COUNCIL ON
EXTENDED INTELLIGENCE

The Council on Extended Intelligence ("The Council" or "CXI") is a multi-disciplinarily group gathered to proliferate the ideals of responsible participant design, data agency and metrics of economic prosperity prioritising people and the planet over profit and productivity. The Council is made up largely of engineers, computer scientists and other ICT disciplines, but we also enjoy the presence of social scientists, lawyers, policy makers and key thinkers about the intersection between technology and society. We have wide geographic representation, and think about the future of humanity and technology from a global perspective.

The Council believes that while our future will undoubtedly be shaped by the use of existing and emerging technologies there is no guarantee that progress defined by "the next" is beneficial. Growth for humanity's future should not be defined by reductionist ideas of speed or size alone but as the holistic evolution of our species in positive alignment with environmental and other systems comprising the modern algorithmic world.

Many of our Members are experts who create technological systems, therefore we understand that technology is not neutral but directly reflects the interests and values of those who pay for or control it. It is a core goal of The Council to offer metrics permitting equitable outcomes for the full diversity of citizen groups, for society, and for the planet. This requires systemic redesign of current norms so human values and ideals that promote sustainability form part of the existing and future design principles of technological systems.

We support the Age-Appropriate Design Code ("The Code") in taking a vulnerable societal group and prioritising their inalienable rights while considering their specific needs. The introduction of bespoke metrics for a specific social group is a cutting-edge approach and of interest to The Council who, above all, support the holistic application of technology in a way that is accessible and beneficial to diverse populations across all sectors of society.

Q1. In terms of setting design standards for the processing of children's personal data by providers of ISS (online services), how appropriate do you consider the age brackets as outlined in the report, Digital Childhood – addressing childhood development milestones in the Digital Environment?

The Council recognises that children of different ages and regions have vastly different interactions with technology. We support autonomous use of digital technologies and therefore welcome the idea that older children should exert growing levels of control and choice. However, all children deserve the highest bar of data protection, a form of protection that must not be confused with other notions of content control or control by another actor. The age ranges mentioned here are very appropriate.

Q1A. Please provide any views or evidence on how appropriate you consider the above age brackets would be in setting design standards for the processing of children's personal data by providers of ISS (online services).

A child's development is not linear and their activities do not necessarily present data risk according to age. For example, very young children have a developmental need for imaginative play[1] where make-believe and the suspension of reality should be unfettered by alternative realities imposed by digital technologies. The data protection considerations encountered by this age group are materially different, for example, to early teens that are at a risk-seeking development stage but have not yet developed the concept of consequence.[2]

[1] P. 32, *Disrupted Childhood: the Cost of Persuasive Design*, B. Kidron, A. Evans, J. Afia, 5Rights, June 2018
[2] *Normal Psychological Development*, MindEd

Likewise, mid-to-late teens present a lucrative market for advertisers[3] so may require more protection from commercial data gathering. The principle of looking at children in development groups is therefore welcome and necessary.

Q3. Please provide any views or evidence you have on how the Convention ("UNCRC") might apply in the context of setting design standards for the processing of children's personal data by providers of ISS (online services).

The United Nations Convention on the Rights of the Child ("UNCRC") codifies the rights necessary for a child to experience a safe and secure childhood.[4] Invoking the UNCRC is useful for the following reasons:

- It reminds us that children's rights are not context specific, but apply in all situations.
- It establishes that a child is any person under the age of eighteen.

While many of its articles relate specifically to data protection, privacy, discrimination and commercial exploitation, the UNCRC offers an overarching requirement to make decisions "in the best interests of the child". This "best interest" metric is a useful tool in establishing the data protection needs of children. Parents and trusted adults play an important and necessary part in promoting and protecting a child's rights in the digital environment. However, the Commissioner must establish data protection standards that meet the needs and fulfil the rights of all children. Therefore, it is in the "best interest of children" that the Code does not automatically rest on adult interventions but provides a regime where children's data is protected by default.

Q4. Please provide any views or evidence you think the Commissioner should take into account when explaining the meaning and coverage of these terms (areas) in the code.

The complexity of the technological environment was unanticipated at the inception of the Internet age and the values and language that are embodied within it have become increasingly commercially driven. In determining the meaning and coverage of The Code it is critical to prioritise societal, rather than technical or economic, metrics of success. Specifically, in relation to the autonomy, creativity, privacy and "best interests" of children, data in the digital economy represents a literal representation, and legal proxy for a child in real, digital, algorithmic and virtual environments. Data is able to describe a child and their interactions in tremendous detail which has significant legal and ethical implications.

