Consumers in E-Commerce*, https://www.oecd-ilibrary.org/docserver/9678e5b1-en.pdf?expires=1597680773&id=id&accname=ocid84004878&checksum=6ECB53953A51765FDF2411018E442218. [74]

OECD (2019), *Good Practice Guide on Online Advertising: Protecting Consumers in E-Commerce*, http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/CP(2018)16/FINAL&docLanguage=En. [83]

OECD (2019), *OECD – University of Zurich Expert Consultation "Protection of Children in a Connected World" - 15-16 October, University of Zurich, Zurich, Switzerland*, https://one.oecd.org/document/DSTI/CDEP/SPDE(2019)3/en/pdf. [48]

OECD (2019), *Online Advertising: Trends, benefits and risks for consumers*, https://doi.org/10.1787/1f42c85d-en. [75]

OECD (2019), *Treating all children equally? Why policies should adapt to evolving family living arrangements*, http://www.oecd.org/els/family/child-well-being/Treating-all-children-equally-Policy-brief-2019.pdf. [27]

OECD (2018), *Consumer Product Safety in the Internet of Things*, https://www.oecd-ilibrary.org/docserver/7c45fa66-en.pdf?expires=1597749594&id=id&accname=guest&checksum=AC6BA01B8478B114F8FDCC5EBA7712D5. [76]

OECD (2018), *Toolkit for Protecting Digital Consumers: A Resource for G20 Policy Makers*, http://www.oecd.org/digital/consumer/toolkit-for-protecting-digital-consumers.pdf. [81]

OECD (2017), *Protection of Children Online: Preliminary Country Survey Findings and Proposal for Next Steps*, https://one.oecd.org/document/DSTI/CDEP/SPDE(2017)3/en/pdf. [69]

OECD (2016), *2016 Ministerial Meeting - The Digital Economy: Innovation, Growth and Social Prosperity*, https://www.oecd.org/internet/ministerial/meeting/Tomorrow%E2%80%99s-Internet-of-Things-discussion-paper.pdf. [41]

OECD (2014), *Consumer Policy Guidance on Mobile and Online Payments*, https://www.oecd-ilibrary.org/science-and-technology/consumer-policy-guidance-on-mobile-and-online-payments_5jz432cl1ns7-en. [73]

OECD (2011), *The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them, OECD Digital Economy Papers no. 179*, OECD Publishing, http://dx.doi.org/10.1787/5kgcjf71pl28-en. [1]

Ofcom (2020), *Children and parents: media use and attitudes report 2019*, https://www.ofcom.org.uk/__data/assets/pdf_file/0023/190616/children-media-use-attitudes-2019-report.pdf. [4]

O'Neill, B., S. Livingstone and S. McLaughlin (2011), *Final recommendations for policy, methodology and research*, LSE - EU Kids Online, http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20%282009-11%29/EUKidsOnlineIIReports/D7.pdf. [10]

Perren, S. et al. (2010), "Bullying in school and cyberspace: Associations with depressive symptoms in Swiss and Australian adolescents", *Child and Adolescent Psychiatry and Mental Health*. [18]

Przybylski, A. and N. Weinstein (2017), *A Large-Scale Test of the Goldilocks Hypothesis: Quantifying the Relations Between Digital-Screen Use and the Mental Well-Being of Adolescents*, https://journals.sagepub.com/doi/full/10.1177/0956797616678438. [44]

Report, M. (2015), *Parents on social media: Likes and dislikes of sharenting*, https://mottpoll.org/reports-surveys/parents-social-media-likes-and-dislikes-sharenting. [57]

Rich, M. (2019), *OECD – University of Zurich Expert Consultation "Protection of Children in a*, https://one.oecd.org/document/DSTI/CDEP/SPDE(2019)3/en/pdf. [19]

Rieke, A., M. Bogen and D. Robinson (2018), *Public Scrutiny of Automated Decisions: Early Lessons and Emerging Methods*, https://www.omidyar.com/sites/default/files/file_archive/Public%20Scrutiny%20of%20Automated%20Decisions.pdf. [61]

