**Submission to the**

**United Nations Committee on the Rights of the Child**

Draft General Comment 25 on

Children’s Rights in Relation to the Digital Environment

*Contributors:*

The American University of Paris Working Group on Human Rights Sub-committee on the Economic Exploitation of Children’s Data

Nicole Brodie

Anel Gonzalez

Meriem El Mokhfi

Michelle Simon

*Introduction:*

The Working Group on Human Rights Sub-committee on the Economic Exploitation of Children’s Data at the American University of Paris welcomes the Committee’s initiative to prepare a General Comment on the Rights of the Child. We are honored to have the opportunity to share our research on children’s data protection. We believe it is critical that the General Comment articulate the importance of State Parties protecting children’s data in an increasingly digital environment. The General Comment must also remind State Parties of their obligation to provide full comprehensive transparency and protection in regards to children’s data.

*We recommend the following changes be made with respect to the four paragraphs below in the draft General Comment:*

71. Interference with a child’s privacy is only permissible if it is neither arbitrary nor unlawful (article 16). This means any such interference must be provided for by law, be aimed at ***providing a safe secure space in which their data is held in a protected site in relation to*** achieving a legitimate purpose, be proportional and not in conflict with the provisions, aims and objectives of the Convention.

76. The digital surveillance of children may result in the constant scrutiny of children while online or offline, for example in educational and care settings. Any surveillance of children together with any associated automated processing of personal data, shall respect the child’s right to privacy and shall not be conducted routinely, indiscriminately, or without the ***full and informed consent of the child’s parent or caregiver***, and where possible the right to object to such surveillance.

91. In supporting and guiding parents and caregivers regarding the digital environment, States should promote their awareness to respect children’s growing autonomy and need for privacy, in accordance with their evolving capacities. States should take into account that children often embrace and experiment with digital opportunities, and may encounter risks, particularly at a younger age than parents and caregivers anticipate. Some children report wanting more support and encouragement in their digital activities, especially where they perceive parents’ and caregivers’ approach to be highly restrictive and not adjusted to their evolving capacities. ***States should take into account the protection of children’s data with respect to*** ***parental control and not only focus on restricting their access to harmful content.***

121. Children should be protected from all forms of exploitation prejudicial to any aspects of their welfare in relation to the digital environment. This may occur in many forms, such as economic exploitation including child labour, sexual exploitation and abuse, ***commercial exploitation***, sale, trafficking and abduction of children, grooming children to participate in criminal activities including hacking, and/or financial crimes.

|  |
| --- |
| 71. Interference with a child’s privacy is only permissible if it is neither arbitrary nor unlawful (article 16). This means any such interference must be provided for by law, be aimed at ***providing a safe secure space in which their data is held in a protected site in relation to*** achieving a legitimate purpose, be proportional and not in conflict with the provisions, aims and objectives of the Convention. |

The child shall not have their data interfered with unless the matter in which it is done provides assurance that there are no unlawful breaches. There is no reason to list exceptional interference without detailing what the exemptions would be. The wording clarifies under which condition children would have their data stored . State Parties must employ adequate data security, retention, and deletion practices in order to ensure that these practices are not in conflict with the Convention. Regarding safe security practices, it is suggested that States look towards integrating robust secure data boxes in their national school system to ensure that the child’s information is kept safe. As stated in the document from the Office of the State Superintendent of Education in DC involving using secure data transfer to protect student privacy “All staff who use student information bear responsibility for handling it in a responsible and confidential manner. Secure file transfer is one important strategy to protect student information.” (Young) This ensures the data remains safe and can only be handled by other parties on a case by case basis.

