Submission for the preparation of the report by the UN Office of the High Commissioner for Human Rights on "Information and communication technology and child sexual exploitation"

October 2015

This submission has been jointly prepared by the Centre for Justice and Crime Prevention (CJCP)¹, Prof. Sonia Livingstone - Coordinator of EU Kids Online,² Data & Society Research Institute,³ Child Rights International Network (CRIN)⁴ and the International Child Redress Project (ICRP).⁵ It seeks to contribute a children’s rights perspective to existing discussions and policies concerning child sexual exploitation in relation to information and communication technologies (ICTs).

While existing efforts to protect children online are well-intended, in practice, they might inadvertently infringe upon children’s other rights. Responses to-date - both at a policy level and within the household - are largely based on perceptions of the dangers of the Internet, rather than the evidence.⁶ It is undoubtedly important to recognise the need for protection; but in devising responses to the risk of child sexual exploitation we must consider a) the range of other rights potentially undermined by exclusively protectionist policies, b) the evidence for specific risks of harm to particular groups, and then promote c) evidence-based interventions. Policies designed to address sexual exploitation in relation to ICTs should respect the full set of rights enshrined in the UN Convention on the Rights of the Child. Particular care is needed to ensure that any one right (e.g. protection from sexual exploitation) is not seen to automatically justify restrictions on other rights (e.g. right to privacy, to access information, and to freedom of expression). In the face of rights violations as a result of inappropriate protection policies, children should have access to justice.⁷

**Right to privacy**

Children’s right to privacy and protection from “arbitrary or unlawful” interference is set out in article 16 of the Convention on the Rights of the Child. Children are particularly vulnerable to breaches of their privacy because of the range of situations in which adults exert power over them. Often justified by a perceived need for protection, parents and technology companies increasingly surveil children’s

---

¹ CJPC works to develop, inform and promote evidence-based crime prevention practice, with a particular focus on children and youth [www.cjcp.org.za](http://www.cjcp.org.za) | [www.cjcp.org.za/contact.html](http://www.cjcp.org.za/contact.html)
² EU Kids Online is a multinational research network which seeks to enhance knowledge of European children's online opportunities, risks and safety [www.eukidsonline.net](http://www.eukidsonline.net) | [info@eukidsonline.de](mailto:info@eukidsonline.de)
³ Data & Society Research Institute is a think/do tank focused on social, cultural, and ethical issues arising from data-centric technological development [www.datasociety.net](http://www.datasociety.net) | [info@datasociety.net](mailto:info@datasociety.net)
⁴ CRIN is a rights-based NGO that advocates for the full realisation of all children's rights [www.crin.org](http://www.crin.org) | [info@crin.org](mailto:info@crin.org)
⁵ ICRP works to ensure that all child abuse victims have access to civil justice [www.internationalchildredressproject.com](http://www.internationalchildredressproject.com) | [Emma@internationalchildredressproject.com](mailto:Emma@internationalchildredressproject.com)
movements. Digital devices and applications enable collection and sharing of children’s personal information, often without their knowledge, and frequently beyond their control.

While such measures are used in the name of protection, blanket surveillance is based on general fears of the dangers of the Internet, rather than proven risks. It also demonstrates adults’ lack of confidence in children - as an entire generation - to make informed choices online. This approach to child protection has implications for children’s right to privacy, as it represents an intrusion into children’s private life and communications.

Case law on the issue is still evolving. A number of rulings have addressed the need to balance children’s right to privacy with their right to protection. In the context of combating the use of child sexual abuse images online, the European Court of Human Rights (ECHR) has said: “Although freedom of expression and confidentiality of communications are primary considerations [...] such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others.” Similarly, the Colombian Supreme Court ruled in August 2015 that parents who monitor their children’s online activity if they suspect abuse do not violate the children’s right to privacy. The decision was issued in relation to a case where the parents of a 12-year-old girl had accessed their daughter’s email account which documented sexual abuse of the girl. The Court made it clear, however, that any parental intervention that is not intended to protect the child would breach the child’s privacy and be “illegal and reprehensible”.

