

The 4Cs: Classifying Online Risk to Children

Livingstone, Sonia; Stoilova, Mariya

Erstveröffentlichung / Primary Publication

Kurzbericht / abridged report

Empfohlene Zitierung / Suggested Citation:

Livingstone, S., & Stoilova, M. (2021). *The 4Cs: Classifying Online Risk to Children*. (CO:RE Short Report Series on Key Topics). Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE - Children Online: Research and Evidence. <https://doi.org/10.21241/ssoar.71817>

Nutzungsbedingungen:

Dieser Text wird unter einer CC BY Lizenz (Namensnennung) zur Verfügung gestellt. Nähere Auskünfte zu den CC-Lizenzen finden Sie hier:
<https://creativecommons.org/licenses/by/4.0/deed.de>

Terms of use:

This document is made available under a CC BY Licence (Attribution). For more information see:
<https://creativecommons.org/licenses/by/4.0>



Children Online:
Research and Evidence

The 4Cs: Classifying online risk to children

CO:RE Short Report Series: Key topics



Sonia Livingstone and Mariya Stoilova

DOI: 10.21241/ssoar.71817



Please cite this report as:

Livingstone, S., & Stoilova, M. (2021). *The 4Cs: Classifying Online Risk to Children*. (CO:RE Short Report Series on Key Topics). Hamburg: Leibniz-Institut für Medienforschung | Hans-Bredow-Institut (HBI); CO:RE - Children Online: Research and Evidence. <https://doi.org/10.21241/ssoar.71817>

Editor: Veronika Kalmus

Language editor: Dawn L. Rushen

The CO:RE project is a Coordination and Support Action within the Horizon 2020 framework, which aims to build an international knowledge base on the impact of technological transformations on children and youth. Part of the knowledge base is a series of short reports on relevant topics that provide an overview of the state of research. This part is coordinated by Veronika Kalmus (University of Tartu, Estonia).

For all reports, updates, insights, as well as full details of all CO:RE Consortium members and CO:RE national partners throughout Europe and beyond, please visit core-evidence.eu



This project has received funding from the European Union's Horizon 2020 EU.3.6.1.1 – The mechanisms to promote smart, sustainable and inclusive growth DT-TRANSFORMATIONS-07-2019 – The impact of technological transformations on children and youth. **Grant Agreement ID 871018.**

Acknowledgements

We thank the joint Insafe and INHOPE networks for their input during an online consultation, and Karl Hopwood for working with us to make this happen. We also thank the CO:RE Consortium for their insights as we developed the classification of online risks, the reviewers of earlier drafts of this report, and the European Union's Horizon 2020 programme for the funding.

Contents

Key insights	3
Understanding online risk	3
The 3Cs of online risk	4
Adopting the classification	5
Contract risks: the fourth 'C'	6
Cross-cutting risks	8
Practitioner reflections	9
The new CO:RE classification	10
Conclusions	12
References	13
About the authors	15

Key insights

- **Risk classifications** guide practitioners and policymakers in their work and in communicating their results. EU Kids Online's (2009) **3Cs of online risk is used widely** as a classic point of reference for stakeholders internationally.
- It is timely to **update this classification**, given the variation in its use, the emerging risks in the digital environment, and our growing understanding of children's experiences of online risks of harm. As part of our CO:RE work on theories and concepts, we:
 - reviewed existing classifications of online risk to children by UNICEF, the International Telecommunication Union (ITU), Organisation for Economic Co-operation and Development (OECD), Council of Europe (CoE) and others;
 - consulted European practitioners of child internet safety from Insafe and INHOPE to build on their experience.
- This report proposes **a new CO:RE 4Cs classification**, recognising that online risks arise when a child:
 - engages with and/or is exposed to potentially harmful **CONTENT**;
 - experiences and/or is targeted by potentially harmful **CONTACT**;
 - witnesses, participates in and/or is a victim of potentially harmful **CONDUCT**;
 - is party to and/or exploited by a potentially harmful **CONTRACT**.
- The 4Cs classification **also distinguishes between aggressive, sexual and value risks**, as this is helpful in retaining a balanced view of the range of risks that children can encounter. We note that risks to the values that shape

childhood and society are increasingly prominent.

- In addition to the 4Cs, the new CO:RE classification **recognises important cross-cutting risks**, notably to children's privacy, health and fair treatment.
- Keeping in mind that **children's online opportunities** are paramount, and that a host of individual and societal **protective and vulnerability factors** mediate between risk and harm, we hope that the new classification is insightful for research, policy and practice that contributes to **realising children's rights** in relation to the digital environment (UN, 2021).

Understanding online risk

In the CO:RE project, our work on theory examines the key concepts that frame the field of research, policy and practice. The aim is to bring together diverse perspectives and interrogate their underlying assumptions in order to contribute to the collective ambition of understanding the experiences and consequences of growing up in a digital world.

A comprehensive understanding of children's engagement with the digital environment requires a balanced consideration of both risks and opportunities, recognising the full range of children's rights in a digital world (UN, 2021). Within this broader frame (Livingstone, 2016), risk is one of the key concepts identified for investigation by the CO:RE Consortium,¹ and is the focus of this short report.

