Privacy matters when enabling a safer online experience for children

By Kruakae Pothong & Sonia Livingstone

Children's life these days are almost digital by default. With moves towards the metaverse, the digital and physical worlds will become more intertwined, and the impact of digital engagement is likely to feel more real than ever in both digital and physical environments. Among the many proposals that will be promoted on Safer Internet Day, it is important to pay attention to data protection. Data protection may seem a dull topic – certainly, it doesn't capture the headlines like safety does. But data – linked to the right to privacy – are the means by which many risks to children's safety are facilitated.

On Safer Internet Day, let's also pay attention to data and privacy

To make the internet safer for children, we first need to understand the risks that children are exposed to when they go online. These risks can be classified according to the 4Cs:

- Content risks (e.g., violence, pornography, self-harm, disinformation) are promoted to children through algorithms that operate on their data traces and digital footprint. For example, third-party cookie surveillance could result in children being served pro-anorexic content.
- Contact risks (e.g., grooming, stalking, harassment) can be facilitated by unauthorised access to or misuse of children's personal data or social media profiles. For example, personal information in users' profiles, their location and social networks are used to suggest random contacts to children without safety vetting.
- Conduct risks (e.g., cyberbullying, coercive sexting) are also facilitated and amplified by the affordances of social media platforms. For example, anonymous accounts can be used to facilitate cyberbullying.
- Contract risks (e.g., commercialisation of children's data and unfair or unclear terms of use) variously stem from data protection failings, misuse of children's personal data and manipulative design techniques, among other problems, infringing children's rights to privacy and freedom from commercial exploitation. An example includes a free mobile game or application that tempts children into making in-app or in-game purchases to fully enjoy the applications or progress in the games.

Collectively, exposure to these four categories of online risks is not in children's best interests (Article 3, UNCRC). All are enabled by privacy violations, which is why CO:RE's 4Cs framework treats this as a cross-cutting risk. And all require intervention by stakeholders to ensure the realisation of children's rights, in accordance with the UN Committee on the Rights of the Child's general comment 25.

