“It’s none of their business!” Children’s understanding of privacy in the platform society

We live in a platform society. What we do online is immediately shared within a lucrative global data ecology and managing our “privacy settings” does not impact on data privacy. So how can we expect children to take responsibility for their privacy online or understand data commercialisation and profiling? Sonia Livingstone talks about her research with Mariya Stoilova and Rishita Nandagiri in this post based on a short essay for the 5Rights Foundation’s recent publication on The Future of Childhood in the Digital World – all the essays are open-access, and you can also watch the launch chaired by Baroness Beeban Kidron.

“We all have our own privacy settings. So, when it comes to your privacy on Facebook, we think you should have the same controls.”

So proclaimed Facebook’s 2019 campaign to recover collapsing public trust following Cambridge Analytica. One advert showed the user’s privacy options (public, friends, close friends, only me) with the last option ticked. But choosing ‘only me’ makes no sense in a networked world – not only does no-one want social isolation, but ‘only me’ does not solve the problem – illustrated by Cambridge Analytica – where personal data were misused for commercial and political purposes. Whatever you tick, none of your actions are private from Facebook.

Privacy from whom?

The Facebook advert illustrates a wider confusion in society between interpersonal privacy and organisational privacy – often now called data privacy. Parents, teachers, government and businesses tend to talk to children as if privacy only means privacy from other people. When children are accused of lacking a sense of privacy by sharing their personal information with all and sundry, when parents worry about cyberbullying or grooming, even when the media panic about accidental data leaks from the ‘internet of toys’ or smart home devices, the focus is children’s interpersonal privacy and its safety implications. Policy responses centre, respectively, on better e-safety education, parental awareness and responsibility, and the regulation of product security. These are all important and urgent.

But adults say little to children about how to protect their privacy from their school, doctor, or police or from commercial actors (many of whom are now also in the personal data business). Yet much of what a child does online – their searches, posts, likes or views – is immediately shared within a lucrative global data ecology. So if they are an Instagram or WhatsApp user, the child’s data will be shared with dozens of Facebook’s partners, since user profiling is the currency for real-time advertising auctions that target users. Attending to one’s privacy settings will not impact on data privacy, where there is no real ‘only me’ option.

This isn’t children’s confusion but ours. When adults talk to children about privacy, they assume an interpersonal context. For instance, to manage their online privacy, children are advised to choose who can see particular posts, and to delete messages that they regret or that might upset others. These are tactics for interpersonal privacy only, and they are ineffective for managing their privacy in institutional and commercial contexts. From Instagram or Snapchat or Amazon – and, probably, from their school or health provider – there is no realistic option to choose, to consent, or to delete.

Children’s understanding of their data privacy

Date originally posted: 2020-07-15

Permalink: https://blogs.lse.ac.uk/parenting4digitalfuture/2020/07/15/privacy-in-the-platform-society/

Blog homepage: https://blogs.lse.ac.uk/parenting4digitalfuture/

No wonder that in our participatory workshops with UK 11-to 16-year olds, we heard children extend what they know of interpersonal relations to the operation of platforms. For example, they might talk trustingly of Instagram because so-and-so’s father works in technology, and he would surely play fair. They assume ethical reciprocity – if they would never track someone without their knowledge or keep images against someone’s will, why would a company? Or they assume that the tactics that keep their activities hidden from their parents or enemies (pseudonyms, ghost mode, incognito search, clearing one’s history) also keep their data private from companies.

Children’s tendency to trust these organisations is also down to us. Who does not teach their child to trust their school or doctor or even the shopkeepers and other commercial services with which they have early dealings? Is the solution to privacy in a datafied world really to teach children to distrust? Meanwhile, schools teach children little or nothing about the global nature and complex proprietary practices of the digital ecology or how this might shape their future. When they find out, they are outraged, saying: it’s creepy, platforms shouldn’t be poking around in my online contacts, and, tellingly, it’s none of their business! If only.

Shifting the burden of privacy protection from user to service provider

But even if we taught children about platform business models, it is unlikely to enhance their agency when the choice architecture is against them. The challenge of protecting privacy in a digital world goes beyond expecting children to understand and manage their personal data. Increasingly, the challenge is one of redesigning the conditions under which their data are collected, inferred, profiled and used by others. These conditions are, currently, systematically opaque to users. How can we expect children to be responsible for their data privacy when their parents, teachers or even policy experts don’t understand it? Even if transparency were dramatically increased, what use would it be if not linked to granular, meaningful and easily-implemented choices about what to share, with whom, and for what?

Children cannot learn to make wise choices when adult society systematically talks to them about their data and privacy online in purely interpersonal terms. We must stop advising children and parents that they can and should control the flow of their data in circumstances when they cannot, or when the result would be a significant disadvantage or exclusion. We should call out businesses which claim they respect people’s privacy when they do not.

We have created a situation in which children learn that they don’t matter, that companies don’t care what they want. It is time to demand that institutions and businesses redesign their digital offer in ways that serve children’s best interests. And for society – especially governments and regulators – to hold them to account.

This post gives the views of the authors and does not represent the position of the LSE Parenting for a Digital Future blog, nor of the London School of Economics and Political Science.

Featured image: photo by Retha Ferguson on Pexels

Date originally posted: 2020-07-15

Permalink: https://blogs.lse.ac.uk/parenting4digitalfuture/2020/07/15/privacy-in-the-platform-society/

Blog homepage: https://blogs.lse.ac.uk/parenting4digitalfuture/