In a fast-changing digital ecosystem, the nature of risk is continually evolving, sometimes exposing children to emerging risks well before adults know how to mitigate them. Risk has been defined as:

Uncertainty about and severity of the consequences (or outcomes) of an activity with respect to something that humans value. (Aven & Renn, 2009, p. 1)

¹ See <https://core-evidence.eu/understanding-children-online-theories-concepts-debates/>

The clash of possibly severe outcomes with human values inevitably raises concerns, and the digital environment, in which children are often very active, adds heightened uncertainties into the mix. No wonder that online risk is one of the most contested areas of children's digital experience, concerning many stakeholders and posing pressing challenges for research, policy and practice.

These challenges include understanding children's exposure to different types of online risk, and how regulatory, technical, social or individual interventions can be effective in developing strategies to cope with risk, mitigating or minimising any harmful consequences.

From the outset, it is vital to distinguish between online risk and harm. Conceptually, risk is the probability of harm, while harm includes a range of negative consequences to the child's emotional, physical or mental wellbeing (Livingstone, 2013). For example, exposure to pornography poses a risk to a child, but it is not a certainty that there will be harmful consequences.

Harmful outcomes depend on the nature of the risk (whether it is more probable or more severe in its consequences) and on the design, regulation and management of the digital environment (privacy settings, moderation services, access to helplines etc.). They also depend on the child and their circumstances, because what is problematic for one child might not be so for another. Such differences reflect societal factors (norms and regulations, political priorities, economic investments, education and family systems, etc.) as well as the individual protective or vulnerability factors that differentiate among children (including age, gender, digital skills, resilience, personality, socio-economic situation and family context).

It is paramount that our understanding of online risk is evidence-based, prioritising robust research conducted with and in relation to children.² Our understanding should also be informed by children's own views and experiences, and those of practitioners responding to child online risk and safety problems, rather than assuming or imposing a vision grounded in adult normative expectations or popular anxieties.

² See OECD (2011); UNICEF (2017); Smahel et al (2020).

In this short report we critically examine how online risks have been classified in order to develop a better understanding of children's online experiences and their potential or actual real-world consequences. After discovering how existing classifications have been adopted in the work of various stakeholders, we propose a new classification of online risk to children to meet the challenges of a changing digital environment and the practical imperatives of policymakers and practitioners.

This new classification highlights four dimensions related to the positioning of the child in the digital environment, and shows how these intersect with three dimensions regarding the nature of the risk. It also recognises the cross-cutting dimensions of privacy, discrimination and health risks.

The 3Cs of online risk

A comprehensive classification of online risk was proposed by EU Kids Online in 2009 (Staksrud & Livingstone, 2009; Staksrud et al., 2009), funded by the European Commission's (EC) Safer Internet Programme (now the Better Internet for Kids Programme).³ It was originally developed to answer the often-asked questions regarding 'What risks are we talking about?' and 'Why should policymakers take action?' It sought to disaggregate risks and raise awareness of the wide array of risks affecting children, including, but also going beyond, the main emphasis on pornography, grooming and cyberbullying that dominated the agenda at the time.

Taking a child-centred and evidence-based approach, EU Kids Online's classification identified two dimensions of risk: the positioning of the child in relation to the digital environment (as a recipient of mass-produced content, a participant in adult-initiated activity, and an actor in peer-to-peer exchanges), and the nature of the risk (aggressive, sexual, values and commercial).

This classification took a strongly child-centred approach. It highlighted that children should not be treated as solely vulnerable victims or protected at all costs, including at the cost of their online

³ www.betterinternetforkids.eu/nl/

opportunities. The idea was to recognise children’s agency as actors in a digital world, but without holding them unduly responsible for risks online or, especially, for the at-times harmful effects on their wellbeing or that of others. As will be seen later, the revised CO:RE classification recognises the child’s perspective and agency but also the power of societal and digital infrastructures to shape the child’s experiences and outcomes.

The original classification was tested using data from EU Kids Online’s two-wave European survey with internet-using children aged 9–16 conducted in 2010 (Livingstone et al., 2011) and 2017–19

(Smahel et al., 2020). It has been incorporated into the Global Kids Online model and its surveys of children in 18 countries (Livingstone et al., 2019). Taken together, these projects have generated cross-nationally comparable data from 40,000 children in more than 35 countries, providing an evidence base to inform policy priorities and establishing a baseline against which socio-technical change and policy interventions have been positively evaluated (Morton et al., 2019).⁴

Figure 1 shows the classification with exemplar risks in the cells.⁵

Figure 1: The EU Kids Online original 3Cs classification of online risks (Livingstone et al., 2011)

	<i>Content</i> Receiving mass-produced content	<i>Contact</i> Participating in (adult-initiated) online activity	<i>Conduct</i> Perpetrator or victim in peer-to-peer exchange
Aggressive	Violent/gory content	Harassment, stalking	Bullying, hostile peer activity
Sexual	Pornographic content	‘Grooming’, sexual abuse or exploitation	Sexual harassment, ‘sexting’
Values	Racist/hateful content	Ideological persuasion	Potentially harmful user-generated content
Commercial	Embedded marketing	Personal data misuse	Gambling, copyright infringement

Adopting the classification

The 3Cs classification became a classic point of reference since 2010, much cited by the policymakers and practitioners working to maximise children’s online opportunities and minimise their risks of harm.