It is important for parents to be engaged in their children’s digital lives as early as possible; but the automatic response to risk should not be one of surveillance and restriction, as intrusion upon a child’s privacy can prove counterproductive because it can damage the child-to-adult relationship and, in the eyes of the child, remove the adult as a trusted source of help when needed. Instead, initiatives should aim to build child-to-adult trust through open communication and support.

Right to information
On the grounds of child protection, surveillance technology and Internet Service Providers (responding to government pressure) are filtering access to websites considered unsuitable for under-18s. But the reach of such filters extends far beyond websites containing, for example, adult sexual content, with many reports of blocks to other websites, including of education, health and charity organisations.

---

9 See, for example, “Are the Kids Alright? Digital Risks to Minors from South Korea’s Smart Sheriff Application.”Citizen Lab, University of Toronto Munk School of Global Affairs, September 2015. Available at: https://citizenlab.org/2015/09/digital-risks-south-korea-smart-sheriff/
12 Royal College of Psychiatrists, Managing self-harm in young people, October 2014. Available at: www.rcpsych.ac.uk/files/pdfversion/CR192.pdf
13 See, for example, the Blocked project, an online tool which monitors the extent of censorship caused by web filters www.blocked.org.uk/
While children should be protected, blanket filters inevitably have consequences for children’s access to information (CRC article 17), as well as their other rights, including to education (articles 28 and 29), health (article 24) and protection (article 19). For instance, laws banning the possession and distribution of vaguely defined ‘harmful information’ often restrict children’s access to websites about sexual health and relationships\textsuperscript{14} -- a subject which helps children to learn about healthy and consensual behaviour and become aware of that which verges on or amounts to abuse or exploitation.\textsuperscript{15} This information is essential for children to make safe and informed choices about interactions with other Internet users.

**Right to protection from abuse**

Because of the hidden nature of online child sexual exploitation and the unregulated setting where it takes place, policies to protect child users of ICTs from sexual exploitation should not merely be reactive. The aim should be to prevent the abuse before it takes place by building children’s capacity to protect themselves when using ICTs. This approach is in line with article 19 of the Convention on the Rights of the Child on the right to protection from abuse, which emphasises States’ obligation to implement, among other measures, educational initiatives to protect children from all forms of violence.

While many schools are opting for risk-averse strategies that limit or even ban children’s access to ICTs on school premises, and parents or guardians have been known to remove the technology from the child on the assumption that no access will remove the risk, simply restricting access (to either technology or sites and services) is not a sustainable or effective approach to protection. Education (on digital literacy and sex, health and relationships) is key in this respect, as children need information to protect themselves and to respond appropriately to risks that they may encounter online.\textsuperscript{16} This entails raising their awareness of potential risks so they are able to identify them, exercise critical judgement and make informed choices. Effective risk prevention depends in part on a child’s opportunities to develop resilience and practice digital citizenship.\textsuperscript{17}

But while awareness-raising and training should be available to adults in children’s lives (parents, legal guardians, teachers) so they know the risks and how to protect children, it should not be a substitute to education specifically for children. Notably, children largely seek assistance or knowledge from peers rather than parents, and there have been some positive evaluations of peer-based mentoring and support services.\textsuperscript{18} Education should be given to children in an age-appropriate and gender-specific way. Also effective are awareness-raising resources that encourage constructive and open dialogue between a child and a parent or legal guardian. ICTs and online technologies should also be examined as both a facilitator of child exploitation and, importantly, as a tool for protection. To this end, the UN Secretary-General’s Independent Expert Advisory Group on a Data Revolution for Sustainable

\textsuperscript{14} CRIN, “Censorship: Laws restricting children’s access to information”. Available at: \url{https://www.crin.org/en/node/39161}

\textsuperscript{15} Sex Education Forum, “Addressing healthy relationships and sexual exploitation within PSHE in schools,” October 2006. Available at: \url{www.sexeducationforum.org.uk/media/3101/pshe_ff37.pdf}

