DIGITAL
LAW
ASSOCIATION

SUBMISSION

UNICEF Public Consultation on Draft Policy Guidance on AI for Children

10 December 2020

Disclaimer and Copyright

While the DLA endeavours to ensure the quality of this publication, it does not accept any responsibility for the accuracy, completeness or currency of the material included in this publication and will not be liable for any loss or damage arising out of any use of, or reliance on, this publication.

© The Digital Law Association (DLA)

Contents

ABOUT THIS SUBMISSION

The Digital Law Association is an organisation dedicated to the promotion of a fairer, more inclusive, and democratic voice at the intersection of law and technology.

Our mission is to encourage leadership, innovation, and diversity in the areas of technology and law, and particularly bringing together female and other diverse leaders in digital law.

This document was created by the Digital Law Association in consultation with its members. In particular, the compilation of this submission was led by:

- Alex Sims, an Associate Professor in the Department of Commercial Law at the University of Auckland and a Research Fellow at the UCL Centre for Blockchain Technologies. Her primary areas of research and publication are on blockchain technology, in particular, DAOs (decentralised autonomous organisations) and the regulation of cryptocurrencies and legal issues surrounding smart contracts.

This submission was coordinated by the following Digital Law member:

- Iris Rad, an Australian lawyer with an LLB (Hons) from Monash University and a Sessional Academic at the Royal Melbourne Institute of Technology. Her primary interests are in the regulatory environment of emerging technologies, particularly cryptocurrencies, and privacy issues surrounding facial recognition. She currently works in Private Advisory at Mills Oakley Lawyers in Melbourne.

This submission has been contributed to by the following Digital Law members:

- Wendy Chen, final-year JD student at Melbourne Law School. She is currently researching data law, cybersecurity and privacy law.
- Ravi Nayyar, a BCom (Hons I) LLB student at the University of Sydney. He facilitates monthly discussions with fellow law students and younger lawyers around digital law issues (including AI), has co-written policy submissions to Australian government inquiries concerning AI and has produced and hosted a current affairs digital law podcast (an episode of which analysed police usage of facial recognition systems).
- Holli Sargeant, a postgraduate research student at the Faculty of Law, University of Cambridge. She is researching legal accountability of the use of artificial intelligence in high-stakes decision making. Holli is an admitted solicitor in Australia having worked in the Herbert Smith Freehills' Digital Law Group and the Australian Human Rights Commission's Human Rights and Technology Project.
- Aarvi Singh, a law student at the Rajiv Gandhi National University of Law, Punjab. She is a researcher at the Institute for Internet and Just Society and a research assistant at Ethical Tech at Duke University. She has also created two bots on Telegram; one summarises judgments, other one is a news aggregator (non-commercial).

Response to Draft Policy Guidance

1. **Is the purpose of the Guidance clear?**

   Very clear

2. **Is the target audience for the Guidance clear?**

   Very clear

3. **Are the format and visual elements of the document easy to understand? If not, please specify what improvements could be made (in the category labelled 'Other').**

   Very clear

4. **What are the aspects and/or sections of the guidance that are the most useful to you and your organisation and why?**

   We do not have substantive commentary on this question but are of the view that this Guidance is likely to be useful across a variety of organisations.

5. **Are the terms and definitions in the guidance understandable? If not, what relevant terms could be added or clarified and how? Please limit your response to include no more than 3 key terms in the category labelled 'Other'.**

   The Digital Law Association recommends the clarification of three key terms in UNICEF's Guidance, being 'ethics', 'personal data' and 'machine learning'.

   ### *Ethics*

   The Guidance should draw out the ethical reasoning that UNICEF is applying towards responsible, lawful, beneficial and robust artificial intelligence. In particular, a discussion could be included on the framework provided by the Convention on Rights of the Child as the yardstick for consideration of Responsible or Ethical AI.

   ### *Personal data*

   The definition of personal data (also referred to as 'personal information') should be broader than 'facts, figures and information'. The Digital Law Association suggests that the definition of 'personal information' for children must be context-based and identifiable as per Australian law.

