# Response to the European Commission's communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence (White Paper COM 2020-65)

The European Commission's White Paper on Artificial Intelligence COM 2020-65 (compare also the strategy papers on Data and on the Digital Future: COM 2020-66, COM 2020-67)[1] announce a global race for quantum computing and the development and deployment of Artificial Intelligence (AI) systems. To join the race, it proposes the facilitation of the next data wave and data interoperability across EU member states. While the White Papers envision a competitive European Union in the data economy of the future, White Paper COM 2020-65 also identifies various risks that stem from faults within AI practice itself. But through this focus on AI's own workings, White Paper COM 2020-65 lacks clarity with regards to various implications of AI practice for the wider social domain.

Our approach in this paper is informed by the following basic principle: that AI practice, and its associated processes of collecting and using data, generate *social externalities* that are highly consequential for people to whom those data relate. Such social externalities cannot in principle be addressed through proposals for conducting AI more rigorously and fairly of the sort mentioned in White Paper COM 2020-65. Such externalities may affect acutely **children**, who are vulnerable human subjects in a transitional phase of their lives. In this paper we focus on that example, arguing that closer attention must be paid to the actual social contexts in which data relating to children comes to affect their lives through AI practices.

**The distinctive situation of children in relation to AI practice**

A third of the world's Internet population are children (UNICEF, 2017). Networked technologies for children (defined as those aged under 18 years old) provide many opportunities for learning, intercultural connectedness and creative expression. While some efforts have been made to protect children's rights and freedoms online (Livingstone et al., 2016), many challenges relating to diminishing potential risks of harm remain unsolved (Smahel et al., 2020; Livingstone, 2020). We argue in what follows that distinct measures need to be taken to safeguard children in the context of developing and deploying AI-based products and services, and the processes surrounding these (i.e. data collection, use and processing), not least in light of and after the COVID-19 global pandemic. We look at children as one example of vulnerable population that can be significantly impacted by AI practices.

In response to White Paper COM 2020-65, we reflect on the growing concerns relating to children's privacy and digital rights and freedoms in the increasingly digitized environments they occupy and propose a number of recommendations that address in an evidence-based and balanced way the benefits and risks from the collection of granular, biometric and "inferred" data (from profiling and diagnostics) and the measures needed to diminish those risks, while enabling children's beneficial use of advancing digital technologies. Our response encourages the European Commission to consider concrete scenarios in which AI-based automation and data-driven decision-making may lead to discrimination against, reduced future opportunities for, and infringement of digital human rights of children (as defined by the UN Convention on the Rights of the Child).

The potential benefits of using AI in education and in relation to children more generally are significant: for example, at the most general level, the use of student and school data may contribute to research in learning and help advance pedagogic theory (Baker and Inventado, 2014). More specifically AI may be used to help guide specific pedagogical intervention, which leads to higher school attainment (Arnold and Pistilli, 2012), including through forms of self-paced learning. At the level of school governance, biometric data can be used to provide better

[1] This response will focus specifically on COM 2020-65, but will sometimes refer as context to the three papers collectively (""The White Papers").

authentication and verification. That said, there are significant risks arising from the use of AI in education and wider relations between adults and children, on which this paper focuses.

Key issues not addressed in White Paper COM 2020-65 on Artificial Intelligence regarding children including the following:

1. **Definitional Issues:**
    a. White Paper COM 2020-65 distinguishes remote biometric identification from biometric authentication,[2] and emphasizes the need for specific safeguards with regard to the use of AI systems in remote biometric identification.[3] We agree that it can be relevant to distinguish between different kinds of systems collecting biometric data depending on how immediately intrusive they are. For example, there are basic biometric identification systems, which collect individuals' physical or behavioural characteristics through equipment that automatically compares the collected biometric data with biometric information stored in the system, but without any Machine Learning. If there is a match, the individual in question can be identified. Other biometric systems (whether for identification or otherwise) may include Machine Learning technologies that combine biometric with other data to "learn" about an individual or user. The latter systems "react" and adapt their intended use according to the collected behavioural or physical biometric data. We agree that this second type of system, which White Paper COM 2020-65 refers to as remote biometric identification, poses more serious and open-ended risks of harm, not least to children as they grow, especially when it is in operation for long time-periods. Nonetheless, it is important to stress than all biometric systems and all practices aimed at collecting and using biometric data, be it for remote identification or for authentication purposes, can lead to problematic data triangulations and unwelcome inferences. This is especially the case when it comes to vulnerable populations such as children. We would therefore recommend applying heightened safeguards also to seemingly less intrusive biometric authentication techniques.
    b. A particular issue about the temporality of data processing arises in relation to data gathered and used in the light of COVID-19. Societies will find some data collection and uses of AI acceptable in an emergency that we ordinarily would not. The pandemic is resulting in an unprecedented amount of data capture, including biometric data, from stay at home school video conferencing, quarantine enforcement, public temperature checks and contact tracing, including children relating to children. If biometric data must be used to limit the spread of the virus, we strongly urge the EU Commission to allow the processing of such data only for specific, necessary and time-limited purposes, and only data collected in public spaces, and not in any case to allow the development and deployment of biometric and AI-based systems aimed at following and tracking intimate aspects of individuals' lives in a temporally unlimited manner. If the latter were to happen, children and vulnerable populations would be the first to suffer lasting consequences.
2. **Contextual issues**:
    a. The collection of data from the use of educational technologies, which children often use outside of school, raises concerns. The key actors here are not just schools and teachers, but a wide variety of private corporations – including data brokers, education platforms, etc. – whose considerable impact in the education field is not specifically addressed in the White Papers. Software installed on school tablets and computers can monitor children's online behaviour outside of school, and safeguards against these practices are needed and not discussed in this and other White Papers.
    b. The White Paper gives insufficient attention to issues relating to transfer of data between contexts: children need to be protected against the transfer of data

