Children Online:
Research and Evidence

Classifying known and emerging online risks for children: a child practitioners' perspective

Sonia Livingstone & Mariya Stoilova,

with Karl Hopwood

1. Executive summary

The aim of the online forums is to initiate a discussion with a wider public around a theory-based topic. Originally envisioned as an online discussion of a piece of writing, we have been exploring different formats for facilitating a conversation. The first online forum (D5.4) sought to collect suggestions from researchers and stakeholders regarding useful and insightful resources on key theories and concepts related to children's engagement with digital technologies; these were then compiled into an annotated bibliography (D5.1) which is being continually updated. The second online forum (D5.5) collected key questions from researchers and stakeholders participating in a public event on the role of digital technologies for children's well-being; it then sourced answers from experts and publicised the results. The third online forum (D5.6) focused on online risks for children and involved a discussion with child safety practitioners from the Insafe[1] and INHOPE[2] networks about known and emerging risks, classifying online risk and applying risk classification to child protection work. The findings of the third forum are explained in this report.

There was widespread agreement that risk classifications are useful for practitioners in their professional task. They identified a range of purposes: to encompass the diversity of online risks, make comparisons, capture trends, communicate results, raise awareness, plan interventions, and structure training. However, existing risk classifications are outdated and need revisions to reflect the changes in the digital environment, particularly related to its globalisation, commercialisation and datafication. The changes also need to reflect children's engagement with digital technologies- their agency and how lives have become "digital by default".[3] Based on the input from this forum the CO:RE project is developing a revised classification of online risk to children.

[1] Insafe is a European network of Awareness Centres promoting safer and better usage of internet, it is co-funded by the Safer Internet Programme.

[2] INHOPE is a network of 47 hotlines around the world that operate in all EU member states, Russia, South Africa, North & South America, Asia, Australia and New Zealand. Its focus is combating online child sexual abuse material.

[3] See Stoilova et al. (2020)

www.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

This document reflects only the authors' view and the Commission of the European Union is not responsible for any use that may be made of the information it contains.

2. Online forum III: Classifying known and emerging online risks for children

2.1. Analysis of the existing risk classifications and their adoption

We first identified the classifications of online risk to children that are currently in circulation and that are applied by key international stakeholders in their practice work. We conducted an online search[4] identifying reports on children's online risk. We also searched the websites of key international stakeholders for relevant reports, working papers, policy papers, etc. Finally, we used the UK as a case study and looked for some national examples of the practical application of risk classifications. We compiled all relevant materials and analysed the main definitions and classification of online risk. In brief, the findings suggest that:

- One of the most comprehensive typologies of online risk, which has become a classic point of reference over the past decade, was proposed by EU Kids Online in 2009.[5] It distinguishes between three types of risk: content, contact, and conduct (3Cs).
- 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 Council of Europe, the Organisation for Economic Co-operation and Development (OECD), the Broadband Commission for Sustainable Development, the International Telecommunication Union (ITU), the ICT Coalition, and others.[6] In the UK the 3C classification is applied by Ofcom, the UK Council on Child Internet Safety (UKCCIS, now UKCIS), the UK Safer Internet Centre (UKSIC), the 5 Rights Foundation.
- In practice, the 3Cs classification of risks is applied with various modifications, particularly relating to attempts to give a more prominent place of risks related to commercialisation, datafication, and profiling.
- Many international agencies work without an established classification of risk.[7]

These findings were used to design the online forum – its aims, topics, and activities. We also designed a task for advance preparation which was distributed to all participants before the forum.