   ### *Machine Learning*

   The Digital Law Association suggests that the definition of AI must consider the perception of machine intelligence and ways to enhance it.

6. **Are the use cases presented in chapter 4 relevant for your local context? Are there any other use cases or examples that should be included to further describe the impact of AI systems on children's rights?**

   Given the international nature of the Digital Law Association we have not provided specific commentary on our local contexts. However, the use cases in Chapter 4 of the Guidance are strong examples of the impact of AI systems on children's rights around the world.

7. **Our aim is to provide practical guidance that can be used by government agencies, companies and organizations. Do you consider the guidance practical enough to use in these settings? If not, please specify what improvements could be made (in the category labelled 'Other').**

   Yes

8. **Are the nine requirements for child-centred AI understandable?**

   Yes

9. **Is a requirement missing or does a requirement need to be expanded further? If so, which one and why?**

   The proposal to develop diverse datasets of children's data in Requirement 3 is valuable considering the potential fairness and algorithmic bias challenges presented by under-represented individuals and groups in commercially available data sets. However, it equally raises privacy concerns and broader social concerns about the types of data that are either being collected or simulated. Further clarity is required on the substance of this requirement in relation to the proportionality between the increased representation of children and young people in datasets, with the responsibility to protect the unique vulnerability of children's data. Alternatively, if this proposal refers to the simulation of datasets, this equally raises questions as to the developers' responsibility of creating accurate and inclusive collections of children's data for use that is therefore beneficial to children.

   We agree with Requirements 4 and 5 that children's privacy and safety must be ensured in an AI world. The Guidance, however, only briefly discusses the right of children to engage in leisure, play and cultural activities. These rights should be highlighted in the Requirements, given the critical need to balance safety and privacy while also offering the opportunity to engage children.

   AI tools will increasingly become a key part of children's play and leisure time, whether through an online connection with classmates and friends, AI-enabled toys, or particularly during the COVID-19 pandemic, capturing online cultural activities, history and information available for children to explore from their homes.

10. Are concrete recommendations missing from any of the nine requirements? Do any recommendations need further elaboration? If so, please propose additional recommendations or edits and explain why they are needed.

Information Environments Recommendation for the First Requirement

The Digital Law Association believes that a concrete recommendation is missing from the first requirement, one which addresses the potential adverse effects posed by AI systems on the information environments that children interact in or are otherwise influenced by (“Information Environments Recommendation”). The Digital Law Association proposes the following wording for the headline of that recommendation:

“Ensure that AI systems do not corrupt the information environments that children interact in, or otherwise influence children, by helping to spread misinformation and disinformation, and confining children’s perspectives to filter bubbles.”

The European Commission’s High-level Group on fake news and online disinformation (Allan et al, 2018) provides a good definition of disinformation and misinformation. The Digital Law Association does not want to see children falling victim to active measures by state and non-state actors (facilitated by AI systems (Smith and Mansted (2020)) and targeted campaigns to confine children's intellectual curiosities and opinions to filter bubbles, as defined by Abrassart et al (2018).

The DLA submits that the Information Environments Recommendation is grounded in the Convention on the Rights of the Child arts 2(2), 3(1), 13(1), 14(1), 15(1), 17 (particularly sub-article 17(e)), 28(1) and the Montréal Declaration for a Responsible Development of Artificial Intelligence*:* 2018 Principle 7(4).

Cybersecurity Recommendation for the Fifth Requirement

The Digital Law Association submits that a concrete recommendation is missing from the fifth requirement. There is a need to expressly address the cybersecurity risks faced by AI systems (the 'Cybersecurity Recommendation”). The Digital Law Association recommends that the headline for the fifth requirement expressly include cyber security and proposes the following wording for the headline of that recommendation:

“Require the implementation of risk-based cybersecurity controls in AI systems — particularly to protect the source code of their algorithms, training data and any tools the operations of which are influenced by the algorithms — that target or otherwise influence children, and the regular testing of these controls for their effectiveness in mitigating cybersecurity risk and enabling cyber resilience. ”The Digital Law Association agrees with the National Science and Technology Council, Committee on Technology, Executive Office of the President (2016), which highlighted: “AI systems also have their own cybersecurity needs. AI-driven applications should implement sound cybersecurity controls to ensure the integrity of data and functionality, protect privacy and confidentiality, and maintain availability."

