

**SPECIAL RAPPORTEUR ON THE RIGHT TO PRIVACY**

**Joseph A. Cannataci**

**BACKGROUND**

**1. Work of the Special Rapporteur on the right to privacy upon children:**

The Special Rapporteur (SRP) released a Call for Contributions for the examination of how privacy affects the development of personality, particularly the evolving capacity of the child and the growth of autonomy. Contributions were sought from interested parties on relevant research; consultations with children, and mechanisms, laws, policies or programs seen as examples of good practice.

The SRP will report to the Human Rights Council in March 2021 on the issues identified together with preliminary options and recommendations to address these.

More information on the SRP’s privacy and children work is available at: <https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2020_July_SRP_Call_for_Submissions_and_Note.pdf>

**2. Approach to Privacy:**

Privacy is critical to the development of personality. Without the conditions of a private life and private spaces, the full potential of the individual and her/his fundamental right to human dignity are compromised.

The concept of privacy is related to bodily and mental integrity; decisional autonomy; personal identity and includes informational privacy; and physical/spatial components of privacy.

Privacy facilitates the enjoyment of other rights such as the right to freedom of expression of assembly, of association, of faith and of health amongst others.[[1]](#footnote-1)

The SRP emphasises the positive, facilitative aspect of the right to privacy that goes to the innate dignity of the person. The importance of privacy to human dignity underlies the need for its protection.

The term ‘unhindered development of personality’ is used to refer to the full development of the person’s potential to participate constructively in their society, and self-determination, that is, the power of the individual to decide whether and to what extent to disclose aspects of their personal life.[[2]](#footnote-2)

**3. SRP’s approach to Child’s Right to Privacy (Article 16):**

The Article must be interpreted broadly and generously to accommodate the full range of children’s privacy experiences, and, all components of privacy, including the interdependency with other human rights.

Children’s right to privacy enables their access to other rights critical to developing personality and personhood such as rights to information, to freedom of expression, association, and to health amongst others.

In terms of the four key principles which provide a lens through which implementation of all other rights under the Convention should be viewed, the work of the SRP Mandate has established;

1. privacy’s capacity to prevent discrimination and associated stigmatisation (Art. 2);
2. protecting privacy secures the best interests of the child (Art. 3), and their right to heard (Art. 12);
3. privacy’s nurturing of personality enables survival and development (Art. 6), and
4. supports evolving capacity (Art. 5).

**SPECIFIC COMMENTS**

**III. General Principles**

**IV. Evolving capacities (Art. 5)**

The draft General Comments relies in a number of areas, primarily in points 50; 52; 56; 102; 104 and 105 on the concept of ‘age-appropriate’. It is important to look closely at this term as it is increasingly used, and its relationship to evolving capacity.

The term ‘age appropriate’ generally is accepted as an alignment between chronological age and behaviours, and an acceptable alignment of chronological age with what is available to the child, such as online content. ‘Age appropriate’ in the regulatory sense is a standard against which online providers are held for services suitable to the child’s age. The UK Age Appropriate Design Code is a thoughtful example of this approach.[[3]](#footnote-3)

The mechanism of ‘age appropriate’ is not a ‘cure all’. Material may still be ‘age appropriate’ and harmful to the child and their human rights. It can protect a child when customised to that individual, but may not meet the needs of a cohort of children given the considerable variation in the intellectual and emotional development amongst children of the same age.[[4]](#footnote-4) As a generic threshold, which is how it is used, ‘age appropriate’ poses inequities for children of differing levels of capacity.

In the SRP’s view ‘age appropriate’ is a crude measure of the child’s evolving capacity, and can constrain development of their personality, the autonomous exercise of their rights, and possibly be discriminatory. As such therefore, use of such a blunt instrument must be adopted with the greatest of caution and only when no better means exists.

The child’s readiness for decision-making and self-responsibility is best determined not by chronological age alone but by the context including the risks and support available, individual experience, the rights affected, and their capacity for understanding the implications of their actions (or non-actions). Determining when a child is capable, for example, of consenting to the processing of their personal data, must consider their ‘actual understanding’ of the data processing, their best interests, rights and views.

Also, in relation to the reference to ‘age verification’ in point 122, when age is the criteria for accessing a service, verifiable identity documents are required. Requiring more data to ‘protect’ children raises concerns around data security, risks of prescriptive approaches and the lack of age assurance standards, tools and industry certification schemes.

In essence, the notion of ‘age appropriate’ contradicts the reality of ‘evolving capacity’ where this depends greatly on the individual child and all the variables mentioned above and more.

It is more consistent to be urging States and digital providers to offer or make available services to children appropriate for their evolving capacities.