The General Comment must also pay particular attention to the child’s confidentiality rights, which may not put the child’s life in danger. For example, the police may look at a young person’s emails if someone who isn’t who they say they are is contacting them, for malicious intent. Their phone calls and emails are indeed private, unless potential harm could befall the child or in cases of medical necessity. There may also be a case that a child has shared risky, even dangerous, content over social media. More active participation by parents/guardians who could intervene in such cases, is a necessary interference on the child’s right to privacy. The child should always be informed, alongside the guardian, that their right to a private space, even in an institution, is protected.

|  |
| --- |
| 76. The digital surveillance of children may result in the constant scrutiny of children while online or offline, for example in educational and care settings. Any surveillance of children together with any associated automated processing of personal data, shall respect the child’s right to privacy and shall not be conducted routinely, indiscriminately, or without the ***full and informed consent of the child’s parent or caregiver***, and where possible the right to object to such surveillance. |

Children cannot legally give consent to be surveilled, or to have their data recorded, even in educational or care settings. Therefore, a parent or guardian of the child must be the one to consent to that child’s being under digital surveillance, according to Article 5 of the Convention, “States Parties shall respect the responsibilities, rights and duties of parents or, where applicable, the members of the extended family or community as provided for by local custom, legal guardians or other persons legally responsible for the child, to provide, in a manner consistent with the evolving capacities of the child, appropriate direction and guidance in the exercise by the child of the rights recognized in the present Convention.”

It is not enough that children or their guardians know that the child is being surveilled, since they may not know or understand what that fully entails. A child’s parent or guardian must be able to fully consent to their child being put under digital surveillance and scrutiny, and aware of what that means. They must be informed exactly what that surveillance will consist of, what data will be collected, and what will be done with that data, and how long it will be stored.

This is especially important with the recent shift towards online schooling from home. Digital surveillance for educational purposes (both the recording of classes and the digitization of schoolwork) is becoming more widespread, and this leaves an opening for the surveillance to become overzealous, forcing children to give up more information than they or their parents may be comfortable with. Article 36 of the Convention states that “State Parties shall protect the child against all other forms of exploitation prejudicial to any aspect of the child’s welfare.” State parties must ensure that surveillance in educational or care settings does not result in the data collected during this surveillance being exploited. Requiring full and informed consent on the part of parents and guardians will help prevent any data collected under educational or care surveillance being used to exploit children, and in the case that does occur, give them increased legal protection.

|  |
| --- |
| 91. In supporting and guiding parents and caregivers regarding the digital environment, States should promote their awareness to respect children’s growing autonomy and need for privacy, in accordance with their evolving capacities. States should take into account that children often embrace and experiment with digital opportunities, and may encounter risks, particularly at a younger age than parents and caregivers anticipate. Some children report wanting more support and encouragement in their digital activities, especially where they perceive parents’ and caregivers’ approach to be highly restrictive and not adjusted to their evolving capacities. ***States should take into account the protection of children’s data with respect to*** ***parental control and not only focus on restricting their access to harmful content.*** |

Parents and caregivers should have access to parental control settings in devices, applications, websites and video games that their children have access to. Parental Control helps the parents prevent their children from stumbling into harmful content that is age-inappropriate.

The current parental control available for parents and caregivers mainly focuses on restricting access to certain websites, information, and words that may offend children; these controls can also limit children’s screen time. This tool is intended to prevent children’s access to pornographic and violent content. However, data collection is not mentioned in any of the settings of parental control. This does not protect children from data collection and the different uses and possible exploitation that may occur via that data. Parental control does not permit the parents and caregivers to block data collection.

The General Comment should take into consideration that data collection is present and required for most websites that are not considered harmful to children according to their content; data collection is also required by all social media platforms. That data is often used for economic purposes. The personal data of the child is therefore not protected because they access most websites as if they were adults.