Q5A-E. Please provide any views or evidence you have on the following:

1. The Council supports the introduction of the highest privacy settings as the default settings for any product or service accessing a child's data, recognising that this reverses current industry norms that set the lowest bar of data privacy for users. The default setting determines the data protection experience of most digital citizens of any age[5] - therefore "default high" would be a powerful change to children's digital experience.

[3]FONA International found that US teens (13-18-year olds) account for $208.7 billion total spending. *Purchasing Power of Teens*, FONA International, 2014. Also *Why Teens Are the Most Elusive and Valuable Customers in Tech*, Inc., 3 March 2014

[4] The Convention has been ratified by all UN member states except, notably, the United States. *Convention on the Rights of the Child*, adopted by the General Assembly resolution 44/25 of 20 November 1989

[5] A team of Microsoft researchers found that more than 95% of users had kept their settings in the exact configuration that the programme was installed in, as users assume that "Microsoft must know what they are doing" and would have features turned on or off by default, for a reason. The experiment also found that programmers and designers "almost always" changed their settings, some changing as much as 80% of the options in the programme. *Do users change their settings?* J. Spool, User Interface Engineering, 14 September 2011

Should they choose to do so, children (or parents on behalf of younger children) must be able to adjust privacy settings of services and products. However, it must be required for service providers to get further detailed agreement to data exchange policies that effectively lessen the default high - in a transparent, age-appropriate style, and with the full recognition of a child's rights (including that of their informed consent where consent is the method by which their data is being processed). For clarity, this must not be done routinely, but rather be done at the behest of a child data subject.

The Council has several members who work exclusively or partially on technological systems of privacy, including but not limited to; blockchain, (local) differential privacy, sovereign data (or zero knowledge proofs). These allow a child to share only finite amounts of data for limited times as unique transactions, thereby avoiding the long-term exposure of data for unlimited downstream use and unwanted sharing or sale by second or third parties.

We would therefore be happy to convene an expert group to advise The Commissioner in creating Principles or recommendations for a standard that will define "high" privacy, and allow children (and where applicable their parents / guardians) meaningful choice and greater control. At the same time, we would be happy to help identify the design elements that pose the greatest data risk to children.

2. We start from the perspective that a child's data belongs to the child, and that all data gathered, shared, sold or otherwise inferred or used, should be at the behest of, or, in the best interests, of that child. Therefore, data exchange should be 'service critical' (as defined by the Information Commissioner), and subject to the highest interpretation of data minimisation standards as defined by the General Data Protection Regulation ("GDPR").[6] For absence of doubt, we do not consider tick box consent, binary consent (i.e. agree or be locked out) or using a child's consent to data harvest at scale, as sufficient cause to take a child's data.

   The Commissioner should set out a definition of "best interest" that may allow an online service to collect and or share a child's data in their "best interest" (for example; a school or medical profession). Any data collected under the definition of "best interest" should be done so in a manner that is transparent, meet data minimisation principles, and allows a child to challenge accuracy and/or its use.

   Again, The Council would be happy to work with the Commissioner to define an appropriate regime for data gathering when the user is a child.

3. We do not recommend, or think appropriate, that terms and conditions and privacy notices be used to offer *any kind* of contract between an organisation (commercial, third sector or government) and a child. Terms and Conditions / privacy notices are universally unread, and therefore do not offer an equitable or even meaningful arrangement between online service and a child and often contravene the legal and cultural norms that protect children from entering into contracts.

   Emerging technological systems, such as biometric, facial recognition or voice-activated services create a further barrier to the usefulness of terms and conditions, whilst at the same time taking previously unimaginably intimate data. For example, sentiment data (emotional state) captured by home assistants,[7] heartbeat and pulse taken whilst playing games,[8] or the increasing use of affective computing methodologies.

[6] Article 5(c) the principle of data minimisation, which stipulates that personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. *General Data Protection Regulation*, 2016/679
[7] *Amazon's Alexa Wants To Learn More About Your Feelings*, Venturebeat, 22 December 2017
[8] *Press Start to Track?* J. Newman, J. Jerome, C. Hazard, American Intellectual Property Law Association Quarterly Journal, 21 August 2014

The Council would recommend the introduction of a child's own machine readable privacy terms.[9] These, created by the child (or on their behalf by a parent/carer), would encapsulate their preferences and attributes *as they see them*, could attest to their development stage, and be machine readable.