To trace its use, we conducted a search for mention of ‘content, contact and conduct risks’ online and among reports and documents by relevant organisations. We found that the 3Cs of online risk

have informed the work of a range of key actors, albeit not always with a direct source, including UNICEF, the European Commission (EC), the Organisation for Economic Co-operation and Development (OECD), the Broadband Commission for Sustainable Development (2019), the International Telecommunication Union (ITU) (2020), the ICT Coalition (O’Neill, 2014; Croll, 2016), and others (O’Neill & Dinh, 2018; Green et al., 2019).⁶

One use is to classify the plethora of problems reported by children who call helplines. Supported by the EC’s Better Internet for Kids programme, the

⁴ See also www.eukidsonline.net and www.globalkidsonline.net

⁵ In keeping with EU Kids Online’s commitment to balance risks and opportunities, a parallel classification was proposed for opportunities, although it was little noted (Livingstone et al., 2018).

⁶ We did not find classifications in the work of ECPAT International, the European Union Agency for Fundamental Rights (FRA), GSMA, INTERPOL, Child Helpline International (CHI), CEO Coalition, European Network of Ombudspersons for Children or UNESCO.

work of the Safer Internet Centres (SICs) provides helplines across Europe:

Helplines provide information, advice and assistance to children, young people and parents on how to deal with harmful content, harmful contact (such as grooming) and harmful conduct (such as cyberbullying or sexting). (O'Neill & Dinh, 2018, p. 68)

Relatedly, the EC's self-regulatory initiative, the 'Alliance to better protect minors online',⁷ called on businesses to tackle 'existing and emerging risks that children and young people face online, including: harmful content (e.g. violent or sexually exploitative content); harmful conduct (e.g. cyberbullying), and harmful contact (e.g. sexual extortion)'.⁸

UNICEF's flagship annual publication *The state of the world's children* focused in 2017 on children in a digital world, and also used the classic EU Kids Online classification, recognising that while it is vital to address online risk, some degree of risky opportunities can afford children the chance to learn and become resilient, depending on their maturity and circumstances (UNICEF, 2017).

Undoubtedly, what has proved most valuable are the definitions of the 3Cs, as illustrated in Figure 2.

It is noteworthy that most uses of the classification refer to just one of the two dimensions (the child in relation to the digital environment) and discuss content, contact and conduct. Thus, they often omit the second dimension – the nature of the risk (aggressive, sexual, values, commercial) – and, perhaps in consequence, the exemplar risks highlighted and researched by EU Kids Online, among other researchers (Stoilova et al., 2021). Without the second dimension, however, commercial risks became somewhat neglected, leading to calls for revision of the original risk classification given rising evidence of the importance of commercial online risks to children.

⁷ See <https://ec.europa.eu/digital-single-market/en/alliance-better-protect-minors-online>

⁸ This framing is problematic in eliding risk and harm, because it is precisely in the gap between them that

Figure 2: The 3Cs of online risk (UNICEF, 2017)

Content risks: Where a child is exposed to unwelcome and inappropriate content. This can include sexual, pornographic and violent images; some forms of advertising; racist, discriminatory or hate speech material; and websites advocating unhealthy or dangerous behaviours, such as self-harm, suicide and anorexia.

Contact risks: Where a child participates in risky communication, such as with an adult seeking inappropriate contact or soliciting a child for sexual purposes, or with individuals attempting to radicalize a child or persuade him or her to take part in unhealthy or dangerous behaviours.

Conduct risks: Where a child behaves in a way that contributes to risky content or contact. This may include children writing or creating hateful materials about other children, inciting racism or posting or distributing sexual images, including material they have produced themselves.

Contract risks: the fourth 'C'

Digital technologies have developed significantly since the original typology was created, and the online ecology affords new opportunities but also new risks for children, particularly in relation to commercialisation and datafication. To respond to these changes and to reintroduce more prominently commercial dimensions of online risk, a fourth 'C' (variously labelled 'contract', 'commercial' or 'consumer') has been suggested.

In a 2018 redevelopment of the EU Kids Online classification, the fourth 'C' is conceived not as a commercial risk, but as a 'contract' risk that directly or indirectly connects children and digital providers. This reflects the dramatic rise in the commercialisation of children's personal data, arguably resulting in the 'datafication' of children themselves (Mascheroni, 2020).