Robust cybersecurity is required for people to trust and be confident in AI systems. Medcraft 2016; Australian Securities & Investments Commission 2015 made this point about technological systems and it applies equally to AI systems.

Micro-targeting children

In online digital environments, the targeting of children in personalised/targeted advertising should not be tolerated. Any forms of nudging that can hurt children's perceptions of reality, particularly in relation to body image and beauty should be tightly controlled. Included in this regulation should be data collection of a child's virtual likes or dislikes in social media profiles.

11. Are there resources, materials or evidence that could be used to further support the guidance? If yes, please specify: (1) the material type (i.e. report, toolkit, guidance, initiative, etc.), (2) the name of the resource, (3) URL, and (4) what specific section of the guidance it relates to.

Initiatives

Abrassart, Christophe et al (2018), *Montréal Declaration for a Responsible Development of Artificial Intelligence: 2018* http://dcfa4bd-f73a-4de5-94d8-c010ee777609.filesusr.com/ugd/ebc3a3_506ea08298cd4f8196635545a16b071d.pdf = **Relates to Guidance Sections 3.1 and 3.5**

Report/Submissions

- Allan, Richard et al (2018), *A Multi-Dimensional Approach to Disinformation: Report of the Independent High level Group on Fake news and Online Disinformation*: https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation = **Relates to Guidance Section 3.1**
- Australian Securities & Investments Commission (2015), *Report 429: Cyber Resilience: Health Check*: https://download.asic.gov.au/media/3062900/rep429-published-19-march-2015-1.pdf = **Relates to Guidance Section 3.5**
- Brown, Ellen et al (2019), *Submission on the Department of Industry, Innovation and Science's Discussion Paper - Artificial Intelligence: Australia's Ethics Framework*: http://go.lawsociety.com.au/l/533512/2019-06-12/34c752/533512/125067/20190611_CET_Submission_on_the_Department_of_Industry_Innovation_and_Science_s_Dis.pdf = **Relates to Guidance Section 3.5**

- Smith, Hannah and Katherine Mansted (2020), *Weaponised Deep Fakes: National Security and Democracy*: https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-04/Weaponised%20deep%20fakes.pdf?IgwT9eN66cRbWTovhN74WI2z4zO4zJ5H = **Relates to Guidance Section 3.1**
- Medcraft, Greg (2016), *Building Resilience: The Challenge of Cyber Risk*: https://download.asic.gov.au/media/4120903/speech-medcraft-acci-dec-2016-1.pdf = **Relates to Guidance Section 3.5**
- National Science and Technology Council, Committee on Technology, Executive Office of the President (2016), *Preparing for the Future of Artificial Intelligence*: https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf = **Relates to Guidance Section 3.5**
- Saygin, Onur et al (2020), *Submission on the Human Rights Commission's Discussion Paper - Human Rights and Technology*: https://go.lawsociety.com.au/l/533512/2020-05-21/3dwnpq/533512/191911/20201404_Human_Rights_and_Technology_Discussion_Paper.pdf = **Relates to Guidance Section 3.0 in its entirety**

Guidance

- Department for Digital, Culture, Media & Sport and Home Office (2020), *Online Harms White Paper*: https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper = **Relates to Guidance Section 3.5**

Articles

- Haidt, Jonathan (2019), *More Social* Media *Regulation*: https://politico.com/interactives/2019/how-to-fix-politics-in-america/polarization/more-social-media-regulation/ **= Relates to Guidance Section 3.5**
- Finnegan, Shannon, "How Facebook Beat the Children's Online Privacy Protection Act: A Look into the Continued Ineffectiveness of COPPA and How to Hold Social Media Sites Accountable in the Future" (2020) 50 *Seton Hall Law Review* 827 = **Relates to Guidance Section 3.4**
- Urgoiti, Lucas, "The Video Privacy Protection Act and Consumer Data: Are You Plugged In?" (2020) 53 UC *Davis Law Review* 1689 = **Relates to Guidance Section 3.4**

