Submission to the consultation on the Draft General Comment 25 on children’s rights in relation to the digital environment

Dear drafters,

We warmly welcome the draft General comment on children’s rights in relation to the digital environment. This General Comment is timely and much needed. We are particularly delighted with the attention for a balance between protection and autonomy, for children’s rights impact assessments (both for legislators and private actors), for data collection and research, for involving children in policy-making and design of products and services, for challenges raised by the deployment and use of Artificial Intelligence and automated decision-making and their impact on children’s rights to non-discrimination, freedom of expression, freedom of thought and privacy and for data protection related concerns.

Below we provide a number of suggestions with regard to other aspects of the draft GC.

1. Definitions and notions

Although the definition that is provided of ‘the digital environment’ in para. 2 is very comprehensive, we feel that it would be helpful to emphasise that the environment in which children grow up is a physical, non-digital environment in which digital technologies are increasingly present and affect children in a variety of ways, because their interactions are mediated by digital technologies (including connected toys or other connected artefacts) and because digital technologies steer their online and offline behaviour (e.g. through persuasive or manipulative design).

Furthermore, in the draft comment, certain notions are used with which not all readers might be familiar, and which require a brief explanation. The notion ‘data minimization’ — used in para. 56 — is a good example.

1. Precautionary approach

The mention of the precautionary approach (para. 17 and 23) is very interesting in relation to children and children’s rights and might deserve more attention in the general comment. Originally a principle of environmental law, scholars have started seeing the importance of this approach as a counterbalance to permissionless innovation. One could argue that banning profiling aimed at children (unless it is in their best interest) could be a manifestation of the precautionary approach because the underlying reason for such a ban is that we are insufficiently aware of the (long-term) impact and consequences of profiling on children. Furthermore, the precautionary approach also has a relationship with impact assessments (child rights impact assessments - CRIAs, data protection impact assessments - DPIAs) as these relate to the identification and mitigation of risks, as well as ‘by design’ solutions to implement values and rights into the design of apps and online services. It is advisable to give this approach a more prominent place in the general comment (e.g. in relevant paras. 36-39, 70, 75).

See further on

* the precautionary principle, children and harmful content: Lievens, E. (2009). Protecting children in the digital era: The use of alternative regulatory instruments. Brill.
* PbD and DPIA in relation to children’s rights: Hof, S. van der, Lievens, E. (2018). The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children’s Personal Data under the GDPR. *Communications Law*, Vol. 23, No. 1.
1. The right to privacy
	1. Data protection

Although Article 16 UNCRC does not explicitly refer to the child’s right to data protection, the elaborate attention that is devoted to this right under the right to privacy can only be welcomed. At the same time, it needs to be acknowledged that very different data protection frameworks exist around the world (see Milkaite, I., Lievens, E., Children’s rights to privacy and data protection around the world: challenges in the digital realm. European Journal of Law & Technology 2019, 10(1)). Some paragraphs under VI.E seem to be inspired by the EU General Data Protection Regulation (GDPR). Yet, when only certain elements are taken out of this particular regulatory framework, accompanying and necessary safeguards and mechanisms might be lost. A good example is the reference in paras. 72 and 74 to consent. Under EU data protection legislation, consent is only one of six lawful grounds that can be used for legitimising the processing of personal data, and - significantly - not the most important or the most protective of children. Emphasising (children’s and parental) consent may therefore not strengthen the protection of children, unless it is embedded as one of the lawful grounds in a comprehensive system of data protection, like the EU General Data Protection Regulation, that includes mandatory data protection impact assessments and data protection by design, as well as a set of important data protection principles. Connected to this it is also not clear why certain data protection principles that are the backbone of the GDPR are mentioned and others are not (for instance, in the last sentence of para. 74).

* 1. The right to privacy *from* parents

It is also relevant that the requirement of parental consent could in certain circumstances be considered an invasion of privacy by children. Children will not necessarily want parents to be too involved in their affairs on the Internet, especially when it comes to sensitive issues (e.g. gender or sexuality) or when the relationship with the parents is problematic (see also para. 78 and 79), but also because they think more generally that parents do not need to know everything. Privacy is therefore perceived as undertaking (online) activities independently of their parents. Related to this, on top of agency, dignity and safety (see para. 69), privacy is relevant to the development of a child's identity and personality.

* 1. Anonymity

Para. 78 which discusses the protection of a child’s identity in the context of their right to a private life, is formulated in a somewhat contradictory manner. It is not entirely clear how the ‘safety by design approach’ that is described in this paragraph (describing illegal and harmful behaviour in terms of service or community guidelines and blocking users who do engage in such behaviour) relates to anonymity. It is important to note that the UN General Assembly in its Resolution on the right to privacy in the digital age (A/RES/73/179) has emphasised that “*in the digital age, technical solutions to secure and to protect the confidentiality of digital communications, which may include measures for encryption, pseudonymization and anonymity, can be important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of expression and to freedom of peaceful assembly and association*”. This protection is essential regardless of age.