\textsuperscript{16} Livingstone, Sonia and Mason, Jessica (September 2015), *Sexual rights and sexual risks among youth online: A review of existing knowledge regarding children and young people’s developing sexuality in relation to new media environments*. Available at: \url{www.crin.org/sites/default/files/sexual_rights_and Sexual_risks_among_youth_online.pdf}

\textsuperscript{17} Digital Citizenship Institute, “Nine elements of digital citizenship.” Available at \url{www.digitalcitizenship.net/Nine_Elements.html}

\textsuperscript{18} Pew Research Center, “Where teens seek online privacy advice,” August 2013. Available at: \url{www.pewinternet.org/2013/08/15/main-findings-4/}
Development (IEAG) has called for new technologies to be utilised to support the UN Sustainable Development Goals, in which goal 16 promotes efforts to end violence and exploitation against children.

**From protection to criminalisation**
Laws designed to protect children from sexual exploitation are increasingly being used to criminalise children themselves, showing that law enforcement solutions can undermine some rights even as they seek to address others.

The phenomenon known as sexting, for example, is not uncommon among teenagers and is recognised as age-appropriate developmental behaviour. But the exchange of sexually explicit images, even if consensual, has resulted in children being prosecuted for sexual exploitation of a minor for possessing the images. Children have even been prosecuted for taking and storing explicit images of themselves, essentially being charged with exploiting themselves. Such charges can result in imprisonment and even being registered as a sex offender. Children have been placed on sex offender registries for years and even a lifetime for consensual sexual activity with another child, despite the negative impact this has on a child’s education and employment opportunities in later life.

There have been instances where the blanket application of sex offender laws, even against children, have been successfully challenged. Until recently in South Africa, for example, child protection legislation dictated that consensual sexting between teenagers would automatically result in both parties being placed on the sexual offences register. But in the face of several Constitutional Court challenges this provision has now been ruled unconstitutional and is under review.

**Access to justice**
Where children experience violations of their human rights, including sexual exploitation, they must have access to justice. The Committee on the Rights of the Child has said that “for rights to have meaning, effective remedies must be available to redress violations”. States must therefore “ensur[e] that there are effective, child-sensitive procedures available to children and their representatives”. This means ensuring that children have meaningful access to the judicial system - including “access to a readily available, prompt and effective remedy in the form of criminal, civil, administrative or disciplinary proceedings” - and any other independent complaints procedures.

---

19 IEAG (November 2014), *A World That Counts: Mobilising The Data Revolution for Sustainable Development*. Available at: www.undaterevolution.org/report/
25 Ibid
Moreover, article 12 of the CRC grants children the right to be heard in any judicial and administrative proceedings affecting them either directly or through a representative. The Committee recommends that children be given the opportunity to be directly heard in any proceedings that affect them.

RECOMMENDATIONS

We urge the UN Office of the High Commissioner for Human Rights to address the following issues in its report by:

Evidence-based policy
- urging States to build national child protection policies based on evidence and data;
- urging States to conduct further research to inform policy development and implementation, especially on areas lacking in data, such as the implications of technology companies storing information of children’s online activities;
- informing States of the importance of building child-to-adult trust through open communication and support, rather than monitoring children’s activities;
- urging the Special Rapporteur on the right to privacy to undertake a study into children’s right to privacy;
- urging States to develop policies through a process that is accountable to and builds on effective consultation with children themselves and their advocates.

Education and training
- emphasising to States the need to deliver digital literacy and safety skills to children as part of basic education by promoting critical engagement with online resources through age-appropriate materials;
- recommending to States they make education on sex and relationships a mandatory part of the school curriculum to empower children to recognise relationships based on respect and consent;
- urging States they ensure children have a trusted and confidential means of reporting, either to parents or guardians, teachers or peers, if they encounter materials or interactions that upset them.

Access to justice
- recommending to States they ensure children’s access to justice, including compensation, for all forms of sexual exploitation, as well as for rights violations resulting from inappropriate protection policies;
- encouraging States to remove unduly restrictive limitation periods imposed on survivors who wish to bring claims against adults who abused them during their childhood;
- urging States to inform children and parents or guardians of the mechanisms and avenues (ICT platforms, courts, etc) available to report actual or suspected abuse.