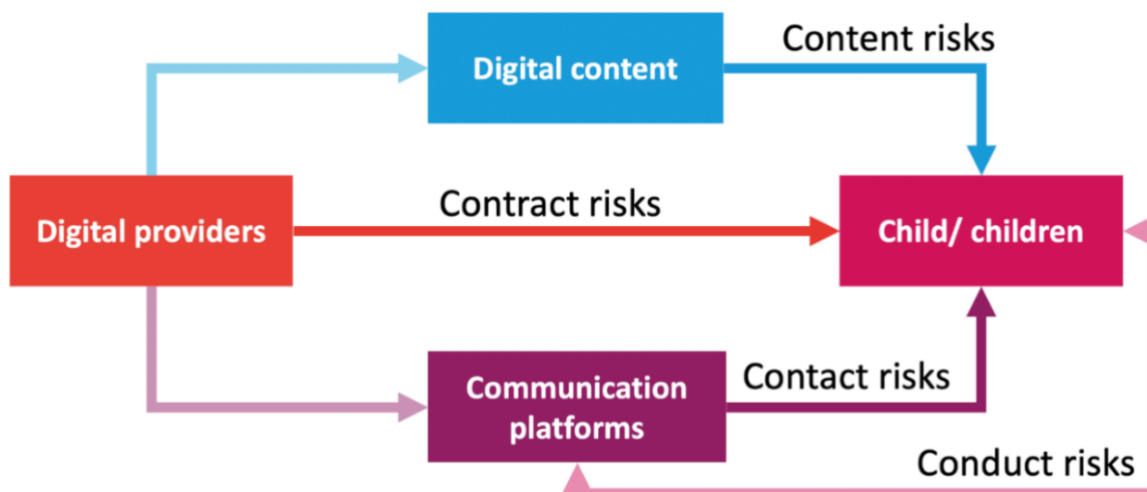
With the 4Cs, EU Kids Online has proposed not only a classification but also a digital ecosystem of online risks in which children are variously positioned and in which the different risks interact in increasingly

many empowering and safety interventions focus their efforts (e.g. digital literacy).

complex ways. This informed the CoE's *Handbook for policy makers on the rights of the child in the*

digital environment (Livingstone et al., 2020), as shown in Figure 3.

Figure 3: The EU Kids Online 4Cs model of online risks (Livingstone et al., 2020, p. 57, adapted from Hasebrink et al., 2018)



Most obviously, contract risks arise when the child 'accepts' (including unintentionally, involuntarily or unknowingly) the Terms of Service (or Terms and Conditions) of a commercial provider of digital products or services. Such contractual arrangements can bind the child in ways that may be unfair or exploitative, or which pose security or safety or privacy risks of which they may be unaware or over which they have little control or means of escape. Related risks arise because of the data processed by public and third sector organisations, as well as through a host of public-private partnerships (Stoilova et al., 2020).⁹ The Broadband Commission observes that children:

... have no way of understanding what they were signing up for when they installed the app or logged on to the site. Services and obligations that are designed for adults must be age-limited — so that children cannot sign up to them without a guardian's permission... While online, children also risk spending money without permission of parents or caregivers and having their data harvested.

(Broadband Commission for Sustainable Development, 2019, p. 34)

In short, contract risks arise when children use digital services as well as when they are impacted by digital transactions conducted by others in other ways (e.g. through institutional uses of digitised databases that include the child's profile, or algorithmic processing of personal data relating to the child or others connected with them; see O'Neill, 2014; 5Rights Foundation, 2019).

In naming this category of risks 'contract risks', we note the legal difficulties linked to contracts involving children, as well as the fact that users (of all ages) can be unaware of the contractual nature of their relationship with digital service providers. We also note that the contract that occasions a risk may not be with the child but with their parent or school or indeed, between a service provider and a third party, among other possibilities in the complex digital ecosystem. Nonetheless, on balance, we propose that the label 'contract' is helpful in pointing to a mix of marketing, data processing and other contractual risks that merit specific attention, most

⁹ This data may be given by or taken from children's digital activities, as well as inferred or assumed about them, or about others connected with them, through profiling operations. The fast-growing data ecosystem now provides an infrastructure not only for commercial transactions impacting on children but also for the digital

products and services that afford content, contact and content risks. The result is that the types of risk are increasingly interlinked, as are the solutions – e.g. data protection regulation can prevent some interpersonal or social forms of online harm (Stoilova et al., 2020).

but not all of which are commercial, and some of which are still emerging.

Cross-cutting risks

Even with the fourth ‘C’, there are dimensions of online risk that might not fit neatly into these categories. UNICEF’s State of the World’s Children participatory workshops (UNICEF, 2017) revealed that children report concerns about risks that do not fit well with the classification, such as technological problems and parental intrusion in their online lives. In its draft *Recommendation on children in the digital environment*, the OECD observes that:

...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. (OECD, 2021, p. 4)

Do we need to go beyond the 4Cs and add new and cross-cutting elements? Recognising that digital service providers need to know which risks are of greatest concern so that they can innovate in safety by design, and building on multi-stakeholder consultation (5Rights Foundation, 2019), the OECD recently proposed that some risks are seen as cross-cutting in nature – such as those related to privacy, advanced technological features (e.g. Internet of Things [IoT], artificial intelligence [AI], biometrics, predictive analytics), health and wellbeing.