It is recommended that:

1. Support be given for comprehensive analyses of children’s capacity for autonomous decision-making for accessing online and other services, for evidence-based child specific privacy laws and regulations

**V. General measures of implementation by States (Art. 4)**

Traditionally, the rights of children have been regarded as an issue for adults to determine. Children’s needs, however, differ from and can conflict with those of adults.

The need for policies and regulation based on child-centred research and comprehensive realistic assessment of the risks to children including their privacy, is evident from recent research indicating that adults who had *not* experienced online harms, such as violent threats or trolling, were more likely to want to restrict online information access and anonymity.[[5]](#footnote-5)

Pt 23 To bring together the various points of this section it would be useful to be clarify that “broad range of legislative, administrative and other measures…” is underpinned by the rights and values of the Convention on the Rights of the Child from legislation, policies, management decisions, services, through to resource allocation.

**A. Legislation**

To ensure laws protect children without restricting their human rights including privacy, States, legislative processes and legislation need to:

1. incorporate children’s views, findings of child-focused research and/or child privacy impact assessments;
2. encourage technological innovations that may improve information communication services while protecting children’s privacy;
3. incorporate conceptions of privacy that prepare children and young people for their futures;
4. enable children to develop and exercise their own strategies for privacy;
5. provide independent means to conciliate, arbitrate, and remedy individual or systemic human rights violations against children;
6. provide remedies, and enforcement of infringements.

**Administrative processes**

It is recommended that administrative processes in the section ‘General measures of implementation by States’ is not neglected.

Specifically, records and record keeping systems underpin Government processes, decision-making and service delivery. Children rarely have agency in regard to their records. The privacy of these increasingly digitalized records is also an issue.

It is recommended there be inclusion of a point along the lines:

“State and member bodies shall require the design and implementation of rights-based recordkeeping systems to support the human rights of all children, but particularly those in alternative care and forced migration environments, to provide agency to the child to access these records, and to enable accountability to the child for all deliberations and decisions impacting on the well-being of a child.”

**I. The business sector - J. Commercial advertising and marketing**

Pt 36 It is suggested that reference be made to the UN Guiding Principles on Business and Human Rights: Implementing the United Nations “Protect, Respect and Remedy Framework”, and the “Gender guidance for the Guiding Principles on Business and Human Rights” within the United Nations official document (A/HRC/41/43). The links are:

<https://www.ohchr.org/Documents/Issues/Business/Intro_Guiding_PrinciplesBusinessHR.pdf>

<https://www.ohchr.org/Documents/Issues/Business/Gender_Booklet_Final.pdf>

**VI. Civil rights and freedoms**

**A. Access to information (Arts. 13, 17)**

Strong support is given to the draft General Comments recognition of the importance of encryption and anonymity for children. For many children, being anonymous enables them to be secure while they obtain information crucial to forming independent opinion and views, and to further their education.

**B. Freedom of expression (Art. 13)**

It is recommended to include:

anonymity, pseudonymity or the use of encryption technologies by children should not be prohibited, in law or practice.

**E. Right to privacy (Art. 16)**

Strong support is given to the elaboration of the actions required by States and others, to meet their obligations to promote and protect children’s rights in and through the digital environment. It is critical that States ensure children are not subjected to arbitrary or unlawful interference with their privacy in the digital environment.

The matters raised in Section E. largely if not solely, relate to informational privacy, and consequently address data protection. It is important to emphasise more strongly the importance of the right of privacy to developing personality. The material provided below seeks the inclusion of material on the broader scope of privacy as it relates to children.

It is recommended that:

clearer and stronger statements are made to the effect that in the digital age, it is essential that States and business enterprises recognise that promotion of the child’s right to privacy:

1. prevents discrimination and stigmatisation (Art. 2);
2. secures the best interests of the child (Art. 3);
3. protects their right to heard (Art. 12);
4. enables survival and development (Art. 6) and
5. supports evolving capacity (Art. 5) .

This is necessary as adult interpretation of children’s privacy needs can result in children’s privacy restricted in the name of ‘protection’.

Adult reliance on surveillance to protect children is a case in point. Parental surveillance increases rather than decreases with a child’s age, that is, when young people are (or should be) becoming more independent. Parents and carers of children with additional needs, favour even more protective stances.

On surveillance, it is recommended it is necessary to mention the deleterious effect of surveillance (educational; commercial; parental and that of the State as part of counter terrorism and/or child sexual exploitation responses) upon children’s ability to exercise their rights.

It is recommended that the guidance under Art. 16 recognises that sexual expression, bodily integrity and physical autonomy are part of the interwoven fabric of children’s right to development of personality to which privacy serves as a gateway or pathway right, an enabling right which facilitates, indeed makes it possible for the child to evolve in as free and independent manner as nature and nurture may allow. Adolescents need to be able to make decisions regarding their well-being and bodies, and to safely and privately explore their sexuality as part of their developing maturity. There is a need to address occurrences where the bodily integrity and autonomy rights of children are infringed by the actions of Governments, commercial entities, health care and other professionals, parents, and peers.