Currently the vast majority of organisations use terms and conditions, community rules and privacy notices to make agreements either by consent, or by another allowable form of data processing. If using this form of agreement they should - by means of The Code - be held to the following:

- Plain language written to the reading and conceptual capacity of lowest age-group invited to use the service

- No generalisations for collection of data, such as "to provide, personalise and improve our Products", "to communicate with you", or similar wording

- Inter-company sharing and/or acquiring personal data by commercial acquisition of a company should be on the same basis as third party sharing and only be allowable in the child's "best interests"

- Routine failure to uphold any of the published rules, terms or privacy regime (including, but not limited to, age, data collection undertakings, community behaviour) must be considered a breach of the Code

The Council would be happy to gather an expert group that could share its work with the Commissioner and in doing so offer a detailed contribution to improvements for terms and conditions, including, but not limited to, machine readable privacy terms.

4. Use of geolocation technology must be service critical (to be determined by the Commissioner), and in *all* other cases default to off.

   Geolocation presents a particular problem for children from a safety perspective when used by other users.[10] It has introduced a level of surveillance that is not in their "best interests"[11] and has the potential to profile them in ways that contravene their rights.[12]

5. We do not support automated and semi-automated profiling of children unless it meets the "best interests" test as set out by the Information Commissioner (see point 2).

6. Children do not have the capacity to comprehend paid-for activity, such as product placement, influencers and marketing. Indeed, many children struggle to understand Google results as "paid-for"[13] and/or that games will demand "in-app" purchases.[14] In addition, the rapid introduction of voice-enabled products and services will make the basis of ranking even more opaque. The Code should require Paid-for content, the criteria and ranking of services, be clear to children, including that which is sponsored and/or provided by influencers.

[9] *IEEE P7012™ - Standards for Machine Readable Personal Privacy Terms*, IEEE Standards Association
[10] *Adopted children face anguish as birth parents stalk them on Facebook*, The Guardian, 23 May 2010
[11] P. 6, *Parental Controls: Advice for Parents, Researchers and Industry*, B. Zaman, M. Nouwen, EU Kids Online, 2016
[12] *Digital Redlining: How Internet Service Providers Promote Poverty*, Truthout, 14 December 2016
[13] P. 149, *Children and Parents: Media Use and Attitudes Report*, Ofcom, 29 November 2017
[14] Executive Summary, *Study on the Impact of Marketing Through Social Media, Online Games and Mobile Applications on Children's Behaviour*, European Commission, March 2016

7. Key to The Council's interest is the use of technology to support democratic institutions citizen participation and autonomy. Strategies that deliberately obfuscate agency by manipulation of messaging, advertisements or data to influence behaviour prioritised by maximisation of profit alone, do not serve democratic ideals or human flourishing. There is growing evidence that the reward loops, social obligations and technological tricks and hooks baked into services have a direct impact on children.

   Making services addictive and then asking children to put their devices down represents an asymmetric struggle in which the technology and its manufacturers, and not the child, will be the victor.

   This is a complex area but there are ways of interrupting, grading and identifying technological regimes that would give children (and the parents and/or guardians of younger children) greater knowledge and choice over which online services they choose to utilise and trust, while giving companies the duty to offer less commercially aggressive services to children.

   Current design norms make this an urgent consideration. The Council would be pleased to provide a short paper that may help The Commissioner identify the loops of behavioural design that extend use and those that present the greatest threat to the autonomy of a child.

8. Reporting data concerns in countries and regions around the world is highly contextual and diverse. We support investment in simple user journeys in key regions to act as case studies (e.g. Estonia, India, the EU, and the US along with the UK), and applaud those companies and services that make reporting simple, effective and quick.

   To enable genuine protection and rapid response to children's data concerns, reporting should be simple and familiar. Responses should happen in a timescale that is both understood by the child, and forms part of a company's reporting duties.

   While it should be easy for a child to access information, it is absolutely certain that no child (nor non-professional adult) can be expected to fully understand data protection law. Therefore, no child (nor non-professional adult) should be expected to be able to fully enact their rights; to understand the full repercussions of the sharing, usage, or storing of their data; nor to fully recognise what they are giving up (or retaining) in regards to their data rights and evolving digital identity without access to specialist advice.

   Simpler data and identity sharing regimes, greater user data protection, and principles of symmetry and agency should lessen the need for complex complaint systems. However, it will still be necessary to provide advice, in particular, advice that can be accessed and understood by children. This should be signposted by default whenever they make a complaint.

   Additionally, the Code should provide that both the regulator and adult civil society are able to take up the data concerns of a child, a group of children or a category of children, without an individual child being a named complainant.

Conclusion

The Council on Extended Intelligence welcomes and supports the introduction of the Age-Appropriate Design Code, and recognise that this is a ground-breaking approach to data protection.

The Commissioner might also consider that:

- Children's data is uniformly and regularly provided unintentionally as schools, homes and cities become "smart" and/or "connected". Therefore "secure by design" should be the mantra of the Code.