2.2. An online forum with child practitioners

We organised the online forum on risk as part of joint training meeting of the Insafe and INHOPE networks of European Safer Internet Centres (SICs). This training aimed to facilitate sharing of experience and good practice between the two networks and to explore areas of common ground and opportunities for closer working between helplines, hotlines and

[4] The search included various combinations of search words including "risk classification", "risk typology" "content+contact+conduct risk", "child", "online".
[5] See Staksrud & Livingstone (2009)
[6] For example, see UNICEF (2017), Livingstone et al. (2020), O'Neill (2014), Croll (2016), Broadband Commission for Sustainable Development (2019), ITU (2020), O'Neill and Dinh (2018) and Green et al. (2019).
[7] However, we did not see the typology mentioned in the work of ECPAT International, the European Union Agency for Fundamental Rights, the GSMA, INTERPOL, Child Helpline International, the CEO Coalition, European Network for Ombudspersons for Children (ENOC), UN Commission on Crime Prevention and Criminal Justice, UNESCO.

awareness centres. The forum was designed to support this task and allow the practitioners to discuss their work on online risk in more detail. The aims were to:

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

The forum was attended by 125 child practitioners from a range of European countries. The participants work professionally with children who encounter online risk of harm in a variety of contexts, including helplines, law enforcement and awareness-raising. Thus, their daily lives put them in touch with the emerging trends and everyday realities of European children's experiences of the digital environment and the risks it affords.

The forum involved (see also Appendix 1):

- presentations from the WP5 team comparing classifications of online risks to children that have been applied by international stakeholders;
- breakout sessions for detailed discussion of country examples in which the practitioners used an online platform to exchange ideas and record their discussion;
- plenaries focusing on sharing insights, the discussion of emerging trends and identifying priorities for practice.

3. Forum findings: the need for a revised classification of online risk

The main findings suggest the need for a revised classification of risks which incorporates recent and new developments and stakeholder requirements for flexibility and adaptability. Drawing on the expertise and work of Insafe and INHOPE, the findings from the online forum will be used to re-evaluate and update the classification of emerging and established risks for children and young people online. We are currently developing a short report which will propose a new CO:RE classification of online risk, developed in consultation with the CO:RE General Assembly.

The main views, opinions and experiences expressed in the forum are summarised below.

Looking across Europe: common and specific risks

- Most risks tend to be relevant to all country contexts. In the last 20 years the digital products and services that young people are using have become increasingly similar across all countries. Some of the more prevalent risks that all helplines, hotlines and awareness centres come across are cyberbullying, aggressive online behaviour, stalking, hate speech, racism, sexting, grooming, fake news, misinformation and disinformation, peers/influencers and the (false) body image, self-esteem.

- While risks are common in many countries, they can become intensified in certain contexts. For example, more racist or biased information might proliferate in relation to certain political events in a particular country. In smaller countries the consequences of some online risks (e.g., defamation or revenge pornography) can have more negative effects than in large countries where the reach of such negative content is more moderate.

- Legislative approaches are common, but policies and mechanisms differ. Legislation is mostly based on EU-level top-down efforts rather than related to the particular country context. However, countries have different capacities to respond to these risks. For example, some countries lack effective mechanisms of tackling online risks, such as cyber bullying, while others have well-developed policy frameworks and venues for action or even a law.[8] (O’Neill, 2014).

- While risks are similar, the language in which they are described might be different. Some countries have their own classifications of online risk, others use the established ones (like the 3Cs), and some do not use classifications. For example, in Luxembourg risks are divided into (1) communication risk (e.g., sexting, “cyberbullying”, grooming); 2) consumption risk (e.g. data protection, attention span of the users); 3) content risk (e.g. hate speech, content not adapted for kids, harmful content, etc).

> *“Legislation is not necessarily based on the national context, it’s coming more top-*down at EU-level. This might leave a gap in relation to the discussion of issues relevant to the national context if everyone is looking only at the EU-*level”*
>
> *“Just because some risks are well*-known to children and young people, this does not necessarily mean that they understand the consequences, for example, from *sexting, cyberbullying, advertising”*
>
> *“Quite a lot of young people do know the consequences, but don’t react accordingly* to theme, since they feel invulnerable themselves – *‘*privacy paradox*’”*
>
> *“Seeing children much more politically and actively engaged in discussions which* can expose them to risk of harm from those with polar opposite views. This can lead to more segregation which we see playing out in online spaces. Online spaces were designed to bring people together but often facilitate polarisation and be *disempowering for young people.”*

New and emerging risks: risks are constantly changing

- Technological changes bring new risks. Some risks have emerged more recently, mostly in relation to technological innovations, and are currently not covered by the existing classifications of online risks. These relate to dark patterns, algorithms, deep fakes, persuasive design, face recognition, the rise of influencer culture.

- Changing nature of existing risks: some risks are becoming more prevalent than before, while previously prominent risks are reducing over time. Fake news is an example of risk which is constantly evolving and is hard for the helplines to keep up with the changing context. Known risks also might transform and receive new manifestations, for example in relation to virtual reality (VR) or artificial intelligence (AI), internet of things (IoT). Hence, well-known risks might need to be re-examined in relation to their new manifestations.

- While risks are fairly well understood, their consequences might not be that well known. There are also differences based on the type of risk: contact risks are well understood and addressed by policy and practice, but conduct risks are understood less well, especially in relation to coercion. Harvesting personal information is still not well understood by children.

[8] Austria has a cyber-bulling law since 2016 §107c StGB

- New engagement with the digital: children tend to start using the internet much earlier than before and the effects of this early engagement, especially in the long-run, are not known. It is also unclear how the more pervasive role of digital technologies in children's everyday lives affect them.

- Child development: as children grow older the nature and intensity of risk they experience changes, and so does children's ability to respond to these risks. This suggests that children need to learn about age-relevant risks at the right time.

- Parental mediation is also changing with gaps between parental skills playing an important role. There is a generation of digitally skilled and engaged parents able to support their children. However, some parents lack the skills or ability to support their children's safe internet use and think that "the digital generation" is competent and needs less help and attention, therefore they engage in much less mediation. We do not know if this might mean more risks for children or increased gaps between children.

- Risks vary based on children's personal experiences: variations in risk would also depend on the personal experience and perception of risk. Online and offline risks are connected, so children's life circumstances can affect their exposure to and coping with online risks as well.

> *"We have evidence from some countries like Austria that children start using online* technologies as early as 1 year old. This is much earlier than before and we are not sure *what the consequences might be for these young children"*
>
> *"If you have a box for* revenge porn and this is no longer one of the main threats, *what do you do to capture that history?"*
>
> *"What is the most important to learn at each age and what is considered a* risk factor for that age? If you are teaching them about the sexual side of think at a very *young age, that's also a potential risk."*
>
> *"Innocent words can have potentially a double meaning online. Children look up* something innocently, see something potentially dangerous but they feel that they have done something wrong by finding that *content, so they don't report it. So* educating them that this is out of their control, that the online environment is a very *different one"*
>
> *"It is hard to place this topic of digital balance in one of the brackets. It is very much* related to the commercia*l risks, but also a bit broader. Young people (and 'old'* people as well) spent more and more time on their devices and I think this could mean a big risk for the way they function within a democracy, as they are in a *constant state of being 'overload' with* disinformation. I think this is a big health risk, both physically and mentally, but it also influences the way you are connected to *your surroundings."*
>
> *"Given the COVID*-19 crisis, new risks have emerged related to increasing isolation and mental health p*roblems"*
>
> *"there is a risk of not having an effective recourse to dealing with risk/harm. […]* you need to put this risk in the context of the support available for young people, and this lack of obvious support can exacerbate the risks facing children to the *point that it almost becomes a risk itself."*

The value of risk classifications: diversity based on stakeholder groups

- The usefulness of risk classifications depends on the stakeholders involved. Hotlines find it important to identify the types of risk in order to report them. This is less relevant for the helplines and awareness centres which focus on providing support. But they too can find risk classifications useful for planning purposes to make sure that the existing provision covers the full spectrum of risks.