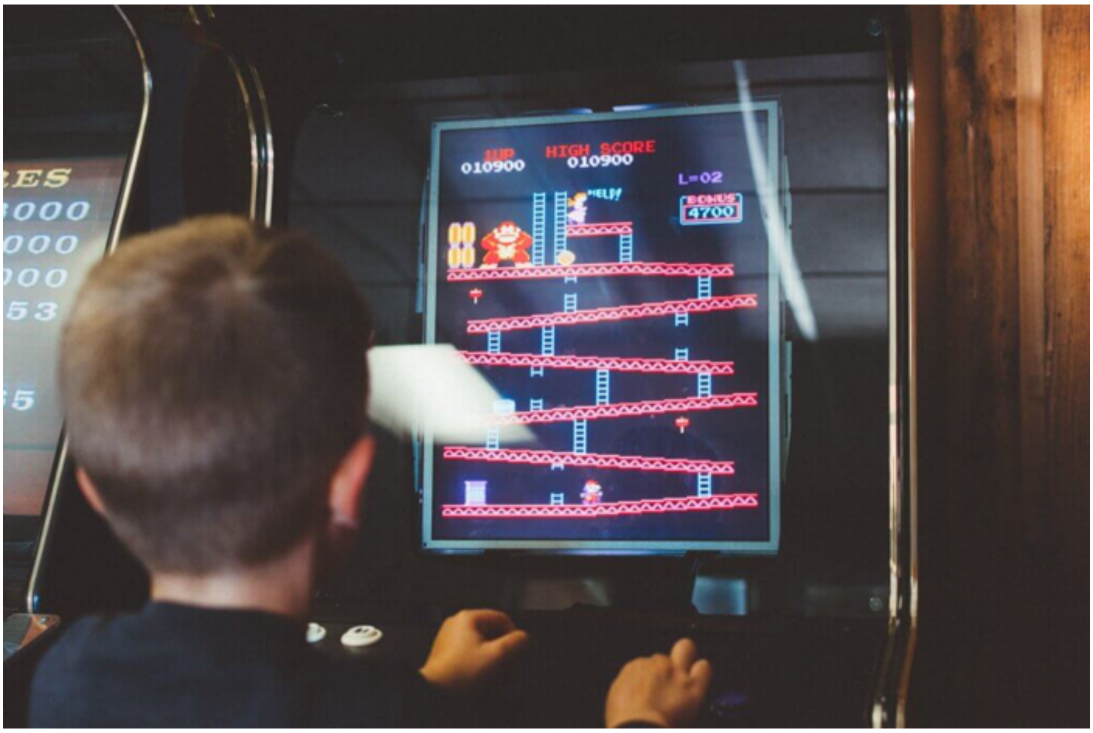


Photo by Kelly Sikkema on Unsplash

Children are sometimes aware of the relation between safety and privacy

In July 2022, the Digital Futures Commission held 20 workshops with 143 children aged 7 – 14 in four schools across Greater London, Yorkshire and Essex about how they see their rights being realised or infringed in the digital environment. In every workshop, we heard of children's experiences with content, contact, conduct and contract risks. Sometimes these were linked to problems of data protection and privacy.

> "I sometimes feel a little bit not safe because sometimes when I'm playing a really, really fun game then a little advert comes on…. it might look really fun, but then I always start thinking, what if that game's not safe, what if that's just a trick?" (Girl, 7-8 years old, Greater London)

> "TikTok isn't that good because anyone can add or see your account unless it's on private." (Child, 11-12 years old, Yorkshire)

> "Streamers sometimes get the cops called on them just because people think it's funny to do. Because if someone knows your address they can say, …someone is being held hostage at this house, but there isn't actually any hostages at that house." (Boy, 12-23 years old, Essex)

> "Sometimes I feel unsafe because sometimes you don't know when you have to pay something. And you might just press it and something pops up and then you just pay this, or pay this." (Girl, 7-8 years old, Greater London)

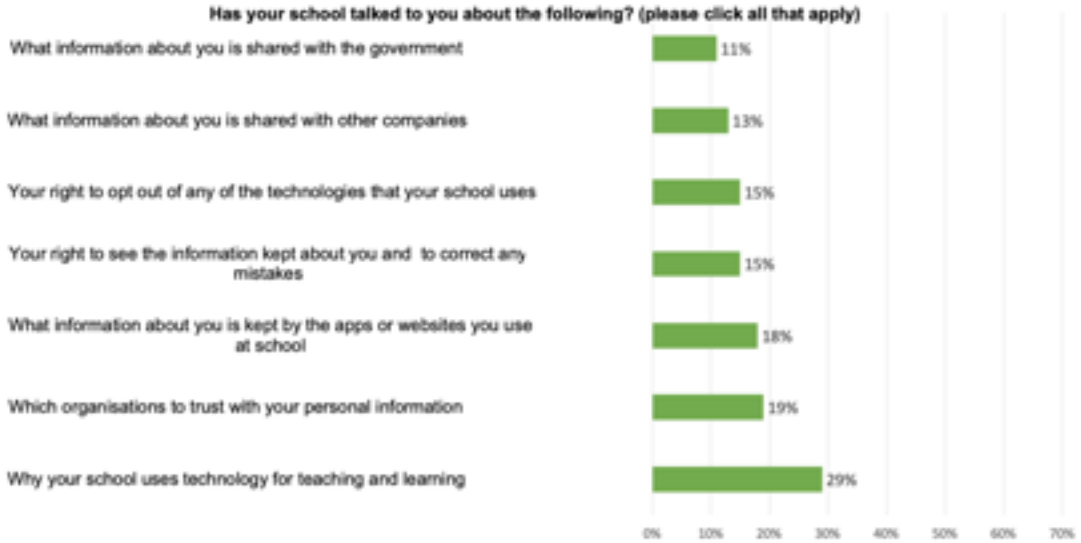
To address safety risks, children called for greater privacy online:

> "Snapchat using your location but giving you a choice if you want to share it." (Child, 13-14 years old, Yorkshire)