Note that the OECD builds on the EU Kids Online classification, although it defines the fourth ‘C’ as ‘consumer risks’.¹⁰ The second dimension of the figure lists ‘risk manifestations’ (or examples of ways in which children might encounter potential harms online), although it does not organise them further. This is shown in Figure 4.

Figure 4: Children in the digital environment: revised typology of risks (OECD, 2021)

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

¹⁰ The OECD’s proposed category of consumer risks includes four manifestations: (1) marketing risks; (2)

commercial profiling risks; (3) financial risks; and (4) security risks.

Practitioner reflections

To discover how practitioners working in the field of child online protection classify risks, and whether they consider that revisions to the 4Cs are needed, in October 2020 we conducted an online workshop with 125 members from the Insafe and INHOPE networks from over 20 countries.¹¹

The consultation sought to:

- **Identify familiar and emerging online risks** affecting children across Europe, and to see whether these are common across or specific to different contexts or countries.
- Consider **whether classifications of online risk are adopted in practice and useful**, and if so, what purpose they serve and what the strengths and shortcomings of the available classifications are.

Insafe and INHOPE members contributed a series of reflections on the risk classification and its possible development.¹² After a lively discussion, there was widespread agreement that risk classifications are useful for practitioners.

Practical purposes of the classification of online risks include:

- Identifying the range and diversity of risks, including identifying emerging risks.
- Making comparisons and capturing trends across risks and across time/contexts.
- Systematically communicating results and priorities to expert, policymaker and lay audiences.
- Highlighting the need for resources, budgets and training.
- Classifying the types of risks reported via input from helplines and complaints mechanisms.
- Targeting planning, interventions and awareness-raising campaigns.

- Mapping evidence to risk categories and identifying evidence gaps.

In practice, some organisations will always generate their own classifications – for instance, when working bottom-up from helpline calls to track local trends – while others will not need to classify risks in their work.

Overall, however, the consensus was that it is valuable to have a shared approach to answering questions such as ‘What do we mean by online risks?’ and ‘Which risks are emerging?’ or ‘Which should be prioritised?’ and ‘How is my country doing compared with others?’

For researchers, the classification is useful in providing a common terminology by which to report and review findings, and for mapping where evidence is sufficient and where there are pressing gaps. As for practitioners, researchers also repeatedly find that risks intersect, bridging offline and online experiences, and compounding adverse outcomes for the more disadvantaged or vulnerable children. But we can only report such complex relations among risks if we first identify those risks, so the classification remains useful.

It was also generally agreed that, to be useful, risk classifications should prioritise:

- **Flexibility** – the classification has to be broad and flexible so that new risks can be added when needed or when we need to refer to different groups of children or address stakeholders.
- **Clarity** – the risks should not overlap with each other and they should map readily onto the reports from children or practitioners about problematic experiences. Recognising that this is a complex domain, the call was also to avoid oversimplification, recognising ‘hybrid threats’ that could be classified in more than one domain (e.g. identity theft could be linked to contact, conduct or contract risks depending on the circumstances; online pressures relating to body image can have both sexual and value dimensions; see Figure 6).
- **Examples** – to be readily understood and applicable to the practical work, including real-

¹¹ See www.betterinternetforkids.eu/practice/articles/article?id=6745701

¹² For detailed findings, see Livingstone et al. (2021).

world examples in the cells of the classification table is important. While it is recognised that the examples provided cannot be comprehensive, they should map onto the actual problems reported by children or encountered by practitioners. They should also resonate with audiences (parents, policymakers, etc.) when risk-related work is made public.¹³

Two structural changes to the online risk classification were recommended:

- **Inclusion of the fourth 'C'** – this is needed, and it was widely thought that the term 'contract' is more inclusive than 'commercial' or 'consumer' risks in recognising that risks can arise when the child is party to a contract with public and third sector organisations as well as commercial bodies, especially with the prevalence of public–private partnerships in complex digital ecologies.
- **Cross-cutting risks** – the recognition of risks that cut across several or all of the 4Cs was also agreed, although much debated. Again, this arises because of the complexity of the digital ecology and also because risks are interrelated, and they can affect multiple dimensions of a child's experience. The effects on children's health (e.g. health risks linked to excessive screen use) were raised by multiple contributors. So, too, were the array of privacy risks experienced by children online, many of which arise from data processing (and so can be classified as contract risks) but that can also arise in relation to content, and through interpersonal contact and conduct.

Even after discussion, different views remained regarding:

- **Country specificities** – should the classification differ by country and context to recognise different legal, regulatory and cultural factors that shape children's exposure to risk? It emerged, however, that pan-European commonalities are more notable

¹³ In this regard, the 'risk manifestations' in the OECD classification were found to be difficult to interpret both because they are abstract and yet overlapping, and because the legal/illegal boundary varies by country/policy context. Relatedly, the idea of cross-cutting technological risks was not taken up, possibly because all online risks have a technological dimension or because the examples given in the OECD typology

than country differences, and are often more worthy of attention given the benefits of sharing insights and best practice across countries, and in working towards common solutions.

