Parental consent, the EU, and children as “digital natives”

International Data Privacy Law

International Data Privacy Law takes a global approach and considers developments and data privacy case law from the UK, Europe, the US and around the world.
Children have become heavy new media users. Empirical data shows that a number of children accessing the internet – contrary to the age of users – is constantly increasing. It is estimated that about 60% of European children are daily or almost daily internet users (http://www.lse.ac.uk/media%40lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/D4FullFindings.pdf), and therefore, by many they are considered to be “digital natives”.

However, in our view, the use of this “digital natives” concept is misleading and poorly founded, and is based on the assumption that children are quick to pick up new technologies. A recent EU Kids Online study (http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/DigitalSkillsShortReport.pdf) invalidates this assumption. The study shows that even though children actively surf on various online applications, they lack digital skills such as bookmarking a website, blocking unwanted communications, and changing privacy settings on social networking sites. Many children are not capable of critically evaluating information and changing filter preferences. Interestingly, the lack of skills to perform specific tasks while being online does not impinge on children’s beliefs in their abilities – 43% of surveyed children believe to know more about the internet than their parents. At the moment, no correlation between this proclaimed self-confidence and their actual understanding of how internet works can be done due to the lack of data. Nevertheless, it is worth questioning whether, and to what extent, it is reasonable to expect that children understand the implications of their behaviour and what measures could mitigate children’s online risks in the most efficient and effective way.

It is probably closer to the truth to say that, in terms of privacy and data protection awareness, children are anything but “digital natives”.

Indeed, children’s actions online are being recorded, commercialised and serve for the purposes of behavioural advertising without them actually realising. This media illiteracy is tackled by awareness raising campaigns and policy measures on domestic and EU levels. However, it seems that these measures only partially address the challenges posed by children’s online engagement.

Image credit: Classroom laptops, by R. Nial Bradshaw. CC-BY-2.0 via Flickr (https://www.flickr.com/photos/33227787@N05/14229163349/in/photolist-nFobwz-gXGgKd-cRJ9fL-fGDgzc). This image has been cropped.

The European Commission (EC) seems to be in favour of legislative measures providing for a stronger legal protection of children’s personal data in the online environment. In Article 8 of the proposal for the General Data Protection Regulation (http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf), the EC introduces verifiable parental (or custodian) consent that would serve as a means of legitimising the processing of a child’s personal data on the internet.

Article 8 of the proposal foresees that parental consent would be required in cases where the processing operations entail personal data of children under the age of 13. The age of 13 would be the bright-line from which the processing of children’s personal data would be subjected to fewer legal constraints.
In practice, this would divide all children into two groups; children that are capable to consent (i.e. 13-18 year olds) to the processing of their personal data and children that are dependent on parental approval of their online choices (i.e. 0-13 year olds). Drawing such a strict line opposes the stages of physical and social development. Also, it requires the reconsideration of the general positive perception of the proposed parental consent from a legal point of view.

In particular, it is necessary to evaluate whether the proposed measure is proportionate and whether it coincides with the human rights framework.

In a recent article published in the International Data Privacy Law Journal, we have analysed the proposal to distinguish between children younger and older than 13 years and found many practical and principled objections. Apart from the practical objections, which are often self-evident (e.g. what about the protection of children in the age group from 13 to 18 year old? How to ensure the enforcement of the proposed parental consent?), there are several fundamental problems with the proposed 13 years-rule.

The bright-line rule, which would require data controllers to obtain parental consent before processing personal data of children aged under 13, seems to be incompatible with the notion of evolving capacities. The proposed measure is based on the assumption that from the age of 13 all children are able to provide an independent consent for the processing of their personal data in the online environment. The proposed Article 8 ignores the fact that every child develops at a different pace and that the introduction of parental consent does not ensure more guidance regarding online data processing. We also regret that Article 8 in its current form doesn't foresee a way in which children could express their own views regarding the data processing operation; the responsibility to consent would rest exclusively with a parent or a legal guardian. This set-up opposes the idea of children's participation in the decision-making process that concerns them, an idea anchored in the UN Convention on the Rights of the Child (UNCRC) and that is recognised by both the EU and its Member States.

Finally, our analysis suggests that children's rights to freedom of expression and privacy may be undermined, if the proposed parental consent is introduced. As a result of Article 8, children's access to information could become limited and dependent on parents. Also, the scope of their right to privacy would shrink as parents would be required to intervene in children's private spaces (e.g. gaming accounts) to make informed choices. Therefore, it can be observed that the introduction of parental consent contradicts the key principles of human rights law enshrined in the UNCRC.

Featured image credit: Student on iPod at school. Photo by Brad Flickinger. CC-BY-2.0 via Flickr.

Lina Jasmontaite works as a researcher at the Katholieke Universiteit Leuven, ICRI-CIR (Interdisciplinary Centre for Law & ICT) based in Belgium. Paul De Hert is Professor at the Vrije Universiteit Brussel, LSTS (Interdisciplinary Research Group on Law Science Technology & Society) and at the Tilburg Institute for Law, Technology & Society based in the Netherlands. Lina Jasmontaite and Paul De Hert are the authors of "The EU, children under 13 years, and parental consent: a human rights analysis of a new, age-based bright-line for the protection of children on the Internet" (available to read for free for a limited time) in International Data Privacy Law.

What to read next

| Requiring Local Storage Of Internet Data Will Not Protect Privacy (http://blog.oup.com/2013/12/Data-Security-Privacy-Storage-Law/) | Protecting Children From Hardcore Adult Content Online (http://blog.oup.com/2014/01/Protecting-Children-From-Hardcore-Adult-Content-Online/) |
| DECEMBER 6TH 2013 | JANUARY 27TH 2014 |