Books

- Mark Burdon, *Digital Collection and Information Privacy, Cambridge* University Press, 2020 = **Relates to Guidance Section 3.4 and 3.6**
- Michael Kearns and Aaron Roth, *The Ethical Algorithm*, Oxford University Press, 2019 = **Relates to Guidance Section 3.6 and 3.7**
- Giovanna Mascheroni and Donell Holloway (ed.), The Internet of Toys, Palgrave Macmillan, 2019 = **Relates to Guidance Section 3.0 in its entirety**

12. Are the 'Tools to Operationalize the Policy Guidance' (roadmap for policymakers and a development canvas for AI software teams) practical for you and your organization? Please describe.

We do not have substantive commentary on this question but are of the view that the Roadmap and development canvas are likely to be useful across a variety of organisations.

13. Is anything else missing from the policy guidance that UNICEF should consider for inclusion in the next version?

Social Media and the 'Internet of Toys'

UNICEF should consider including a discussion or policy suggestions on the use of social media by children. The intentionally addictive design of social media feeds, the personalisation of targeted advertising, use in cyberbullying and spreading gossip and private information, create a harmful digital environment. This environment does not support children's development and well-being (including as discussed above in relation to information environments). The toll on teenagers' mental health, including an alarming increase in self-harm rates, is widely documented. Given the potential risks to the safety and well-being of children who are some of the highest users of social media, UNICEF should consider this for further review of the Guidance.

A focus is required on the harms and complexities surrounding the 'Internet of Toys'. The IoT amplifies data collection, the learning process and the communication practices that are fodder for algorithms to function. Children are monitored and surveilled in real-time and there is a constant cycle of calculating and predicting children's behaviour and shaping their development. There is a danger that this pervasive real-time monitoring and surveillance of children normalises surveillance.

The Digital Law Association suggests the following:

1. Because children learn from these toys, specific guidelines are required for the information supplied by IoT toys.

2. The content and the algorithm must cater to all sections of society, so that they represent minorities and vulnerable groups equally to dominant or majority groups.
3. An intermediary checks the content delivered by these toys.
4. Secured storage of backup data and a minimum standard for processing and transfer of data.
5. An oversight board to review security standards of the data processing and third party sharing of such data.

Disclosure and consent

Another gap in the Guidance is the disclosure and consent model in relation to children and AI. The multi-data collection mechanisms that exist within and across different platforms obscures the possibility for data principals to control this data collection. The structure is so complex that individuals are unable to make informed, meaningful and autonomous decisions required by the control basis of information privacy law. The problems caused by continuous data collection, in a framework where data is often shared with or sold to third parties, or is otherwise used for behaviour identification, raise major issues of consent and disclosure. The existing mechanism of withdrawing or curtaining data share is limited as the individual is unlikely to know what data is being collected and how that data is being used.

The Digital Law Association recommends that regulators must share the burden of privacy management rather than placing this responsibility on parents. The Digital Law Association suggests the following steps be taken (and provided in the UNICEF guidance) to make the information exchanges more rational and equitable:

1. Regular and compulsory audit of companies collecting and processing data.
2. Regular survey of parents in the form of questionnaires to assess their cognitive capability to understand privacy policies.
3. Short courses for parents, children and teachers over the mechanism of data and the meaning of consent, privacy etc.
4. Data minimisation practices should be used so that only relevant data is collected.
5. Privacy policies and other terms and conditions displayed on websites should be written in accessible language (for example, plain English) and avoid the use of confusing language such as double negatives.
6. Opt-in processes should be used rather than opt-out processes.

FIND US AT

@digitallawassociation

@DigitalLawAssoc

@digitallawassociation

@DigitalLawAssoc

CONTACT US

info@digitallawassociation.com