Parental control should be extended to prevent websites and social media platforms to have access to, collect, share and use the personal data of the child. Parental control of content only gives parents and caregivers the illusion that their children’s online activities are safe. But, what is done with all the data that is collected on minors who are not even aware that they are providing data to servers, companies and social media platforms.

|  |
| --- |
| 121. Children should be protected from all forms of exploitation prejudicial to any aspects of their welfare in relation to the digital environment. This may occur in many forms, such as economic exploitation including child labour, sexual exploitation and abuse, ***commercial exploitation***, sale, trafficking and abduction of children, grooming children to participate in criminal activities including hacking, and/or financial crimes. |

Paragraph 121 of the Draft General Comment recognizes the indispensability of children’s protection against *“all forms of exploitation [...] in relation to the digital environment”*. As the Convention on the Rights of the Child under article 32 does not give a clear definition what economic exploitation consists of, we appreciate the provision of the Draft General Comment with such a specific listing of factors constituting economic exploitation. We welcome the drafting of the General Comment as an opportunity to extend the international framework on children’s rights by considering the impact of digital economic activities on children’s well-being and development. While article 121 acknowledges *“sale”* to be a noteworthy form of economic exploitation, it is not clear what activities that involves. Even more critical is the fact that commercial exploitation has been completely left out of Paragraph 121.

Although digital technologies have already become an integral part of children’s daily lives, lockdown measures implemented during the Covid-19 pandemic have increased the usage of digital devices by children. Children’s active participation in the digital space, reinforced through the current dependence on digital tools for distance learning (Wong et al., 2020), suggests an alarming possibility of children’s data being processed and collected for commercial purposes. Children are especially vulnerable to inappropriate handling of their data by corporate actors due to their higher persuasibility by behavioral advertising and a lower awareness of their rights and the risks arising in relation to personal data processing. Research has shown that data tracking, (automated) profiling and targeting instruments used by companies pose a fundamental threat to children’s privacy (Montgomery, 2007). Moreover, covert data collection, meaning the accumulation of personal data without consent, undermines children’s well-being and development for example by causing negative health impacts from food marketing, sexualizing children or reducing parent’s authority (UNICEF, 2018: 18-19).

As the obscured commercial intent of advertising often used in commercial profiling and automated advertising amounts to economic exploitation, we recommend commercial exploitation to be specified as a coequal form of exploitation in place of *“sale”* in Paragraph 121. To guarantee children’s full rights under article 32 of the Convention on the Rights of the Child in a highly commercialized, digital environment the Draft General Comment should urge State Parties to develop and implement guidelines for prohibiting the collection of children’s personal data for commercial purposes. Mechanisms to protect children from commercial exploitation in the digital environment must be in place especially where children are targeted by marketing strategies which are not suitable for their age. Furthermore, improved transparency with regard to children’s personal data processing and targeting by advertisement must be ensured in consultation with children and their guardians.

*Sources:*

Google’s response to the Committee on the Rights of the Child consultation. May 2019. <https://www.ohchr.org/_layouts/15/WopiFrame.aspx?sourcedoc=/Documents/HRBodies/CRC/GCChildrensDigitalEnvironment/OtherStakeholders/Google.docx&action=default&DefaultItemOpen=1>

Montgomery, Kathryn C. “Protecting Children’s Privacy Online: The Battle Continues.” *Human Rights*, vol. 39, no. 3, American Bar Association, Mar. 2013.

UNICEF. “Children and Digital Marketing: Rights, risks and opportunities. Discussion Paper.”, July 2018, available at: <https://www.unicef.org/csr/files/Children_and_Digital_Marketing_-_Rights_Risks_and_Opportunities(1).pdf> [last accessed: 12 Nov. 2020].

Wong, Chee Wai et al. “Digital Screen Time During COVID-19 Pandemic: Risk for a Further Myopia Boom?.” *American journal of ophthalmology*, S0002-9394(20)30392-5. 29 Jul. 2020, doi:10.1016/j.ajo.2020.07.034.

Young, Shana. "Using Secure Data Transfer to Protect Student Privacy." 1 February 2018. *Office of the State Superintendent of Education.* Document. 12 November 2020. <https://osse.dc.gov/publication/using-secure-data-transfer-protect-student-privacy>