- **Extending the classification with a fifth 'C'** – a range of possibilities was suggested, including that the classification could identify **the consequences** of risk, such as health or wellbeing, or other abuses of children's rights; and/or distinguish illegal ('*criminal*') from harmful risks. However, this discussion threw up the many differences not only by country (e.g. in which online risks are illegal) but also organisational sector, type and purpose. It was agreed, therefore, that although 5Cs may be useful on occasion, this should be left to each country or organisation to determine for itself.

The new CO:RE classification

We propose a new CO:RE classification of online risk, learning from the above experiences and from consultation with the CO:RE Consortium. Risk is recognised as relational, emerging from the dynamic interaction between the child's agency and the agency of others operating in the digital environment (including through automated processing such as algorithms and as embedded in digital design and operation).¹⁴

The 4Cs of online risks of harm are content, contact, conduct and contract risks, as explained in Figure 5. The classification has the merit, we suggest, of order and clarity. We believe it to be fit for purpose, recognising the multiple positions that children may occupy in an increasingly significant and powerful digital environment, including continually emerging online risks. It is orderly and clear, and it provides practitioner-tested exemplars of key risks, including those that have become familiar in recent decades and those that are emerging and new.

The introduction of contract risks as the fourth 'C' incorporates risks previously labelled 'commercial'.

are linked most closely to contract risks or again, to privacy or discrimination.

¹⁴ This framing of the 4Cs overcomes the previous potential for misunderstanding (e.g. the implication that a child may participate willingly in contact abuse, or that they are mere receivers of content rather than also actively seeking it).

Figure 5: The CO:RE 4Cs of online risk


- **Content risks:** The child engages with or is exposed to potentially harmful content. This can be violent, gory content, hateful or extremist content, as well as pornographic or sexualised content that may be illegal or harmful, including by being age-inappropriate. Content online may be mass-produced or user-generated (including by the child), and it may be shared widely or not.
- **Contact risks:** The child experiences or is targeted by contact in a potentially harmful adult-initiated interaction, and the adult may be known to the child or not. This can be related to harassment (including sexual), stalking, hateful behaviour, sexual grooming, sextortion or the generation of sharing of child sexual abuse material.
- **Conduct risks:** The child witnesses, participates in or is a victim of potentially harmful conduct such as bullying, hateful peer activity, trolling, sexual messages, pressures or harassment, or is exposed to potentially harmful user communities (e.g. self-harm or eating disorders). Typically conduct risks arise from interactions among peers, although not necessarily of equal status.
- **Contract risks:** The child is party to and/or exploited by potentially harmful contract or commercial interests (gambling, exploitative or age-inappropriate marketing, etc.). This can be mediated by the automated (algorithmic) processing of data. This includes risks linked to ill-designed or insecure digital services that leave the child open to identity theft, fraud or scams. It also includes contracts made between other parties involving a child (trafficking, streaming child sexual abuse).
- **Cross-cutting risks:** Some risks relate to most or all of the four categories and can have multiple manifestations across the different dimensions (aggressive, sexual, values). These include online risks relating to privacy, physical or mental health, inequalities or discrimination.

Hence the new classification now distinguishes three dimensions in relation to the nature of the risk: aggressive, sexual and values. It is noteworthy that interest in value-related risks (e.g. misinformation, radicalisation, self-harm, algorithm bias) has grown in recent years, now attracting as much attention and anxiety as aggressive and sexual risks.

Finally, the new classification recognises three types of cross-cutting risk – to children’s privacy, their health, and their fair treatment and equal inclusion in a digital world. These risks, we suggest, can occur in relation to any and all of content, contact, conduct and contract risks (see Figure 6).

Importantly, it should be noted that, although some risks are particularly cross-cutting in nature, many of the online risks to children intersect and hybridise, depending on the circumstances, and more so as the digital environment evolves. Hence the classification and its exemplars are offered here as a way of organising and opening up further investigation, rather than as implying that risks are simple or disconnected.

Figure 6: The CO:RE classification of online risk to children

	Content Child engages with or is exposed to potentially harmful content	Contact Child experiences or is targeted by potentially harmful <i>adult</i> contact	Conduct Child witnesses, participates in or is a victim of potentially harmful <i>peer</i> conduct	Contract Child is party to or exploited by potentially harmful contract
Aggressive	Violent, gory, graphic, racist, hateful or extremist information and communication	Harassment, stalking, hateful behaviour, unwanted or excessive surveillance	Bullying, hateful or hostile communication or peer activity e.g. trolling, exclusion, shaming	Identity theft, fraud, phishing, scams, hacking, blackmail, security risks
Sexual	Pornography (harmful or illegal), sexualization of culture, oppressive body image norms	Sexual harassment, sexual grooming, sextortion, the generation and sharing of child sexual abuse material	Sexual harassment, non-consensual sexual messaging, adverse sexual pressures	Trafficking for purposes of sexual exploitation, streaming (paid-for) child sexual abuse
Values	Mis/disinformation, age-inappropriate marketing or user-generated content	Ideological persuasion or manipulation, radicalisation and extremist recruitment	Potentially harmful user communities e.g. self-harm, anti-vaccine, adverse peer pressures	Gambling, filter bubbles, micro-targeting, dark patterns shaping persuasion or purchase
Cross-cutting	Privacy violations (interpersonal, institutional, commercial) Physical and mental health risks (e.g., sedentary lifestyle, excessive screen use, isolation, anxiety) Inequalities and discrimination (in/exclusion, exploiting vulnerability, algorithmic bias/predictive analytics)			