The SRP’s recommendation on privacy and gender and bodily integrity issues directly relevant to children are set out in the mandate’s ‘Recommendations for protecting against gender based privacy infringements’ ([A/HRC/43/52](https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session43/Documents/A_HRC_43_52_AdvanceUneditedVersion.docx)).

Infringements of bodily privacy impact other rights, for example:

1. mandatory pregnancy testing infringes girls’ rights to dignity, equality, and autonomy;
2. “voluntary” virginity testing, often imposed or otherwise insisted upon by parents also infringes girls’ rights to dignity, equality, and autonomy
3. surveying students to identify those with different sexual orientations and gender identities, violate the right to non-discrimination, and when applied to expel students, breach their right to education;
4. Highly medicalised processes entailing surgery to access legal gender recognition, implicate the right to health.

Therefore, it is important to acknowledge and address this issue in section E.

The free development of personality requires that the individual is protected against the unlimited collection, storage, use and sharing of personal data.[[6]](#footnote-6) In the case of children, their personality and autonomy can be nurtured by minimising their digital footprints.

Governments must establish frameworks that allow innovation around tools and mechanisms addressing children’s privacy. New technologies can advance the purpose of (often outdated) laws and regulations. Privacy engineering is needed as a counter to “persuasive design”.There is much more scope to work in partnership across governments, civil society, industry and children to co-build as prototypes, privacy- promoting online experiences for children.

It is recommended that:

1. States actively encourage proactive privacy engineering approaches to maximise children’s positive online experiences including through establishment of research grants or other mechanisms;
2. In a conflict between a commercial use and the right to privacy of a child, the primary consideration is the best interest of the child to enjoy their rights without being exposed to commercial practices which are likely to impair their development and autonomy.

In terms of data protection, the other matters addressed are supported.

**F. Birth registration and right to identity (Arts. 7, 8)**

Records and record keeping systems underpin official identity and are increasingly digital. The lack of legal recognition affects children’s access to many rights necessary for autonomy, such as education.

It is recommended that reference be made specifically to the difficulties facing transgender and intersex children to obtain whether offline or online, official records that accord with their self-determined gender identity. Birth and other official records of identity can become barriers to accessing services from both public and private sectors such as education, as well as undermining their fundamental human rights to dignity, identity (Art. 8), privacy (Art. 16) and development (Art. 6). States need to address and remove these barriers for this group of children.

It is recommended that this section also acknowledges that the identity of the child includes gender identity, and the specific link to official records such as birth registration for the child and also their parents when the parents are gender diverse, and, that all records and registration systems, including those online, need to address this from an inclusive approach ([A/HRC/43/52](https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session43/Documents/A_HRC_43_52_AdvanceUneditedVersion.docx)).

One’s biological parents are an important dimension of identity and record-keeping and access policies should be such so as to enable a child to eventually establish the identity of their biological parents irrespective of whether insemination was natural, assisted or artificial.

**VII Violence against children**

Pt 87 Concomitant to urging States to “ensure business enterprises meet their responsibility to effectively protect children from all forms of violence…..in the digital environment”, it is incumbent upon States to provide the legal environment within which business enterprises can do this.

Currently, in some parts of the world, there is concern that the legal frameworks do not enable voluntary action by companies to detect online child sexual abuse material.

It is recommended that this issue be considered for inclusion.

Also recommended for inclusion, is a statement to the effect that “Effectively and comprehensively combating ICT facilitated child abuse and exploitation for example, requires a multi-stakeholder approach, actively involving children, families, communities, governments, civil society and the private sector.”

**VIII. Family environment and alternative care (Arts. 5, 9, 18, 20)**

Defining children only by their vulnerability without consideration of their potential or capacity, is likely to result in adults adopting overly protectionist agendas, potentially harmful to children’s personality. Parental controls also must be proportionate and aligned with the child’s evolving capacities, and children’s views sought.

The recognition in the draft General Comment of the complex factors and dynamics in this environment, including that parents may not always act in the child’s best interests is supported.

**IX. Basic health and welfare (art. 24)**

The statements concerning the need for accessible sexual reproductive health services for children is strongly supported, as are statements concerning the need for sexual education. For some children, the internet can provide safer places for children to understand their gender identity and sexuality than the family home, school or faith institutions.

The SRP has made detailed and comprehensive recommendations regarding sexuality, gender, bodily integrity and physical autonomy issues directly related to children in the digital world ‘Recommendations for protecting against gender based privacy infringements’. These are available at ([A/HRC/43/52](https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session43/Documents/A_HRC_43_52_AdvanceUneditedVersion.docx)).