[2] See, e.g., footnote 52 on page 18.
[3] See page 21 and following.

about or affecting them collected for one purpose (for example education or health) and subsequently used for other purposes, unless this is specifically permitted within the reasonably expected terms of operation of the institutions concerned. When repurposing data, companies operating with children and in school settings must be subjected to heightened safeguards beyond those that already exist in data protection legislation.

c. Data about children is insufficiently regulated under EU law. The EU Commission should consider including data about children aged less than 16 years of age as a special category under Article 9 of GDPR (special categories of personal data), as such data should be subject to stronger exceptions than adult personal data. The consent guarantees in Article 8 GDPR are insufficient.

3. **Consent issues:**

a. In this context, the legal definition of a "child" as set out in the United Nations Convention on the Rights of the Child (CRC) (UN 1989) must be carefully considered: the interpretations and accepted norms of children's rights as part of their human rights are different in different cultural contexts. In particular, while the CRC (UNICEF, 2016) guarantees all children, among other rights, the right to access information and education, and acknowledges other rights commonly related to adults (such as the right to participation and assembly), it recognizes children's unique needs, capacities and vulnerabilities. As a result, the CRC states that children have the right to development and play; the right to protection from all forms of violence, abuse and exploitation; and the right to be brought up in a protective and caring environment. Reference to and acknowledgement of these substantive rights as expressed by the CRC must be made, since those rights are without question affected by big data use and the development of AI products and services. For instance, privacy risks stemming from the collection of children's data extend from interpersonal risks (lack of privacy from others, including parents, which can condition children's behaviour and basic freedoms: Livingstone, 2008) to institutional risks (Livingstone et al., 2018). Data collection by third-party agencies such as state or local education agencies is increasingly becoming the norm. Further access to other personal data for example, to predict problematic or even criminal behaviour can pose future limitations and prejudice towards still developing young people before they have even committed a crime (DefendDigitalmed, 2018).

b. In the context of intrusive biometric technologies or data-intensive AI systems, consent is rarely a sufficient safeguard for the fundamental rights of children and vulnerable populations (Bietti, 2020). More stringent safeguards must be put in place to avoid repurposing data and de-contextualising it. Nonetheless, we here make a few comments on how consent can be made more empowering for children in the digital economy.

c. Current basic information provided about how data is used or by whom to parents and guardians is insufficient to give children an adequate awareness of the meaning and consequences of such data use. This issue is not sufficiently addressed in EU legislation, nor is it mentioned in White Paper COM 2020-65, or in the other White Papers relating to data in the EU Digital Single Market. Consent to collect and use children's biometric data cannot just be parental or guardian consent, as per Article 8 GDPR. The UK's Protection of Freedoms Act of 2013 also stipulates that parents must give consent for their children's biometric data to be collected, processed, stored, and used. However, as we have seen elsewhere (Livingstone, 2020), parental consent is, in practice, very often not enough. This also becomes problematic for teenagers (e.g. raising the age of consent, as proposed by COPPA Rule and Act) and can lead to "chilling" effect on teens' freedom of expression' among other problems. If reliance on parental consent is to be reduced for certain age-brackets, the consent of young people themselves must also be required or taken into account.

d. Opting out of data collection systems becomes problematic for young people and their parents because it means opting out of opportunities for education and other benefits afforded by AI-based technologies

4. **Jurisdictional issues:** White Paper COM 2020-65 calls for the development of highly sophisticated technologies that necessitate the processing of data (personal and non-personal). Data is generated through the interaction and consumption by individual users of networked digital products and services. The multiplicity of legal regimes regulating these products and services poses jurisdictional challenges. For example, the global impact of US rules with regard to the development and deployment of AI-based technologies will impact European citizens, children in particular, since many US-based companies continue to provide products and services to consumers in EU Member States. It is therefore important for EU institutions to proactively step in and protect children in the transnational digital economy.