Conclusions

We hope this new classification serves constructive purposes for researchers, policymakers and practitioners working to minimise or manage online risks to children’s rights and wellbeing. The classification offers the foundations of a better understanding of online risk to children, and it can underpin the work of different stakeholders:

- Policymakers can use it to identify what risks matter and why, what evidence supports them, and how they fit within or fall outside existing regulatory frameworks.
- Parents and the public can use it to learn what can be done about the different risks and what to look out for.
- Researchers can use the classification to develop comprehensive definitions and

measures of online risk, and to organise, compare and report findings.

- Practitioners can use it in their work to classify and understand the problems reported to them, to communicate with different audiences, and to manage and bid for resources.

The classification will need careful framing for different audiences, so more work needs to be done on implementation. Moreover, as society and the digital environment continues to change, the classification will need revisiting in the future.¹⁵

It should be noted that our focus has been on children online, leaving others to attend to the important risks of *not being online* – digital exclusion, struggles for access and connectivity, lack of digital skills, and so forth.

We did not focus on the factors that account for whether, when or why some children are more likely to encounter particular online risks than others, nor the protective or vulnerability factors – whether

¹⁵ We sought to future-proof the classification by describing risks in broad terms rather than focusing on very particular or time-bound risks, although we

appreciate they arouse concern (e.g. sharenting, influencers, deep fakes, viral challenges).

concerning children, their circumstances, the digital environment or its regulation and management – that account for harmful outcomes. Again, this has been amply addressed elsewhere.¹⁶

It is also important to see risk as only one of the dimensions of children's online experiences, alongside opportunities and among many factors that intersect to influence children's outcomes (Livingstone, 2016). Indeed, while the digital environment affords children a range of risks, it also offers many opportunities to benefit, and this merits a parallel analysis. If society becomes overprotective, it can inadvertently undermine the very opportunities for which society provides children with internet access. We will address the 4Cs of online opportunities in our future work.

References

- 5Rights Foundation (2019). *Towards an internet safety strategy*. 5Rights. <https://5rightsfoundation.com/uploads/final-5rights-foundation-towards-an-internet-safety-strategy-january-2019.pdf>
- Aven, T & Renn, O. (2009). On risk defined as an event where the outcome is uncertain, *Journal of Risk Research*, 12(1), 1–11.
- Broadband Commission for Sustainable Development (2019). *Child online safety: Minimizing the risk of violence, abuse and exploitation online*. ITU and UNESCO. <https://unesdoc.unesco.org/ark:/48223/pf0000374365?posInSet=1&queryId=1a93f340-75cf-42d8-adfe-4f4b718fcad3>
- Croll, J. (2016). *Let's play it safe: Children and youths in the digital world. Assessment of the emerging trends and evolutions in ICT services*. ICT Coalition. www.ictcoalition.eu/medias/uploads/source/available%20here.pdf
- Green, A., Wilkins, C. & Wyld, G. (2019). *Keeping children safe online*. Nominet, NPC and Parent Zone. www.thinknpc.org/wp-content/uploads/2019/07/Keeping-Children-Safe-Online-NPC-Nominet-ParentZone-2019.pdf
- Hasebrink, U., Rechlitz, M., Dreyer, S., Brüggem, N., Gebel, C. & Lampert, C. (2018). *What are you concerned about? Classifying children's and parents' concerns regarding online communication*. ECREA Conference, November. https://leibniz-hbi.de/uploads/media/default/cms/media/hl9lr5_2018-11-01_ECREA_Hasebrink%20et%20al_What%20are%20you%20concerned%20about.pdf
- ITU (International Telecommunication Union) (2020). *Child Online Protection (COP) guidelines*. www.itu-cop-guidelines.com/
- Livingstone, S. (2013). Online risk, harm and vulnerability: Reflections on the evidence base for child internet safety policy. *ZER: Journal of*

¹⁶ OECD (2011); Livingstone et al. (2012); O'Neill and Dinh (2018); Smahel et al. (2020); Stoilova et al. (2021).

Communication Studies, 18(35), 13–28.
<http://eprints.lse.ac.uk/62278/>

Livingstone, S. (2016). *A framework for researching Global Kids Online: Understanding children's well-being and rights in the digital age*. London: Global Kids Online.
www.globalkidsonline.net/framework

Livingstone, S., Haddon, L., Görzig, A. & Ólafsson, K. (2011). *Risks and safety on the internet: The perspective of European children: Full findings and policy implications from the EU Kids Online survey*.
<http://eprints.lse.ac.uk/33731/>

Livingstone, S., Haddon, L. & Görzig, A. (eds) (2012). *Children, risk and safety online: Research and policy challenges in comparative perspective*. Policy Press.

