CRIN's submission for OHCHR's report on the right to privacy in the digital age

This submission was made on behalf of the Child Rights International Network - CRIN (www.crin.org) on 9 April 2018.

This submission focuses on children's right to privacy in the digital environment. However, the right to privacy in this context cannot be seen in isolation. The right to privacy overlaps with children's right to free expression, to access information the cross-cutting rights provisions within the Convention on the Rights of the Child. The overlap and relationship between these connected rights is key to the full realisation of children's rights in the digital age.

Undue interference with children's right to privacy in the digital age

As transactions and interactions move online, users are increasingly monitored and tracked as they buy, talk and browse. This is a reality for children as well as adults, with undeniable impact on the right to privacy, but there are a number of child-specific concerns and rights issues in this context.

No child may be subjected to arbitrary or unlawful interference with his or her privacy, a right protected in almost identical terms under the Convention on the Rights of the Child (CRC) and the International Covenant on Civil and Political Rights (ICCPR)[1] ensuring that the right to privacy is guaranteed regardless of age. However, the mutually supportive nature of children's right under the CRC impacts the way the right must be interpreted and applied. This section will address privacy concerns related to the collection and use of children's data, as well as the connection between children's other rights in this context.

Consent, minimum ages and children's privacy

Informed consent is among the core grounds for the collection and processing of a person's data online.[2] When used as a basis for the collection and processing of children's information, it empowers children to decide and understand how their privacy is affected by the online collection and use of their personal information. To be meaningful, however, it must be freely given, specific, informed and unambiguous requiring a clear action authorising the use of personal information.[3]

Where children lack capacity to make these decisions for themselves, however, their consent cannot be the basis for making these decisions. The setting of a minimum age of digital consent - an age at which children sign up to and use digital services - is, therefore, becoming a common feature of national law. The EU's General Data Protection Regulation will require all EU Member States to set this age at between 13 and 16 years by the time the

[1] Convention on the Rights of the Child, Article 16; International Covenant on Civil and Political Rights, Article 17.
[2] The soon to be implemented General Data Protection Regulation (GDPR) applicable across all EU Member States identifies six bases for lawfully processing personal data, namely consent, contract, legal obligation, vital interests, public tasks and legitimate interests.
[3] This standard is set out within the EU GDPR, Recital 32.

regulation enters into force in May 2018 and many have already done so.[4] In the United States, this age is similarly set at 13.[5]

While not itself an issue of privacy, the setting of this minimum age has privacy implications. Legal provisions permitting only children over a certain age to access services means that online providers of services must collect and process the personal data of children in order to determine their age, perhaps including information vulnerable to misuse, such as copies of official identification documents. It has also become common for online service providers to rely on each other to provide age verification, for example by requiring a user to sign in using a Facebook account or other service that requires that users be over a certain age. The sharing of information across disparate services in conjunction with highly technical terms of service risks the spreading of, and in practice has commonly spread, personal information between companies without the fully informed consent of the children affected.

Recommendation:

- Terms of service must be written in clear language understandable to children in order to ensure children are able to give informed consent and understand how their data is being collected and shared;
- To ensure the privacy of children, where age determination is necessary, the data collected must be the minimum necessary to fulfil this function and the information collected should not be used for any other purpose without separate consent;
- Children must be able to withdraw their consent and have their personal information deleted on request.

Collection and use of children's data

Children's data is collected, legitimately and illegitimately, across all areas of their lives, whether at home, at school or in the community. In many countries, there is a chronic lack of transparency about who is holding children's data and on what legal basis. Clarity about this issue is fundamental in assessing whether interference with the right to privacy is arbitrary or unlawful.

Filters, controls and monitoring

Particularly within the home and schools, the use of restrictions and monitoring of children's internet use is common and raises serious privacy concerns. Where, for example, a parent installs software on a child's computer or phone that reports where a child is, what online material they are accessing or requires parental consent to access certain materials the use of this software engages the child's right to privacy.

[4] See Better Internet for Kids: https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=2019355.
[5] Children's Online Privacy Protection Act. Available at: http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim.

The Committee on the Rights of the Child has not comprehensively addressed this issue, but the provisions of the Convention have a clear application in this setting. The Convention provides that parents have an obligation to provide direction and guidance to children's exercise of their rights in a manner consistent with the evolving capacities of the child.[6] The Committee has expanded on the meaning of this provision, finding that "Article 5 contains the principle that parents (and others) have the responsibility to continually adjust the levels of support and guidance they offer to a child. These adjustments take account of a child's interests and wishes as well as the child's capacities for autonomous decision-making and comprehension of his or her best interests."[7]

The application of these standards is particularly important in situations where laws or tools prevent children accessing, or reports children's attempts to access, information online that can support them to make informed choices, including honest, objective and age-appropriate information about issues such as sex education and drug use.

