

Data protection safeguards for children ('digital age of consent')

Proposals from CARI on the Consultation paper from the Department of Justice and Equality

Authors: Eve Farrelly, Child Accompaniment Support Service Manager
Lynette Bradshaw, Court Accompaniment Team Leader

In considering its view on the appropriate digital age of consent CARI looked at the right to privacy and autonomy online versus the right to protection from online activities that could become risks in the real world. There were several issues that CARI considered:

1. Commercialisation of children
2. Development of children
3. Cyber bullying and sexual exploitation
4. Child deception on age and its consequences, and
5. How it would be enforced

Commercialisation of children

The growing commercialization of childhood which is increasing at a high rate and to essentially protect children from the following uses of their data

- geo-location tracking,
- data profiling,
- embedded marketing
- cross-platform convergence of data

Older children should have more opt-in, transparency and individual control over their personal data. They should also be aware of how their data could be used as bullet-pointed above. This type of use would typically outstrip both parents' and children's digital literacy.

Development of Children

One aspect that needs attention is the effects of social media from a developmental perspective. How can children aged between 8-11 years' cope with many followers?

Cyber psychology would state that digital relationships that exceed 150 lead to social stress and exhaustion in adults. How would children aged 13/14 cope with networks far exceeding 150? (Dr. Mary Aiken, Cyber Psychologist)

With respect to Erikson's Identity Formation¹ which happens between the ages of 9-13, another challenge that young people face is the divide that can occur between their real self and the idealized self that they create on social media. and its direct connection to the young person's sense of self.

Cyber bullying and sexual exploitation

The Swedish Data Protection Board ¹ conducted a study of 522 participants aged between 15-18 and found that the majority had experienced unkind words written about them, around a quarter were sexually harassed online, and half of those on Facebook had had their account hijacked. Furthermore, it found that the young people had a generally good understanding of privacy issues.

From a CARI perspective and as an organisation who has worked with vulnerable children for over twenty-five years, our understanding of levels of maturity must be balanced with the actual knowledge that young people have. We must consider their usage of social media sites in a child being open to online grooming and cyber bullying. The statistics highlighted by CARI over the last number of years shows an increase in sexual assault on teens by teens. This figure increased by 43% from 2012 to 2014¹. The over sexualisation of children and young people through online activity and social media needs to be considered.

Child deception on age and its consequence

A potential negative impact of keeping the age at 16 is that it may lead some teenagers to lie about their age to create or maintain an account, potentially putting them in more danger by pretending to be older than they are. Janice Richardson, former Coordinator of the European Safer Internet Network, said that denying the under-16s access to social media would "deprive young people of educational and social opportunities in a number of ways, yet would provide no more (and likely even less) protection".

How would it be enforced?

Although it is clear what the penalty will be for organisations that do not adhere to this Directive, there does not appear to be much detail or clarity on how this will be enforced?

Children are protected under the EU data protection law, as are adults. Are children aware of this? Do they know how to exercise this?

A study from Ofcom² the communications watchdog in the UK, found that teenagers couldn't tell the difference between search results and adverts placed around them, demonstrating that young people's understanding of how the web works, and the role of their personal data, is not always sufficient – and perhaps insufficient to represent real, informed consent.

¹ CARI Annual Report, 2013 & 2014.

² <http://theconversation.com/at-what-age-should-teenagers-pass-the-digital-age-of-consent-52587>

Informed consent is paramount when considering online activity of children and the balance that should be sought between a child's right to making their decisions regarding their online activity on social media sites compared to their protection of their personal data.

UN Convention of the rights of the child identifies that if the child is unable to exercise these rights then the onus lies with the parent/carer/guardian of that child. Furthermore, Article 5 of the UN Convention of the rights of the child allows for the "evolving capabilities" of the child thus allowing them to be proactive in their choices made online on social media sites. Article 12 in the UN Convention of the rights of the child states, when a child can form their own decision they should be afforded the right to express these views freely and carry the weight consequently. Surely leading to the question; Where do children think the digital age of consent threshold should be set?

Within the EU this threshold will be set at sixteen. Is this the ideal age?

CARI view

Considering the issues around informed consent and the real-world consequences of online activity, education is paramount. CARI would like to see the responsibility on social media companies to fund educational and awareness campaigns and engage with relevant organisations and stakeholders to promote safe online activity.

CARI's conclusion from looking at the above is that thirteen is far too young, and sixteen may be a little too old and problematic. A balance must be struck between participation and protection and the reality of the dangers that bringing the age to sixteen may incur for children, as outlined above. CARI is recommending that the statutory age of consent threshold ('digital age of consent') should be set at fifteen, with the supports of education.