Royal College of Paediatrics and Child Health (2019), *The health impacts of screen time: a guide for clinicians and parents*, https://www.rcpch.ac.uk/sites/default/files/2018-12/rcpch_screen_time_guide_-_final.pdf. [49]

Royal College of Psychiatrists (2020), *Technology use and the mental health of children and young people*, https://www.rcpsych.ac.uk/docs/default-source/improving-care/better-mh-policy/college-reports/college-report-cr225.pdf. [50]

Smahel, D. et al. (2020), *EU Kids Online 2020: Survey results from 19 countries*, http://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf. [6]

Staufenberg, J. (2016), *French parents 'could face prison' for posting photos of their children on Facebook*, https://www.independent.co.uk/news/world/europe/french-parents-told-their-children-might-sue-them-for-pictures-put-on-facebook-a6906671.html. [56]

Steinberg, S. (2017), *Sharenting: Children's Privacy in the Age of Social Media*, https://law.emory.edu/elj/_documents/volumes/66/4/steinberg.pdf. [55]

Teixeira, C. and M. Boyas (2017), *Predictive Analytics in Child Welfare: An Assessment of Current Efforts, Challenges and Opportunities*, https://aspe.hhs.gov/system/files/pdf/257841/PACWAnAssessmentCurrentEffortsChallengesOpportunities.pdf. [39]

Twohey, M. (2020), *New Battle for Those on Coronavirus Front Lines: Child Custody - The New York Times*, New York Times, https://www.nytimes.com/2020/04/07/us/coronavirus-child-custody.html?referringSource=articleShare (accessed on 15 April 2020). [28]

UK Government (2017), *Internet Safety Strategy - Green Paper*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/650949/Internet_Safety_Strategy_green_paper.pdf. [3]

UNICEF (2019), *Faces, Fingerprints & Feet: Guidance on assessing the value of including biomtetric technologies in UNICEF-supported programs*, https://data.unicef.org/resources/biometrics/. [38]

UNICEF (2017), *Children in a Digital World*, https://www.unicef.org/media/48601/file. [11]

UNICEF (2017), *The State of the World's Children in 2017: Children in a Digital World*, https://www.unicef.org/publications/index_101992.html. [46]

UNICEF and Human Rights Center (2019), *Artificial Intelligence and Children's Rights*, https://www.unicef.org/innovation/media/10726/file/Executive%20Summary:%20Memorandum%20on%20Artificial%20Intelligence%20and%20Child%20Rights.pdf. [37]

United Kingdom Safer Internet Centre (n.d.), *What are the issues?*. [9]

United Nations (2020), *Policy Brief: The impact of COVID-19 on children*, https://unsdg.un.org/sites/default/files/2020-04/160420_Covid_Children_Policy_Brief.pdf. [33]

Van Der Hof, S. (2017), "I AGREE. . . OR DO I? — A RIGHTS-BASED ANALYSIS", *Wisconsin International Law Journal*, https://openaccess.leidenuniv.nl/bitstream/handle/1887/58542/S_van_der_Hof_-_I_AGREE._._._OR_DO_Ioe1oe.pdf?sequence=1. [12]

Whittaker, M. et al. (2019), *Disability, Bias, and AI*, https://ainowinstitute.org/disabilitybiasai-2019.pdf. [64]

World Childhood Foundation et al. (2020), *COVID-19 and its implications for protecting children online*, https://www.unicef.org/media/67396/file/COVID-19%20and%20Its%20Implications%20for%20Protecting%20Children%20Online.pdf. [31]

World Health Organization (2019), *ICD-11 for Mortality and Morbidity Statistics*, https://icd.who.int/browse11/l-m/en#/http%3a%2f%2fid.who.int%2ficd%2fentity%2f1448597234. [20]

Notes

[1] Hate messages are related to hate speech (which does not have a commonly accepted definition and may include “all forms of communication that spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance”).