At the most invasive and discriminatory level, laws prohibiting the "promotion of homosexuality to children", particularly across Eastern Europe, have persecuted LGBTQ children and prevented them accessing information to which they have a right.[8] At a less severe, but also concerning level, filters that prevent children accessing age appropriate information about sexuality, health issues or drug use without asking for parental approval can prevent them accessing information that makes them safer. If children do not have a supportive home life or are simply not ready or willing to discuss these issues with their parents, teachers or other members of their community, these filters can prevent children accessing information to which they have a right. As noted by the Special Rapporteur on freedom of expression has noted, these kinds of restrictions may exacerbate rather than diminish children's vulnerability to risks.[9]

Evidence also indicates that informed and actively engaged parents who discuss the internet and their experience with their children are the strongest protective measures for ensuring a safer online experience.[10]

Recommendations and best practice:

- Children's use of digital tools should never be monitored without their knowledge;
- In the context of children's access to online materials and the appropriateness of monitoring, parents and caregivers may play a more active role in deciding the scope and nature of the information and content that younger children access, but this must give way as children mature and their capacities evolve to make these decisions for themselves.

---

[6] Convention on the Rights of the Child, Article 5.
[7] Committee on the Rights of the Child, General Comment No. 7 (2005), CRC/C/GC/7Rev.1, para. 17.
[8] CRIN, Censorship: Laws restricting access to information. Available at: www.crin.org/node/39161.
[9] See *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/69/335, 21 August 2014, para. 49.
[10] See *eport of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/69/335, 21 August 2014, paras. 71 to 74; Livingston and Bulger, "A global agenda for children's rights in the digital age" recommendations for developing UNICEF's research strategy" September 2013.

"Anti-radicalisation" measures

Where the monitoring of children as well as the collection and sharing of their personal information takes place in the context of "anti-radicalisation" or "anti-extremism" policies, it also engages further protection based arguments and children's rights concerns. The United Kingdom is used here as an example to highlight related privacy concerns, though its use of "anti-radicalisation" programmes for children is not unique.

Since 2015 in the United Kingdom, professionals working with children have had a legal duty to "identify children at risk" of being drawn into terrorism and "intervene as appropriate".[11] One of the means of response is referring children deemed to be at risk to be referred to what is called the Channel programme, which screens individuals referred to it and and, where it considers appropriate, intervenes to prevent the individual being drawn into terrorism. While the intention may be laudable - to identify children at risk of being recruited by terrorist groups and intervene to protect them - the implementation and impact has been widely criticised as counter-productive, discriminatory and a violation of the rights of children.[12]

To address the privacy related issues directly, the programme requires the collection and sharing of sensitive personal data between a diverse range of agencies. Schools initially assess the risk of children being drawn into terrorism, the information schools collect may be passed onto a specialist police officer who in turn can request more information about a child from the full range of professionals working with them.[13]

CRIN has used freedom of information requests in an attempt to find out the ways that schools are using filtering and monitoring programs to detect signs of "radicalisation" in students. We submitted 61 requests to schools across a London Borough[14] to ask what filtering and monitoring programs were installed on school ICT equipment for the purposes of detecting signs of "radicalisation", information about how the software worked and how many students had been flagged up by the software. None of the schools provided detailed information and a common response was that their filtering software was operated by a public-private partnership that is not subject to the Freedom of Information Act.

Without a clear picture of what information schools, or private companies working on behalf of schools, are collecting and where it is held, it is impossible to assess the adequacy of mechanisms to protect the data of children. The outsourcing of services to the private sector

[11] Counter-Terrorism and Security Act 2015, Section 26(1) and Schedule 6; HM Government, *Revised Prevent Duty Guidance,* July 2015, p. 11.
[12] See, for example, *Report of the Special Rapporteur on the rights to freedom of peaceful and assembly on his follow-up mission to the United Kingdom*, A/HRC/35/28/Add.1, 24 May 2017, paras. 6 to 14; Rights Watch UK, *Preventing Education? Human rights and the UK counter terrorism policy in schools*, 2016.
[13] For fuller details on the Prevent and Channel programmes, see HM Government, *Prevent Strategy*; HM Government, *Revised Prevent Duty Guidance*, July 2015; HM Government, *Channel Duty Guidance.*
[14] Requests submitted have been retained on file.

has also extended the number of bodies holding children's data, while limiting the potential for independent scrutiny.