- Having a classification offers a good way of communicating findings, for example to policy-makers, industry, parents, teachers and children. It helps to point out where efforts need to be concentrated to minimise harm, and with planning and attracting funding.

- Risk classifications can be used to quantify risks and make comparisons between different dimensions of risk, different country contexts, and to reflect on changes over time.

- Risk classifications can be used to develop robust research methodology or train practitioners.

- In countries where the focus is more on the positive aspects of internet use, a classification which only focuses on risk but does not discuss the opportunities is less relevant.

> *“There is a practical value in online* risk classifications especially for comparing research across countries and even more importantly for seeing the development of risks over time.*”*

> *“We agreed altogether that we should classify risk for better awareness*-raising, *study and research.”*

> “From a hotline point of view, the classification has a great practical value. A classification is already present from a legislation point of view (crime/not crime; illegal/legal). The value of a risk classification is in helping to understand grey areas which s*hould taken into account if there is a risk for a minor’s well-being”*.

> “When supporting parents and/or adults who work with children, it will help us understand and communicate where children and young people are most certainly in need of some sort of help *or adult supervision.”*

> “There is definitely practical value in this classification, mostly for people who are *working with children. There is the need to put ‘a label on things’ so it is good that* we have clarifications of certain behaviours. When we have, for example, teachers, who are involved in children's everyday lives, they have to be familiar with the terminology (and not only the classification, but also elaborated meaning of it) so *they can react appropriately.”*

> *“We don’t have any official classif*ication especially since the boundary between the given threats can be quite fluid and unclear (but of course there are some classifications we use that are more less the same). The classification types may be slightly different depending on the target groups we are addressing it to (or aims). Of course, there are some main groups of content types that help to classify threats but it always needs to be clarified based on the context (e.g., sexting might be classified as *‘risky behaviours’ and ‘privacy’ or cyberbullying to ‘contact’ or ‘content’”)*

> *"We use the 3Cs in our parent sessions but do want to move towards a more* holistic approach. Many risks can be seen on one app, a video, a link etc. With parents we cover a broad range of issues but are seeking to simplify the advice. With young people, we tend to tackle issues. We choose those to fit the age of the *audience."*

Adapting current classifications

- Risk classifications need to be flexible in order to reflect the changing nature of online risk. Some dimensions of online risks are cross-cutting the issues (e.g., well-being), therefore it is helpful to acknowledge that their effects might be observed across the spectrum of risks. At the same time, there are many "hybrid threats" of overlapping risk aspects which makes such classifications difficult to apply in practice. A methodological explanation of where these "in-between" risks would fit would be useful.

- Classifications need to be both comprehensive and simple. There is a tension between trying to construct a comprehensive risk framework which captures all risk aspects and needing a simple way of communicating it to stakeholders like parents. A simple approach might be more useful for reaching out to stakeholders while a more complex or comprehensive approach might be helpful to experts and practitioners who already work in the area and are familiar with the issues.

- New conceptualisations of online risks need to pay greater attention to health and well-being aspects. While there has been a lot of discussion of screen time and excessive use, the existing typologies of risk are not explicit enough in their inclusion of health-related risks and well-being. These elements need to be incorporated better.

- 4 C for "contract": it was acknowledged that recognising the commercial environment is necessary but there was a debate on whether this should be a new dimension (4th C) or a cross-cutting category. "Contract" was preferred to "consumer" as a concept.

- 5th C for "consequences": risk classifications do not help to identify the consequences from online risk, they do not explain the harm that some children might experience or vulnerability. So, it is hard to understand the seriousness of risks from a risk classification. At the same time some risk classifications conflate risk and harm, which is very problematic. Illegal and harmful content is also different, so finding a way to represent the differences between the two is important. Emotional effects can also be added here.

- Applying such classifications requires awareness and training of practitioners to make sure the classifications are applied consistently. Including examples in the classification can also help to reduce confusion. A joint classification between Insafe and INHOPE can be helpful for streamlining the work.