**Resulting Legal Risks**

1. Discrimination based on genetic information: in the US the Genetic Information Non-discrimination Act (GINA) of 2008 bans discrimination based on genetic information in health insurance and employment. However, GINA does not protect individuals from genetic discrimination by life, long-term care, and disability insurers. There is a wider risk here relevant to the EU. In the case of children, medical data collection in schools, combined data collection from the use of AI and biometrics can identify individuals with great precision (Dwork and Roth, 2014). This can lead to discriminative decision-making beyond school, against the consequences of which children are not protected

2. Biometric data can be altered, using "deepfake" software, causing psychological harm of distress, physical threat, exploitation and other risks to individuals. Children are particularly vulnerable to such risks and long-term damage, given their particular vulnerabilities as recognised in the CRC. For example, young children (0-8) are already regular users of networked devices. However, at this age children do not have a clear understanding of commercial information, disinformation ("deepfakes") and other content that requires not only digital media literacy but also basic literacy (Chaudron et al., 2018)

3. Loopholes in data privacy laws such as COPPA (for the US) and GDPR (for the EU) lead to loss over data protection safeguards as both frameworks allow for disclosures of personally identifiable information and the use of student data by third parties under the conditions that such use is intended for educational purposes.

4. Particular attention must be made with regards to children from less privileged backgrounds and those with disabilities. They are particularly vulnerable in cases of data-driven environments and AI-based automation, medical, such as DNA and other biometric data collection because of the heavy costs of correction and limited access to legal representation.

5. The COVID-19 pandemic may act as an incentive on the creation and deployment of data harvesting and monitoring tools that rely on sensitive data about individuals, including biometric data. These tools should not be made lawful to use unless they are strictly necessary to tackle the pandemic and must be withdrawn from the market as soon as the pandemic is gone. As said, pervasive surveillance tools can become entrenched in our societies and radically undermine the freedoms and wellbeing of children and other vulnerable populations. If EU law needs to be amended to allow for exceptions during the pandemic, those exceptions must remain narrow and must be time-limited.

**Conclusion**

This response to White Paper COM 2020-65 has taken children as a paradigmatic example of a group particularly vulnerable to the social externalities of AI and data processing practices, harms that extend to other social groups. Such externalities cannot in principle be addressed solely by adjusting AI practices, but require separate civic, legal and social attention.

We have attempted to summarise the key issues that arise in relation to children. However the lives of children are just one of many aspects of the social world touched by AI practices. Because children have particular vulnerabilities, and because harms done to them now may shape the rest

of their lives, we have placed particular emphasis on the risks caused to them. But the issues raised here are only examples of the many social externalities predictably generated by AI practice that, we submit, are insufficiently addressed by EU law and the position expressed in the White Papers, and specifically White Paper COM 2020-65, to date.

**REFERENCES**


Arnold, K. E., and Pistilli, M. D. (2012). Course signals at Purdue: using learning analytics to increase student success. *The 2nd International Conference on Learning Analytics and Knowledge*, Vancouver, 267-270 Retrieved from: https://doi.org/10.1145/2330601.2330666

Baker, R., and Inventado, P. S. (2014). Educational data mining and learning analytics. in Larusson, J. A., and White, B., *Learning analytics experiences*, New York: Springer, 61-75.

Bietti, E. (2020). Consent as a free pass: Platform power and the limits of the informational turn, 40 Pace L. Rev. 307. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3489577

Chaudron, S., Di Gioia, R., and Gemo, M. (2018). *Young children (0-8) and digital technology, a qualitative study across Europe*. EUR 29070. Retrieved from: https://doi.org/10.2760/294383

DefendDigitalMe (2018). The state of data. Lessons for policymakers. Retrieved from: http://defenddigitalme.com/wpcontent/uploads/2018/05/StateOfDataReport_policymakers_ddm.pdf

Dwork, C., and Roth, A. (2014). The algorithmic foundations of differential privacy. *Theoretical Computer Science, 9*, (3-4), 211-407. http://dx.doi.org/10.1561/0400000042

Livingstone, S. (2020). Realizing children's rights in relation to the digital environment. Retrieved from: http://eprints.lse.ac.uk/103563/

Livingstone, S., Carr, J. and Byrne, J. (2016). One in three: Internet Governance and Children's Rights. Innocenti Discussion Paper No.2016-01, UNICEF Office of Research, Florence.

Livingstone, S., Stoilova, M., and Nandagiri, R. (2018). Children's data and privacy online: Growing up in a digital age. Retrieved from: http://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Evidence-review-final.pdf

Smahel, D., Machackova, H., Mascheroni, G., Dedkova, L., Staksrud, E., Ólafsson, K., Livingstone, S., and Hasebrink, U. (2020). EU Kids Online: Survey results from 19 countries. EU Kids Online. DOI: 10.21953/lse.47fdeqj01ofo

UNICEF (2018). Make the digital world safer for children - while increasing online access to benefit the most disadvantaged. [Press Release]. Retrieved from: https://www.unicef.org/media/media_102303.html



**VELISLAVA HILLMAN** Fellow (2018-19), Berkman Klein Center for Internet and Society, Harvard University

**NICK COULDRY**, Professor of Media, Communications and Social Theory, London School of Economics and Faculty Associate, Berkman Klein Center for Internet and Society, Harvard University

**ELETTRA BIETTI**, Kennedy Scholar, Doctoral Candidate at Harvard Law School, and Affiliate, Berkman Klein Center for Internet and Society, Harvard University

**GRETCHEN GREENE**, Fellow, Belfer Center for Science and International Affairs, Harvard Kennedy School and Senior Advisor, The Hastings Center


**APRIL 2020**