Statistics on who is being targeted by these measures also raises concerns about potential discriminatory application of these rules that may violate the requirement that interference with the right to privacy is not arbitrary. Between March 2014 and March 2016, 3,105 people under the age of 18 were referred to Channel across England and Wales - accounting for 48 percent of all referrals during the period.[15] Among these children, certain minority religious and ethnic groups have been disproportionately targeted by these measures. Nearly 40 percent of the children referred to Channel were recorded as Muslim in the figures[16] and more than a quarter were recorded as being ethnically Asian.[17] More recent figures have grouped children aged 15 to 20, making it difficult to assess how children in particular are affected by the measures.

Commercial collection and use of children's data

In the commercial setting, the collection and processing of data to target children as consumers also raises privacy and protection controls.

The Committee on the Rights of the Child has not addressed online advertising in depth, but has set out the implications of the CRC with regards to commercial advertising more broadly. The Convention requires States to encourage the development of appropriate guidelines for the protection of the child from information and materials injurious to his or her well-being.[18] Applying this provision to advertising, the Committee has recognised that children are vulnerable in this context and may regard marketing and advertising as truthful and unbiased. In this vein, the Committee has recommended that "States should ensure that marketing and advertising do not have adverse impacts on children's rights by adopting appropriate regulation and encouraging business enterprises to adhere to codes of conduct and use clear and accurate product labelling and information that allow parents and children to make informed consumer decisions."[19]

In the context of online advertising, the standards on the advertising to children further overlap with the right to privacy, in that targeted advertising is based on the collection of personal data. As noted above, reliance on consent for the collection of processing data for children shows the greatest respect for children's right to privacy.

Recommendations and best practice:

[15] Figures compiled from freedom of information requests and held on record.
[16] Breakdown by religion: Muslim (38.5%); Christian (4.7%); Sikh (0.26%); Jewish (0.2%); Buddhist (0.1%); Hindu (0.1%); none (1.1%); other (0.3%); not known (11.2%).
[17] Breakdown by ethnicity: Asian 37.7%); White (33.0%); Black (5.3%); Mixed (4.0%); Chinese (0.2%); other (7.2%); unknown (11.6%).
[18] Convention on the Rights of the Child, Article 17(e).
[19] Committee on the Rights of the Child, General Comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights, CRC/C/GC/16, 17 April 2013, para. 59.

- The collection and processing of children's data for the purposes of advertising must be based on the child's consent and the personal information of children who do not have the capacity to consent should never be collected or used;
- Children's data must not be shared without their explicit and informed consent;
- Children's personal information should not be sold on for profit;
- Advertising and commercial messages, particularly those targeted at children, should be clearly identified;
- The "profiling" of children, whereby their data is automatically processed and a profile applied to make decisions about the child or to analyse or predict preference, behaviour or attitudes, should be prohibited by law.

Digital literacy

As it is increasingly difficult for children, as well as adults, to establish how personal data is being collected processed, shared and monetised online, digital literacy has become key to ensuring that children are equipped with the skills necessary to enjoy their privacy. To effectively protect children, this education must include how children can use technological tools, how children's information is collected and used online and how children can protect themselves from the improper use of their information.

Recommendations:

- Digital literacy education should be a core part of the education curriculum from the earliest years, including on how children can protect their privacy online;
- States should not prohibit in law or practice anonymity, pseudonymity or the usage of encryption technologies by children and children should be taught how to understand and use these tools.

Safeguards and remedies

Access to justice is a fundamental right in itself and a prerequisite for the protection and promotion of all other human rights.[20] For this right to be meaningful for children, they must be able to file complaints that cover the full scope of their privacy rights, and complaint procedures must be transparent and tailored to meet the needs of children. In particular, for these complaint procedures to be meaningful and effective, they must allow children and/or their parents, carers or legal representatives to have personal information corrected or deleted and for content to be removed where it is unjustly damaging to reputation.

Recommendations and best practice:

- Simple and easily accessible complaint mechanisms must be established to allow children to request the information held about them and that it be corrected or deleted;
- Effective appeal processes must be in place to challenge the failure to provide children these remedies, including access to the courts where a legal right has been violated.

[20] OHCHR, *Report of the United Nations High Commissioner for Human Rights on access to justice for children*, A/HRC/25/35, 16 December 2013, para. 3.