- The classifications should reflect children's active role online in their terminology. Concepts like "consumer" are very passive and do not reflect children's engagement and agency. The classifications should also include risks based on children's own perceptions or risk and concerns (e.g., violations of their privacy, hacking attacks, financial fraud).

> *"The temptation is to keep adding and adding but one of the pur*poses of the classification that we find really helpful is using it in our session with parents. We try to help to break down all the things that they might be worried about into a way which is more understandable and gives them confidence in relation to some of

these issues. The temptation to broaden out the grid does harm the communication efforts that we want to make. There is a paradox of wanting it to be all-encompassing but at the same time to be effective for our communications around it.”

“There are many interdependencies and connected risks that you have an artificial divide if you try to have a more detailed classification.”

“The classification is interesting because it gives an idea about the incidents of risk, like a snapshot. But you cannot really understand risks into a broader context, it *doesn’t give an idea of how harmful certain risks are, only an idea of which risks are more common.”*

“Fears referring the future, the development of the Internet - when asked for their internet-related fears for the future, young people themselves quite often indicate the concern related to the increase of violations of the law: the number of hacking attacks, break-ins, theft of money and / or data, etc. (these cases will be increasing). Also they are afraid of censorship of public administration or the private sector. They are afraid of violations of their privacy and surveillance by foreign countries, government and business and advertisers. Another concern is related with the fear that in the future it will not be possible to use the Internet resources as freely as before, due to the additional fees imposed on services. They are afraid *of making all aspects of life dependent on the virtual sphere.”*

“Strengths of classifications are that every behaviour can be sorted into the ‘right’ group and acted upon accordingly. The problem is that sometimes there is a thin line between behaviours and in which category they are sorted, so it can be confusing sometimes, but if we elaborate them in a concise and simple way, maybe that problem can be avoided. The problem can also be - who is the one who will classify all those behaviours? If it is someone that has experience in the field, that *would probably be ok, but if it is someone who doesn’t have that experience, then we would have a problem.”*

“The classifications help to understand which risks are the most common ones (incidence), but they do not necessarily help to understand which of these risks are *the most serious ones (harmful) or what is causing such risks.”*

4. References

Broadband Commission for Sustainable Development (2019) Child Online Safety: Minimizing the Risk of Violence, Abuse and Exploitation Online. ITU & 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: White Paper for the ICT Coalition for Children Online. Brussels: ICT Coalition, https://www.ictcoalition.eu/medias/uploads/source/available%20here.pdf

Green, A., Wilkins, C. and Wyld, G. (2019) Keeping children safe online. Nominet, NPC and Parent Zone. https://www.thinknpc.org/wp-content/uploads/2019/07/Keeping-Children-Safe-Online-NPC-Nominet-ParentZone-2019.pdf

International Telecommunication Union (ITU) (2020) Child Online Protection (COP) Guidelines, https://www.itu-cop-guidelines.com/

Livingstone, S., Lievens, E. and 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

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

O'Neill, B. (2014b) Policy influences and country clusters: a comparative analysis of internet safety policy implementation. EU Kids Online, London, UK. http://eprints.lse.ac.uk/57247/

O'Neill, B. and Dinh, T. (2018) The Better Internet for Kids Policy Map Implementing the European Strategy for a Better Internet for Children in European Member States. https://www.betterinternetforkids.eu/documents/167024/2637346/BIK+Map+report+-+Final+-+March+2018/a858ae53-971f-4dce-829c-5a02af9287f7

Staksrud, E. and 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/

Stoilova, M., Livingstone, S. and Nandagiri, R. (2020) Digital by default: children's capacity to understand and manage online data and privacy. Media and Communication, 8 (4). 197-207. http://dx.doi.org/10.17645/mac.v8i4.3407

UNICEF (2017) State of the World's Children: Children in a Digital World. Available at: https://www.unicef.org/publications/index_101992.html