**XI. Education, leisure and cultural activities**

**A. The right to education (Arts. 28, 29)**

The purpose of education is to develop the child’s personality, talents, and mental and physical abilities to their fullest potential.[[7]](#footnote-7) Schools play a large part in how a child experiences life and privacy on a day to day basis.

The right to education requires States to respect, protect and fulfil by removing barriers to education such as gender bans and bullying.[[8]](#footnote-8) Violent and exclusionary practices do not meet the requirements of article 29(1).

To facilitate the shift to online education due to the pandemic, several governments waived existing child data privacy laws. In Wales, the government waived the requirement for parents’ and students’ consent for example. In some countries, there is no protection for children’s right to privacy in government schools.[[9]](#footnote-9)

At the same time, in September 2020, an analysis of 496 EdTech apps across 22 countries foundmany were collecting device identifiers;27 apps were taking location data; 79 out of 123 manually tested apps were sharing user data with third parties such as advertising partners.[[10]](#footnote-10)

Ensuring that children’s privacy and autonomy rights flourish requires a child centred, human rights-based approach that moves beyond data protection models based on ‘consent’ for data collection and use.

It is recommended:

1. a child’ right to protection of their personal information and data should not be waived or reduced in order to facilitate online education,
2. the enjoyment of privacy and other rights should be reinforced not undermined by the educational process wherever or however it occurs.[[11]](#footnote-11)
3. require EdTech companies to protect children’s privacy in the design, operation and data processing, and enable data erasure and opting out of data collection.

The statements concerning digital literacy at pts 33, 89, 113 and 114 are strongly supported. The UN General Assembly recently has encouraged States to invest in digital literacy and regulations that ensure children’s privacy, data protection and safety online[[12]](#footnote-12), and children and youth agree that digital literacy education enables them to control their privacy and develop autonomy.

It is recommended that:

1. as education is for the full development of the child’s potential, and that so much of this development now occurs online, it is appropriate that digital literacy is properly established within schools without delay.
2. early digital literacy/citizenship education is needed given the increasingly younger ages children go online and the inability of many parents to offer effective support or intervention.
3. digital literacy education involving children, adolescents and parents in information about safety online, respectful relationships and human rights, can prevent harmful online behaviour at its source.[[13]](#footnote-13)

**XII Special Protection measures**

**B. Administration of child justice (Art. 40)**

It is recommended that States ensure:

1. any linking of civil and criminal identity databases is preceded by a privacy and human rights impact assessment, and wide consultation to assess the necessity, proportionality, and legality of biometric surveillance infrastructure and its implications for children and their privacy;
2. information provided to, and by, the media does not violate children’s right to privacy, and that reporting by media and other bodies protects the privacy rights of children of parents in conflict with the law.
3. Subject to reasonable and proportional measures in cases where probable cause for creation of risk exists, children’s privacy is upheld in all contacts with incarcerated parents, including written, electronic and telephone communications, and prison visits.
4. biometric data is not collected from children unless as an exceptional measure, and lawful, necessary, proportionate and fully in line with the rights of the child.
1. General Assembly resolution 68/167, A/HRC/13/37; Human Rights Council resolution 20/8). [↑](#footnote-ref-1)
2. Abstract of the German Federal Constitutional Court’s Judgment of 15 December 1983, 1 BvR 209, 269, 362, 420, 440, 484/83 [CODICES] [↑](#footnote-ref-2)
3. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/01/ico-publishes-code-of-practice-to-protect-children-s-privacy-online/ [↑](#footnote-ref-3)
4. CRC GC 7 [↑](#footnote-ref-4)
5. DEMOS 20 October 2020 at: <https://demos.co.uk/blog/online-harms-a-snapshot-of-public-opinion/> viewed 18 November 2020. [↑](#footnote-ref-5)
6. Abstract of the German Federal Constitutional Court’s Judgment of 15 December 1983, 1 BvR 209, 269, 362, 420, 440, 484/83 [CODICES] [↑](#footnote-ref-6)
7. CRC Article 29(1)(a) [↑](#footnote-ref-7)
8. A/C.3/75/L.16/Rev.1 [↑](#footnote-ref-8)
9. The States of Western and South Australia in Australia are examples. [↑](#footnote-ref-9)
10. International Digital Accountability Council CNET September 2020. [↑](#footnote-ref-10)
11. CRC General Comment No. 1 2001; A/C.3/75/L.16/Rev.1 [↑](#footnote-ref-11)
12. A.C.3/75/L.16/Rev.1 [↑](#footnote-ref-12)
13. Bailey & Steeves, 2015; Bailey & Burkell, 2020 [↑](#footnote-ref-13)