* 1. Paragraphs that require further clarification and missing issues in this section

We feel that para. 74 requires further clarification. It is not clear to which processing activities this paragraph refers to.

An issue that is relevant and is not touched upon in the draft General Comment relates to the use of children’s biometric data and requests to obtain access to smartphones and social media accounts in the context of migration.

See, for instance: Fundamental Rights Agency, Under watchful eyes: biometrics, EU IT systems and fundamental rights, 2018, <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf>

1. Sexting

Sexting is addressed in a limited manner in the draft General Comment.

* 1. Sexting as part of legitimate exploration of sexuality

Sexual acts or expressions constitute a part of children’s legitimate exploration of their sexual identity and a way to express their sexual individuality. In this sense, the production of sexually suggestive or explicit images by children for private use (sexting) may be conceived as falling within the scope of a child’s freedom of expression and right to privacy (articles 13 and 16 UNCRC). In the current version, sexting is only mentioned in the context of illegitimate behaviour (infra).

See: Witting, S., Regulating bodies: The moral panic of child sexuality in the digital era, Critical Quarterly for Legislation and Law Vol. 1 (2019), 5-34.

* 1. Non-consensual sharing as illegitimate behaviour

In para. 85 there is a reference in relation to sexting: “These may include cyberbullying, harassment, violence, and sharing of sexualized images of children (“sexting”), and the promotion of self-harming behaviours such as cutting, suicidal behaviour or eating disorders.” We suggest adding ‘non-consensual’ before ‘sharing sexualised images of children’, in order to reflect illegitimate behaviour.

* 1. Balanced regulatory frameworks regarding sexting

Having clear and foreseeable national regulatory frameworks that protect consensual sexual activities in which children may be involved and which can be regarded as the normal exploration of sexuality in the course of human development, on the one hand, but that address coercive and non-consensual acts, on the other hand, is of crucial importance in the world in which children grow up today. To that end, such frameworks should include provisions that enhance and safeguard trust, control and privacy for children. When sexting occurs on a consensual basis among children, criminalisation of such behaviour is not in the best interests of the child.

See: Chatzinikolaou A, Lievens E., A legal perspective on trust, control and privacy in the context of sexting among children in Europe. Journal of Children and Media 2020;14(1):38-55.

1. Gaming as part of the right to leisure and play

There is little attention for gaming in the General Comment and especially the positive aspects of gaming. The few times that gaming is mentioned it is about the negative side ('excessive gaming'). Gaming is an important online pastime for children (both gaming themselves and watching other gamers). Moreover, it is part of youth culture (including meme culture) and in-game items that are acquired can be part of children’s identity development.

Of course, there are also issues that deserve attention such as gaming business models, including marketing and manipulative or exploitative design (as is done in para. 119), as well as, in very problematic cases, forms of addiction of which gaming may be a part, but it is questionable whether children will recognise themselves very much in the General Comment if it is not also acknowledged how important gaming is as part of their right to leisure and play.

1. Protection from economic exploitation
	1. Commercial advertising & marketing

It seems a little bit odd that section V.J. ‘Commercial advertising and marketing’ is included under the Chapter General Measures for Implementation by States. The section contains paragraphs that refer mostly to data protection related aspects of commercial advertising and marketing and could also fit under section XII.A ‘Protection from economic, sexual and other forms of exploitation (arts. 32, 34, 35 and 36)’. Children should especially be protected from manipulative and exploitative ways of targeting them for commercial purposes. Paragraph 43 would better fit under section VI.E ‘The right to privacy’.

* 1. Child influencer work

In the digital environment, some children have become an important source of income for their families by becoming (social media) influencers, or professional e-Sports players. The General Comment could point to the fact that article 32 UNCRC requires that influencer work or e-Sports activities are not harmful to a child’s health, or physical, mental, spiritual, moral or social development, and may not interfere with the child’s education.

See:

* van der Hof, S., Lievens, E., Milkaite, I., Verdoodt, V., Hannema, T., Liefaard, T., The Child’s Right to Protection against Economic Exploitation in the Digital World, International Journal of Children’s Rights (forthcoming)
* Verdoodt, V., Hof, S. van der, Leiser, M., Child labour and online protection in a world of influencers, in: C. Goanta, S. Ranchiordas (Eds), The Regulation of Social Media Influencers, [Elgar Law, Technology and Society series](https://www.e-elgar.com/shop/gbp/book-series/law-academic/elgar-law-technology-and-society-series.html) 2020.

\*\*\*

Thank you for the opportunity to contribute our thoughts to the consultation process. We remain available for further clarification or questions.

Prof. dr. Simone van der Hof (eLaw, Leiden University); s.van.der.hof@law.leidenuniv.nl

Prof. dr. Eva Lievens (Law & Technology, Ghent University); eva.lievens@ugent.be