Schools could do more to build awareness and critical understanding

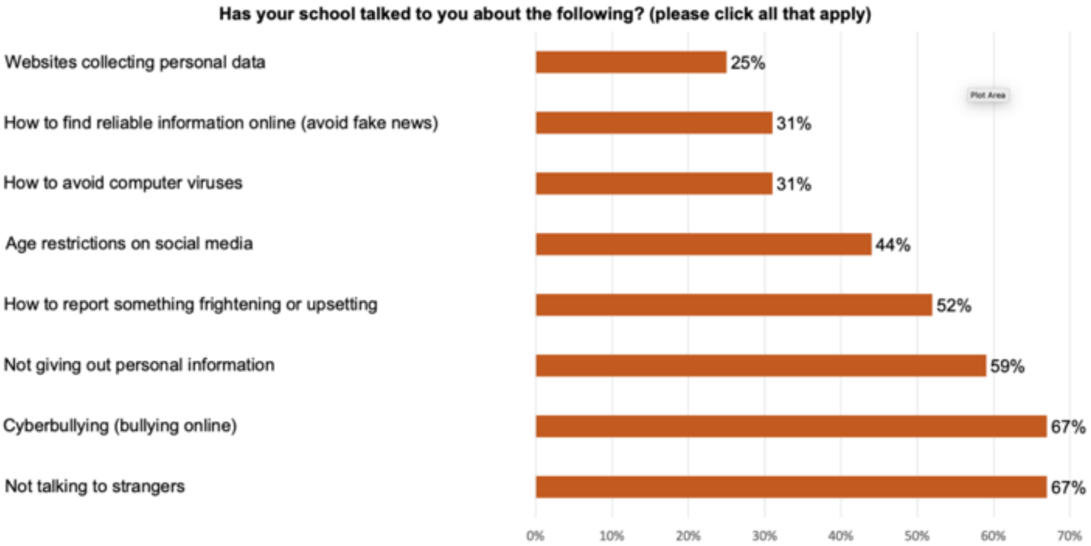
Our Digital Futures Commission nationally representative survey with 1,014 school children aged 7 to 16 across the UK found that schools offer fewer opportunities to talk about data processing than they do online risks.

Only 19% of children said their schools had talked to them about which organisation they could trust with their personal data. Just 15% said their school had talked to them about their right to see the information kept about them and to correct any mistakes. And 13% had been told which information about them is shared with other companies.



Yet, as our deep dive into EdTech made clear, school data protection practices can expose children to the onward sharing of their data in the commercial ecosystem in ways they cannot control.

By contrast, questions asked in the same survey by Family Kids & Youth for their annual Wellbeing and Internet Study found that schools offer children much more advice about conduct risks (67% talked about cyberbullying) and contact risks (67% talked about not talking to strangers).



In effect, schools appear focus on what children can be expected to control (e.g., giving out personal information) but less on what they cannot control (e.g., data shared about them with companies). Yet, when the design interfaces of virtual platforms allow children to access other services with inferior privacy safeguards, children can be subjected to third party cookie surveillance and targeted for inappropriate advertisements

Legal protections for children's online safety

Legal protections are spread across three groups of legislation: online safety, data protection and consumer protection:

- The Online Safety Bill mainly addresses content and conduct risks, prescribing “children’s risks assessment duties” to “user-to-user services likely to be accessed by children”. The bill also offers some safeguards against contact risk, requiring digital providers in scope to assess the risk that “functionalities enabling adults to contact other users (including children) by means of the service.”
- The UK Data Protection Act 2018 and UK General Data Protection Regulation (GDPR) are key to protecting the right to privacy in digital contexts, and the Age Appropriate Design Code specifically adds protections for children to prevent their data being used in ways that share their location, nudge them in harmful directions or are against their best interests.
- The UK Consumer Protection from Unfair Trading Regulations (CPUTR) 2008 and the Consumer Rights Act 2015 protects children from contract risks that stem from unfair and misleading commercial practices such as in-apps or in-game purchases.

Joining up privacy and safety through policy, education and design

The recently formed Digital Regulation Cooperation Forum promises a more joined up approach to online safety and data protection henceforth – we look forward to the fruits of this new effort and to greater efforts to ensure that “online service providers comply with both online safety regulation and data protection regulation.”

It is less clear how privacy and safety will be better integrated into the school curriculum. The national curriculum in England’s specification for computing mentions ‘keeping personal information privacy’ and urges children to use technology responsibly, but says little about teaching the critical knowledge needed to understand how businesses use personal data to drive profit (or, however inadvertently, to undermine children’s safety).

In our work at the Digital Futures Commission, we draw attention to the challenge of design. In April we will publish our Child Rights by Design Toolkit, crunching the 54 Articles of the UN Convention on the Rights of the Child into 11 principles that we map to a universally accepted design process – the double diamond – to inform the rights-respecting design of digital products and services. This toolkit will combine laws, regulations, standards and good practices relevant to privacy, safety, and other children’s rights into one document. Coming soon!

Originally posted on https://digitalfuturescommission.org.uk/ on February 7, 2023 .