Livingstone, S., Kardefelt-Winther, D. & Saeed, M. (2019). *Global Kids Online comparative report*. UNICEF Office of Research – Innocenti, Florence.
www.unicef-irc.org/publications/1059-global-kids-online-comparative-report.html

Livingstone, S., Lievens, E. & Carr, J. (2020). *Handbook for policy makers on the rights of the child in the digital environment*. Council of Europe.
<https://rm.coe.int/publication-it-handbook-for-policy-makers-final-eng/1680a069f8>

Livingstone, S., Mascheroni, G. & Staksrud, E. (2018). European research on children's internet use: Assessing the past and anticipating the future. *New Media & Society*, 20(3), 1103–1122,
<http://eprints.lse.ac.uk/68516>

Livingstone, S., Stoilova, M. & Hopwood, K. (2021). *Classifying known and emerging online risks for children: A child practitioners' perspective*. CO:RE–Children Online: Research and Evidence.
https://core-evidence.eu/wp-content/uploads/2021/02/WP5_online-forum-III_event-report.pdf

Mascheroni, G. (2020). Datafied childhoods: Contextualising datafication in everyday life. *Current Sociology*, 68(6), 798–813.
[doi:10.1177/0011392118807534](https://doi.org/10.1177/0011392118807534)

Morton, S., Grant, A., Cook, A., Berry, H., McMellon, C., Robbin, M. & Ipince, A. (2019). *Children's experiences online: Building global*

understanding and action. UNICEF Office of Research – Innocenti. www.unicef-irc.org/publications/1065-childrens-experiences-online-building-global-understanding-and-action.html

O'Neill, B. (2014). *First report on the implementation of the ICT principles*. Dublin Institute of Technology & ICT Coalition.
www.ictcoalition.eu/medias/uploads/source/First%20Report%20on%20the%20Implementation%20of%20the%20ICT%20Principles.pdf

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*.
www.betterinternetforkids.eu/documents/167024/2637346/BIK+Map+report+-+Final+-+March+2018/a858ae53-971f-4dce-829c-5a02af9287f7

OECD (Organisation for Economic Co-operation and Development) (2011). *Recommendation of the Council on the protection of children online*.
<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0389>

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

Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S. & Hasebrink, U. (2020). *EU Kids Online 2020: Survey results from 19 countries*.
<https://doi.org/10.21953/lse.47fdeqi01of0>

Staksrud, E. & Livingstone, S. (2009). Children and online risk: Powerless victims or resourceful participants? *Information, Communication and Society*, 12(3): 364–387.
<http://eprints.lse.ac.uk/30122/>

Staksrud, E., Livingstone, S., Haddon, L. & Ólafsson, K. (2009). *What do we know about children's use of online technologies: A report on data availability and research gaps in Europe* (2nd edn). EU Kids Online.
<http://eprints.lse.ac.uk/24367/>

Stoilova, M., Livingstone, S. & Khazbak, R. (2021). *Investigating risks and opportunities for children in*

a digital world: A rapid review of the evidence on children's internet use and outcomes. Innocenti Discussion Paper 2020-03. UNICEF Office of Research – Innocenti. www.unicef-irc.org/publications/1183-investigating-risks-and-opportunities-for-children-in-a-digital-world.html

Stoilova, M., Livingstone, S. & Nandagiri, R. (2020). Digital by default: Children's capacity to understand and manage online data and privacy. *Media and Communication*, 8(4), 197–207. www.cogitatiopress.com/mediaandcommunication/article/view/3407

UN (United Nations) Committee on the Rights of the Child (2021). *General Comment 25 on children's rights in relation to the digital environment*. Geneva: UN. https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=5&DocTypeID=11

UNICEF (2017). *State of the world's children: Children in a digital world*. www.unicef.org/publications/index_101992.html

About the authors



Sonia Livingstone FBA, OBE is a professor in the Department of Media and Communications, London School of Economics and Political Science (LSE). Her 20 books include *Parenting for a digital future: How hopes and fears about technology shape children's lives*. She directs the Digital Futures Commission (with 5Rights Foundation) and Global Kids Online (with UNICEF Office of Research – Innocenti) and has advised the UN Committee on the Rights of the Child, European Commission, European Parliament, Council of Europe, ITU, OECD and others on children's risks and rights in a digital age. See www.socialivingstone.net



Mariya Stoilova is a post-doctoral researcher at the Department of Media and Communications, London School of Economics and Political Science (LSE). Her work falls at the intersection of child rights and digital technology, focusing particularly on the opportunities and risks of digital media use in the everyday lives of children and young people, data and privacy online, digital skills, and pathways to harm and wellbeing. Mariya's work incorporates multi-method evidence generation and cross-national comparative analyses. For projects and publications, see <http://www.lse.ac.uk/media-and-communications/people/research-staff/mariya-stoilova>