- Companies should undertake a Children's Data Impact Assessment as a means to demonstrate full knowledge of, and compliance with, the issues laid out in the Code.

- Impact Assessments will not "hinder innovation" but actually increase market-driven, trust-based accountability that can imbue trust in relation to citizen data that has been eroded, as demonstrated by the recent case of Cambridge Analytica.

- There must be a philosophical shift to see a child as a single data subject who has rights and needs that an online service must meet. This is quite different from the current system of collecting and centralising data at any costs. There is no technological barrier to this, but one of purpose, values and ethics.

- The argument is often made that insisting on a higher bar of data protection for children will force companies to lock out young people. This is not our view. One in three people online is under 18;[15] they represent a huge market that should be met on more respectful age-appropriate terms. If some companies move out, others will move into the child/youth space. It will foster innovation and competition. Furthermore, it is self-evident that wilfully continuing a data regime that fails to meet the needs and rights of its users, in this case children, constitutes regulatory failure.

However detailed her guidance is, we suggest that The Commissioner put a final requirement in each aspect of design, that the design of service meets the "best interests" of the child. In that way, The Commissioner has a mechanism by which to interpret the spirit as well as the letter of the Code.

This definition is something that CXI would be happy to contribute to articulating.

In considering the Code, we are mindful of the fact that technology, when used to increase human flourishing, democratic ideals and the needs of diverse global populations, can be an extraordinary force for good. It is in that spirit that we commend the UK government for introducing The Code. As we have indicated, we would welcome further engagement in looking at how to articulate and advance specific areas of The Code.

[15] P. 7, *One in Three: Internet Governance and Children's Rights*, S. Livingstone, J. Carr, J. Byrne, Chatham House, GCIG Paper No. 22, November 2015

Q6. If you would be interested in contributing to future solutions focused work in developing the content of the Code please provide the following information.

CXI Representative: [redacted]

Email: [redacted]@ieee.org

Brief summary of what CXI can offer:

The Council on Extended Intelligence would be happy to convene an expert group to advise The Commissioner on any of the issues raised in the Age Appropriate Design Code, including the specific items mentioned above:

- *Create Principles or recommendations for a standard that will define "high" privacy, and allow children (and where applicable their parents / guardians) meaningful choice and greater control.*
- *Define an appropriate regime for data gathering when the user is a child.*
- *Offer a detailed contribution to improvements for terms and conditions, including, but not limited to, machine readable privacy terms.*
- *Identify the design elements that pose the greatest data risk to children. Current design norms make this an urgent consideration. The Council would be pleased to provide a short paper that may help The Commissioner identify the loops of behavioural design that extend use and those that present the greatest threat to the autonomy of a child.*
- *Contribute to a definition of the "best interests" of a child mindful of the technological context in which it will be needed.*

Q7. Please provide any other views or evidence you have that you consider to be relevant to this call for evidence.

We encourage the Commissioner not to be deterred by a "technical 'can't" when it is, in fact, a "corporate 'won't" on the part of tech companies. The Council has considerable expertise in most of the aspects of design that the Commissioner has set out. We have indicated in this document specific areas in which our expertise could usefully support the development of the Code, and additionally The Council's members would be happy to meet with the ICO and/or to set up a technical group to support the Code process, over the next few months.

The Code applies to all online services "likely to be accessed by a child". We would urge the Commissioner to also consider *all online services likely to access a child's data*, which is at this time, a more urgent consideration.

Issues of privacy are compounded by questions about the impact of AI-enabled toys on cognitive development. AI enabled devices are increasingly able to manipulate and addict users, to which children are more susceptible. This is particularly salient given the prevalence of bias and commercial purposes baked in AI, to which children are less attuned than adults. Likewise, it raises the issue of how children (or parents of children) playing with another child's device prevent gathering of data. Data gathered from a child from when he/she first opens his/her mouth and speaks until eighteen years of age offers unprecedented access to a child for unscrupulous individuals and companies.

The Code is a welcome and sophisticated tool for establishing equitable data agreements between online services and the societal group whose long-term data is most at risk: children. Additionally, the Code should recognise the widespread use of children's data in video-gaming environments, including the use of Augmented and Virtual Reality as part of online services' platforms. These new reality environments are setting precedents for human data collection at a scale and level of detail that will, in time, challenge the interests of humans against those of intelligent machines (and those who control them). This data is, currently, casually collected with no oversight.

This is a position paper of The Council on Extended Intelligence (CXI).

Signatures below are provided in Members' personal capacity and do not necessarily represent the official position of the CXI member institutions.

Names: