CHILDREN'S PRIVACY AND DIGITAL LITERACY ACROSS CULTURES: IMPLICATIONS FOR EDUCATION AND REGULATION

By Sonia Livingstone, Monica Bulger, Patrick Burton, Emma Day, Eva Lievens, Ingrida Milkaite, Tom De Leyn, Marijn Martens, Ricarose Roque, Katharine Sarikakis, Mariya Stoilova and Ralf De Wolf

Digital technologies increasingly provide the infrastructure for education, political and cultural participation, work and family life. This makes them a crucial means by which people can exercise their rights and have their needs met. One such right, to privacy, is particularly threatened by the adoption of new forms of data collection, processing and surveillance enacted by businesses, the state (including education, health, law enforcement and welfare systems) and the general public (including the family). Recognizing children's rights as set out in the UN Convention on the Rights of the Child (UNCRC, 1989), and their relevance to digital technologies as explained in the UN's *General Comment No. 25 on Children's Rights in Relation to the Digital Environment* (UN Committee on the Rights of the Child, 2021), this chapter examines the implications of digital technologies for children's privacy, both as a human right and as a means of exercising other rights in a digital world.

A child rights approach focuses on the responsibilities of a government as the primary duty bearer. While there are many actions open to governments, protecting children's privacy has become, in part, a task for educators, newly charged with explaining the digital world to their students so that they can, supposedly, protect themselves. From the basics of access to and operation of devices through to a critical grasp of how personal data is processed, digital literacy is crucial to inclusion, equality and other rights in a digital age. For this reason, and to promote the full range of human rights in relation to the digital environment, digital literacy is a policy priority in the EU (Carretero et al., 2017) and internationally (Nascimbeni and Vosloo, 2019), recognized as important for a host of democratic and social justice outcomes. However, the imbalance in power between platforms and individual users sheds a critical light on the expectation that the right to privacy depends on individuals taking on the responsibility for acquiring digital literacy. Such a burden is even less appropriate when it comes to children. Consequently, protecting children's privacy is also a task for legislators and regulatory authorities, charged with establishing and enforcing privacy-respecting frameworks within which the government itself, as well as businesses and other actors, including individuals, should act.

Neither the educators' nor the legislators' task is easy, and in many parts of the world, each is hardly begun. Moreover, in ways that are rarely examined, they are in certain ways interdependent. On the one hand, privacy and data protection regulations work more effectively when data subjects (that is, users, children, the public) are educated to be informed, critically aware and capable of giving meaningful consent. On the other hand, education is best facilitated when its subject matter is knowable – orderly, transparent, documented and regulated. At present, most people, children or adults, have a poor understanding of how digital systems work, including the commercial data ecology. This

poor understanding is both cause and effect of people's relative exclusion from opportunities to transform, generate or intervene in such systems (van Dijk and Hacker, 2003; Chakravartty and Sarikakis, 2006). The problem is exacerbated by the fact that regulatory solutions (such as requirements for transparency and accountability of platforms and data brokers) do not work well in practice and are insufficiently enforced (Milkaite and Lievens, 2020). During the COVID-19 pandemic, the lack of public understanding regarding data processing played a key part in the confused debates regarding the surveillance potential of government-sponsored health-tracking, the legitimacy of the data-mining strategies of the educational technologies rolled out for home learning, or the difficulties in preventing 'anti-vax' and other disinformation.

In this chapter we examine the interdependences between educational and regulatory solutions for children's privacy in a digital world. We ground our analysis in our qualitative research with children in diverse countries exploring how they perceive privacy as an idea, how this in turn manifests in their privacy practices, and the changes they call for, before suggesting ways in which education and regulation could be more responsive to children's needs.

THE CO-EVOLUTION OF EDUCATION AND REGULATION APPROACHES

Both educational and regulatory 'solutions' to digitally mediated threats to children's privacy have their particular histories and legacy. Digital literacy initiatives, the 'heir' of the technological literacy debates of the 1990s (see, for example, Fulton, 1997), as well as the media literacy debates of preceding decades (Buckingham, 2007), have co-evolved with the technological innovation. Digital literacy initially focused on the access and resources that inhibited or enabled people to be technologically fluent (and affluent). Although research has since expanded expectations beyond the functional use of technological interfaces, the critical rethinking needed to overcome instrumentalist approaches and encompass the dynamic spectrum of critical capabilities required for digital and social justice (Aviram, et al., 2006; Raffaghelli, 2020) has only partially been realized (Livingstone et al., 2008). While in the past it could be expected that people could gain a degree of critical knowledge of media and information systems, the complexity of today's technological context is increasingly challenging.

In short, early digital literacy education developed for a simpler technological world and has not kept pace with innovation or regulation. The level of literacy demanded in today's technological complexity, even to manage the interface (for example, by adjusting or changing default privacy settings) requires a significant investment of time, let alone to grasp the privacy implications of technological design or the data ecology. Moreover, the economic and educational environments in which children are growing up are highly variable cross-nationally, resulting in considerable inequalities in the educational resources available to children for digital access and digital literacy (Nascimbeni and Vosloo, 2019). Expecting a thorough understanding of digital environments from ordinary citizens, especially children, would be a serious error in regulatory thinking.

Since 2000, the most influential legislation internationally has been the US Children's Online Privacy Protection Act (COPPA), which established the data collection regime under which the major US companies (notably, Facebook, Apple, Amazon, Microsoft and Google) operate regarding children. COPPA imposes certain requirements regarding notices and collecting verifiable parental consent on operators of websites or online services that direct their services to children under the age of 13 or who have actual knowledge that they are collecting personal information from a child under the age of 13. The European Union's (EU) regulatory response has been far more wide reaching in scope, applying to all EU citizens. The individual's right to data protection being recognised as a separate fundamental right (Article 8 of the EU's Charter of Fundamental Rights, 2012), the EU established specific legal requirements and obligations to realize this right in the General Data Protection Regulation (Regulation EU, 2016). This is possibly the strictest data protection framework internationally and is influential well beyond Europe. The GDPR makes provision for children in Recital 38:

> Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.

Significantly, the rationale for extra protections for children is their presumed awareness regarding uses and abuses of their personal data. This represents but one of many challenges facing both those who process children's data and those who need to enforce the GDPR. Beyond Recital 38, references to children throughout the GDPR are few, and provisions are notoriously vague. Looking more widely, legal contexts around the world leave considerable room for interpretation for actors processing data in regard to their specific obligations towards child data subjects (Milkaite and Lievens, 2019). In this context it is important to note that the USA jurisdiction refers primarily to 'data privacy' while the European regulatory frameworks set up 'data protection' rules. In this chapter, we refer to privacy as encompassing both data privacy and data protection, since 'privacy' is the notion that children use most often, including when they discuss the collection, processing and control of their personal data in digital contexts. Where we explicitly discuss the regulation thereof, we refer to data protection.

INCLUDING CHILDREN IN MATTERS THAT AFFECT THEIR LIVES

Today's children are the first generation to grow up with a ubiquitous and omnipresent reliance on digital technologies for learning, communication, health, leisure, work and politics. Hence the imperative for society to attend to the rights and needs of its young citizens in relation to the digital environment, as set out by the UN Committee on the Rights of the Child (2021). Article 12 of the UNCRC concerns children's right to be heard on all matters that affect their lives, and to have their views given due weight by relevant decision makers. Yet children are rarely invited to participate in formal consultations on the

development of legislation and policy relating to education or regulation, and they have little opportunity to co-construct the processes and environments that affect them, although child rights advocates have developed effective methodologies for such purposes (Lansdown, 2014).

Only recently has literature sprung up asking what children understand about their privacy in digital contexts and what changes are needed to realize their rights (Stoilova et al., 2019; De Wolf and Vanden Abeele, 2020). Children's lives differ on many dimensions, and particularly relevant to their privacy are familial and cultural values, education (especially digital literacy curricula), public debate about technology, and trust in government. Using a common methodology that combined research and consultation with children, this chapter explores children's voices and perspectives on their privacy and the uses of their personal data in relation to the digital environment in very different parts of the world – Austria, Belgium (Flanders), Cambodia, Indonesia, Malaysia, Thailand, the UK and the USA. In each context, the researchers began by asking children about their online activities and their unprompted perceptions of privacy and digital practices (such as selecting apps, checking age restrictions, reading terms and conditions and changing privacy settings). We then discussed more complex questions, such as types of data they share and with whom, gradually building an account of children's online behaviour and enabling discussion of less thought-of areas such as data harvesting and profiling A particular focus was placed on listening to what children had to say, treating them as experts on their own technology use but also attending to their struggles and concerns (Livingstone et al., 2019).

Conducted during 2019–20, the studies include 690 children living in high- and low-income countries, ranging from marginalized children living on the street to children from well-resourced, upper middle-class families. In East Asia (Cambodia, Indonesia, Malaysia and Thailand), we interviewed 34 focus groups with 301 social media users aged 11–19 as part of a broader study about digital technology with children with disabilities, street children, refugees, juvenile offenders and survivors of sex trafficking (Bulger and Burton, 2020). In the UK, 28 focus group interviews were conducted with 169 11- to 16-year-olds around the country to explore their understanding of interpersonal, institutional and commercial privacy in digital contexts (Stoilova et al., 2019). In Austria, in the Vienna metropolitan area, we talked with 18 focus groups of 116 children aged 8–9, 11–12 and 12–16, drawn from schools that represented the ethnic and socioeconomic make-up of the city (work in progress). The study in Belgium (in Ghent, Flanders) included 16 co-design workshops with 83 children aged 9–10 and 11–12 in two public primary schools (work in progress). In the USA, we interviewed 15 sets of parents and children (41 in total) in an upper-middle class community in Colorado (work in progress).

CHILDREN'S PRIVACY OFF- AND ONLINE: MEANINGFUL INTERPERSONALLY AND CONTEXTUALLY

It is to be expected, perhaps, that abstract notions of privacy cannot be readily deciphered by children of all ages. Yet even young children express a clear understanding of privacy as important – a matter of controlling access to oneself, of the interior world, of dignity (Laufer

and Wolfe, 1977). As theorized in relation to both digital and non-digital communication contexts, privacy is "neither a right to secrecy nor a right to control but a right to *appropriate* flow of personal information" (Nissenbaum, 2010: 127). According to Gavison (1980: 423), "the reasons for which we claim privacy in different situations are similar. They are related to the functions privacy has in our lives: the promotion of liberty, autonomy, selfhood, and human relations, and furthering the existence of a free society."

In our research, we heard how privacy for children means, first and foremost, "somewhere where no one else is allowed in", "something that I don't want to show to someone" and "something that I only know." Privacy is also not being seen when taking a shower, "things that one does not even show to siblings" and "when one wants to do something by themselves", as we heard from 10-year-old boys and girls from Austrian schools. Although privacy in physical contexts is easiest to grasp, these days privacy is also a passcode for a phone; indeed, a child in Austria said, "privacy is your mobile phone".

When we say that privacy is contextually meaningful, this is to emphasize the user's perception of the context in which they share information about themselves and the actors involved. Children are primarily conscious of their privacy in interpersonal contexts – in relation to other people, whether parents, peers or strangers. We heard from children in all the countries researched that, for example, it depended on the audience that would have access to them. Particularly problematic was whether they looked strange or silly in photos visible to their contacts when shared by their parents or school. Sharing passwords among good friends is commonly regarded as a sign of interpersonal trust. Further, children find it acceptable to share their home addresses or location with their friends but not with strangers, being highly aware of "people with bad intentions" who could abuse such information.

Privacy violations in interpersonal contexts can be intensely felt. An 11-year-old girl from Austria gave us an example: "like, that someone just takes my mobile phone and can read all my messages; unless he asks and I say he is allowed, something like that I think is shit." Similarly, when children in Flanders were asked what kind of information they share online, they would first inquire whether the researchers meant sharing with friends or with strangers. Protecting one-self from the potential abuse of social media information by strangers extends not only to personal protection but also family and home. A 13-year-old girl from Austria said that posting on social media should be done only "after a lot of thought; for example, my mum doesn't post any holiday photos when we are on holidays, like on Facebook. But when we are back, she makes a diary or something like that." Similarly, an 11-year-old girl in Flanders and a 14-year-old girl in the UK noted that they had heard of instances where social media posts about a child's family being on holiday could lead to house break-ins.

When it comes to other contexts in which personal information is shared, notably institutional contexts such as the school, and commercial contexts such as marketing and advertising, children's understanding is generally less developed, and their efforts to extend what they first learned about privacy in interpersonal contexts to these other contexts can even impede their recognition of the different logics at work (Livingstone, 2020; Stoilova et al., 2020).

Children generally made generous assumptions of "good faith" regarding the decisions that their school makes about their data. Behind those expressions of trust in both schools and third-party platforms was the recognition that children can no longer participate in school without extensive data processing, given that platforms are increasingly embedded in their everyday interactions with the school, for example to track their absences or use learning technologies. Hence children had little choice but to assume that only teachers would have access to their data and trusted the school not to do anything "creepy" with it, as "they're my school, they're going to keep my data safe" (boy, 11, UK). In the USA, one child observed that while he used many Google products for school, he assumed that Google would not sell his data or use it beyond "target advertising or impersonal data collection."

Children generally had a particularly limited understanding of the collection and processing of their personal data by commercial actors. For example, children know that Google (or the "boss of Gmail") "sees" their personal data (such as their names and passwords) (boy, 12, Flanders) or that "Google knows my favourite music, point blank" (girl, USA). Among children in East Asia, "Google knows everything about us" was a frequent refrain. Children in the UK explained that "Mark Zuckerberg, he's always watching" and, aware of the Cambridge Analytica scandal, some knew that "Facebook sold the information of their users to a different company", and that "even if it is a big company, you can't always trust them." Yet children were also puzzled, believing their data to be of little value since they were still young. As children in the UK put it, "Why would somebody want to track me?" and "I just don't think that what the ordinary everyday person does on the internet is really that interesting to companies."

DIGITAL LITERACY AND THE OPAQUE DATA ECOLOGY

Does children's understanding matter? The digital environment poses citizens with multiple decisions about how to manage the flow of information about them across often-opaque contexts; here, the concept of decisional privacy is helpful, as it refers to the decisions and choices of a person with regard to their personal actions (Sarikakis and Winter, 2017). Yet research in OECD countries found that "most educational systems explicitly teach operational, critical informational, social and creative skills in primary and secondary school" but with more focus on basic operational skills and much less on programming/coding and computational thinking (OECD 2019) and, we might add, with much less focus on gaining a critical understanding of the digital ecology.

We found that children are aware of some of the different audiences that can access their information, and they try to manage those audiences by adjusting settings or maintaining different accounts. They told us that they rely on a wide variety of privacy management techniques, including deleting emails with password information, using different passwords for games, changing passwords, using two-factor authentication (through email and phone messages) and providing false information (such as names, addresses and location). But these decisions mostly concern individuals they are aware of (friends, family, peers or strangers), rather than the (commercial) platforms they interact with or that interact with them. The fact

that social media users are offered and can change their personal privacy settings, at the interface level, may seem to afford options for active privacy protection. But even as they enable decisional privacy regarding interpersonal relations, end-user "privacy settings" obscure the fact that users are afforded little or no decisional privacy regarding the commercial data ecology invested in by platforms (Heyman et al., 2014; Livingstone, 2020). The architectures of data exploitation lack transparency and are hence difficult to scrutinise, even by the authorities that are meant to supervise the activities of commercial actors (Katyal, 2019). The opacity of commercial data sharing reveals the limits of both privacy and digital literacy. For example, children may say that "the great thing is, when you close the app [Snapchat] your images are gone" (girl, 13, Austria), and Snapchat may even tell them this. But it is not true. Snapchat maintains those images on its servers – they may no longer be available to the child's contacts, but they are still integral to the data ecology that fuels the internet.

In sum, while children have varying understandings of privacy and how their data is processed, these are not necessarily aligned with definitions deployed in regulation. It is no wonder that they do not always understand what 'data privacy' or 'data protection' means. Some talked of codes and anti-virus programmes, or ways of keeping files secret. Some confused it with internet safety or other forms of protection, for example the use of age restrictions for films. Crucially, children mostly do not understand the underlying commercial data processing practices behind the services they routinely use. Is this a realistic expectation from children, given that such digital literacy is inaccessible even to the average adult (Park 2013). It seems that children's expectation of agency in interpersonal contexts, and their tendency to trust familiar institutions such as their school, can be misplaced in relation to commercial contexts, resulting in a mix of frustration, misapprehension and risk. We saw them trying to piece together snippets of information, but without this necessarily adding up to the deeper knowledge they need to make wise privacy decisions. For instance, older children especially were aware that others can seek information about them: "they Google you" (boy 14, Austria). In East Asia, a group of young teens explained that even when they provided false information about their age or location, apps "already know the truth, they just let you fake it." They are increasingly aware of the Faustian deal whereby children must give their data to get access to services "for free", which, after all, they want and need, lacking funds to pay for subscription services. Hence, when it comes to 'cookies', they "click them away" by accepting them, because they are "annoying" and because one "cannot go further" without accepting them: "If it's something you're going to use and then you have to accept it, I think" (girl, 11, UK). Those children who are aware of cookies also know that they collect information about online behaviour, sometimes pointing to the advertisements for online shopping that they receive as a result.

Children's privacy protection is thus not only limited by their digital literacy but also crucial is the design and management of digital services. They are well aware that they are expected to consent to the terms and conditions imposed by platforms. This requirement is one of the most 'visible' to the user, operating directly on the user interface, which means that children are very likely to come across it. Given this awareness of terms and conditions, it is

particularly problematic for their decision-making about data that users have no option but to consent if they want to participate. In interviews across the countries children expressed their scepticism regarding requests to consent to privacy policies online. Not only do they rarely study them, they find them too long and complex, wondering whether anyone actually reads them before agreeing or consenting to the processing of their personal data, which they saw as unavoidable. As children in Flanders put it, "they are written in such a way that no one wants to read them." Older children in Austria were also critical: "I don't believe anyone reads the terms and conditions and decides no, I won't download this app." And, of course, they are right – again, the design decisions of digital providers (and the failure of regulators to intervene on the side of the user) precludes the possibility of children's understanding or trust, both prerequisites for informed consent. Hence children learn that uninformed consent is the acceptable norm. Children in Flanders even questioned why they are presented with a choice in the first place, since they do not have a real option when asked for their agreement to the terms and conditions and/or consent for data processing or cookies, and can hardly choose "to press no" if they want or need to use the service, whether because their friends all use the service or because their school does not permit them to opt out. Children in Malaysia and the USA had similar complaints: "Nowadays, almost all the applications want you to allow access to your GPS and your media," and, "You're asking for too much information, and I just want to access these features."

Equally salient to children are the minimum age restrictions set by many online services that require users to be at least 13 years old, although children are less likely to realise that this is a result of companies seeking to comply with COPPA and/or the GDPR without having to invest in measures for younger children. But, children sometimes they have also learned to create "workarounds" to bypass the barriers – for instance, that it is commonplace to "lie" about one's age, and that there are generally no adverse consequences for doing so, while there is definitely an adverse consequence to telling the truth, namely, not being able to access the chosen service. Therefore, even though some expressed concerns about "lying", young children frequently provide an older age to have access, circumventing the generally weak age assurance mechanisms operated by platforms; and sometimes they pose as adults (for example, by entering the details of a parent), which can put them at risk (Livingstone et al., 2013). According to a 12-year-old boy in Austria: "I think it's actually okay that younger people register with older ages. I find it a little stupid that social media have now changed the rules to 16 although there is nothing nasty on their sites." Such a comment reveals a confusion shared by many adults – the recent age change in WhatsApp, for example, was to avoid GDPR obligations by simply excluding children from the service rather than by taking the trouble to provide for their needs. In short, the change resulted from both regulators and businesses failing to anticipate how the introduction of data protection rules could negatively affect children's rights, but it was commonly (mis)interpreted as an internet safety measure, thereby undermining public trust in regulation.

SIMILARITIES AND DIFFERENCES ACROSS COUNTRIES

Our findings reveal some interesting contrasts because of variation in regimes of regulation and education as well as the practicalities (and inequalities) of internet access. These differences shape how children approach and understand privacy in the digital age, as well as how their data are treated by industry and regulators. Children's expectations of agency and control vary in consequence – how much they expect to be consulted, and to have their rights respected. Our findings lead us to emphasize the importance of contextualizing questions of privacy within diverse experiences of childhood, including how privacy is conceptualized and enacted by children and caregivers in the datafied world.

For example, in the USA, a country that has not ratified the UNCRC because it is held to interfere with family life (US Congress, 2011), the findings reveal how greatly children want more privacy from their parents. In Austria, where children are aware of the recently introduced GDPR, the regulatory shift has afforded them a language for privacy and data rights as well as a degree of confidence in its implementation. In Flanders, children showed great interest in the fact that they have rights under the GDPR but did not testify to knowing which rights they have, let alone to exercising them. In the UK, the site of the Cambridge Analytica scandal, and with an assertive EdTech strategy (DfE, 2019), children are torn between wanting their schools to teach them digital literacy yet distrusting the companies that increasingly provide the educational infrastructure in what is commonly dubbed either a Google or a Microsoft school. In East Asia, we interviewed children who had experienced very difficult circumstances. For children living in poverty, basic literacy and tech access were the primary focus and privacy was largely beyond their sphere of attention. Notably, among those who had been exploited, some neither sought out nor expected privacy, and some considered privacy almost a risk itself – equating it with the secrecy that left them open to exploitation.

Despite these fundamental differences deriving from the structures and lifeworlds of children's lives, the value of privacy as a person's sense of control of their 'own' digital space and personal interiority remained intact across all groups. Even among the particular groups we interviewed in East Asia, where the mobile phone was often the means of their exploitation, it was also the route to access help and support. Considering the intense experiences linked to the phone, these young people talked of chatting on their phone or protecting their passwords in much the same way as those living in much more affluent or safer conditions in Europe or the USA. Despite the ways in which they had been failed by the system, they still had expectations that it would act in their best interests, including educating them as needed and protecting them and their data from further exploitation. For example, children in Cambodia expected companies to use their data to provide educational content and promote wellbeing, while a few of their peers in Thailand asked for apps that could mine their chats to identify harmful content before they could see the messages. On the other hand, the potential invasion of privacy linked to efforts precisely to protect children, especially by collecting personal information from those who are already vulnerable, is proving controversial in regulation debates, as the current debates on age assurance demonstrate (5Rights, 2021).

The similarities across countries are nothing less than striking. In all countries where we researched, children, much like the adults, around them struggled to grasp the consequences of growing up with such an omniscient and omnipresent technology. Like Altman (1975), we found that interpersonal privacy management is a universal phenomenon. Children primarily conceptualize privacy in relation to interpersonal contexts, conceiving of personal information as something they have agency and control over while 'data privacy' or 'data protection' was not something they knew much about. At the same time, we also found children to be engaged by and keen to understand the data ecology in which their lives are now enmeshed.

Wherever we interviewed children, we heard their rising tide of concern about the assaults on their privacy in a datafied world and found some misapprehensions about how personal data is collected, inferred and used by organizations, be these public institutions such as their school or, especially, businesses. Everywhere, too, we heard the outraged cry that "the internet knows everything about us" and "we have little choice", although some were more fatalistic and others more tactical in their responses. So even though we have noted the hints of contextual variation in children's understanding, far more compelling were their unified concerns, tying together expectations of education and regulation in a growing awareness of the digital environment and their relative lack of agency to manage it.

Of course, in every country children would benefit from greater educational efforts that treat them as agents, able to construct norms regarding appropriate data usage and information flows (Pangrazio and Selwyn, 2019). But the very complexity of the current digital ecology makes it hard, if not impossible, for the public to anticipate the long-term consequences of their digital footprint. Children face particular difficulties because of their age and maturity, because they may use digital products and services that are neither age-appropriate nor respectful of their rights, and because the adults responsible for them (parents, teachers and wider society) often fail to grasp or defend their interests, even undermining them through everyday surveillance practices (Leaver, 2015). Educators, too, face significant challenges regarding the effort to explain complex socio-technological changes, including scaffolding children's critical grasp of the data ecology and its algorithmic processing, technological architecture, business models, regulatory frameworks and available options for remedy or complaint. Crucial questions for educators concern their capacity (in terms of training and resources) to go beyond the usual and already-taxing expectation for a basic understanding of digital literacy to produce a dedicated and sophisticated media literacy curriculum provision that answers the questions raised by children interviewed in our research (Stoilova, Livingstone and Nandagiri, 2020).

CHILDREN'S RIGHT TO BE HEARD ON MATTERS THAT AFFECT THEM

In many of our focus group discussions, children not only revealed their understanding but they also expressed concerns, including their political claims and demands for change, even though these were not always articulated as such. Over and again, the discussions with children pointed to a gap between what the law requires and what happens in practice. For

European children, for example, although the GDPR emphasizes user rights, transparency and control, they do not feel that they are informed, and want greater control. Not only educators but also data controllers should make greater efforts to consider children and their needs seriously, and they should be held accountable for this by national data protection authorities. This is reinforced in the UN Committee on the Rights of the Child's General Comment No. 25 (2021), which states that businesses should be required to "maintain high standards of transparency and accountability and […] take measures to innovate in the best interests of the child" (para. 39), along with many requirements regarding the protection of children's privacy and data in relation to the digital environment.

In the spirit of Article 12 of the UNCRC – children's right to be heard in all matters that affect them – we note here some of the demands from children that we heard during our research across the different countries.

From a 15-year-old in Austria, a request for basic respect of privacy:

> It always springs to my mind that in any case we are spied upon. I mean, alone by our mobile phones. Why? They shouldn't do it.

From a 12-year-old in the USA, a request for transparency:

> Why do you need my location? If they could just say what they're gonna do with my location, then I'd be fine.

From a 16-year-old in Thailand, a request for limiting data shared with third parties:

> Don't share every bit of information to third party companies.

From an 11-year-old in Flanders, a request not to collect location data when this is not necessary for the app or game:

> Not all apps should know my location. Because why do they need that? Why do they ask for it? Then I think to myself: 'No, this is just a simple little game'.

From a 13-year-old in the UK, a request to choose what information is collected and with whom it is shared:

> Your information is specifically yours. Like your full name, mental health, that's to do with you. So you should be able to choose who knows and who doesn't.

From a 16-year-old in the USA, a request for meaningful consent:

> You should always have consent and boundaries ... consent with data, consent to have a hug. You're saying, 'These are my boundaries.'

From a 15-year-old refugee in Malaysia, a request for social media apps not to directly approach children:

> You can use it, but the parents need to be involved.

From an 11-year-old in the UK, a request for contacts to be private:

> Companies shouldn't really be poking through your contacts. Because there might be some sensitive information in there which they shouldn't get a hold of.

Clearly, children are able to reflect on their experiences and express ideas, suggestions and recommendations on ways to improve how their personal data are processed. For example, instead of plain, long and complicated pieces of text, children in Flanders suggested that details of data collection and use could be presented to them in the form of posters, mind maps, (animated) videos, online and offline games, quizzes, vlogs, sketches, explanatory pictures or drawings, letters, funny advertisements, puzzles and websites. The guidance provided by the EU's Article 29 Working Party (2018) and the UK Information Commissioner's Office (ICO, 2020) corresponds with children's own recommendations for child-specific information provision measures, such as cartoons, infographics, flowcharts, comics, animation, graphics, privacy dashboards, symbols, video and audio content, as well as gamified and interactive content.

In addition to specific formats, children consider links to their day-to-day reality very important when referring, for instance, to their school life and social media environment. Some children from the UK wanted to have conversations with their parents and teachers about the data collection and options for protection. Children in Flanders also wanted to see information about the processing of their personal information in ways that were tailored to their specific (age) group as much as possible, and wanted to be involved in its creation (for example, to feature in the information videos created for them and their peers). Whatever the presentation format, a 12-year-old boy in the USA summed up many children's view that "if people know that their information is not kept private on the internet then they might do something about it…I think it's less about not caring and more about not knowing."

CONCLUSIONS: THE INTERDEPENDENCIES OF EDUCATION AND REGULATION

Communication technologies are becoming continuously more sophisticated, artificially intelligent, globally networked and commercially profitable. Protecting children's privacy in a digital world compounds the already-familiar challenges of implementing a universal rights framework, not least because children live in highly diverse contexts and political cultures around the world (UNICEF, 2014). Government actions regarding the digital environment

often favour a limited vision of what 'adequate' education might entail as regards digital literacy, even in more affluent countries that could afford systematic approaches to protecting privacy, including through the introduction and implementation of data protection regulation and other forms of privacy legislation to ensure that public and private sector organizations protect children's privacy and data, as well as by promoting children's knowledge of their rights.

More fundamentally, this chapter has argued against the common view that digital literacy education and data protection regulation are mutual alternatives, to be traded off against each other in public debates as a matter of political expediency. Supposedly, if only children could understand the data ecology, they could take responsibility for their personal data and exercise wise judgement regarding the ways in which it is processed. Conveniently, since children constitute a group commonly deemed too immature to be consulted as a stakeholder, making this assumption has the effect of relieving regulators of the requirement to address children's specific vulnerabilities. The brunt of the burden to 'provide' digital literacy is instead outsourced to the educational systems, especially the teachers and, indirectly, the parents 'responsible' for their children's upbringing. In short, notwithstanding the immense socioeconomic and resource inequalities within and across countries, it is held to be the individual's responsibility to obtain, maintain and develop digital literacy skills. Yet this is a regulatory response which fails to serve emerging citizens.

By rights, literacy is a matter of civic empowerment and participation meant to operate side by side with other provisions, such as public services, public interest journalism, corporate social responsibility to name some. Yet too often, policy debates only seek to redress the damage already inflicted by private and public bodies on citizens' privacy by burdening the individual with their own protection. If regulation operated effectively in children's best interests, then the role of educators would not be limited to warning children against the potentially abusive actions of public and private organisations, for these would offer children meaningful choices that respect their evolving capacities and needs. Nor would they be called upon merely to pass on information but could be freed to creating knowledgeable participatory pathways for children to intervene in the technologies they use. But regulation relies on an effective and interventionist state, and that can in itself have problematic consequences depending on the kind of government in power; partly in consequence, there are many commercial and political interests that lobby to keep regulation weak.

Even in the wealthy countries studied, not only do disparities among educational institutions within the same country create further digital inequalities in educational environments, but also even the best available education is proving insufficient to support children's agency in a datafied world. Meanwhile in the poorer countries, the lack of resources obviates any choice between regulation and education. Moreover, the polarization of educational versus regulatory approaches distracts from assigning responsibility to all actors involved each according to their negotiating power. The discursive construction of education *versus* regulation or even education *as* regulation does not work either in principle or in practice. In principle, children have the right to know and exercise their rights, however benevolent the

state or effective its instruments, while education about legal rights is an important element of legal empowerment. In practice, education and regulation have co-evolved, with education tasked with teaching children about the available forms of governance, and with regulation embedding assumptions about what the average citizen may be expected to understand. Across a range of social issues, legal empowerment initiatives which educate the public about the law and how it impacts them have been found to increase the agency of participants both in terms of willingness to act and actual action (Goodwin and Maru, 2014). Rather than focus on either educational or regulatory dimensions of children's understanding of their privacy in a digital world, our discussion has shown that digital literacy, crucial though it is, cannot be a match for multi-country, multi-billion, oligopolistic companies that control digital platforms. It has also shown the interdependencies, by exploring how children understand both the digital environment and also its regulation, before highlighting the changes children call for from educators and regulators alike.

When it comes to ensuring that children's rights in the digital environment are truly respected, protected and fulfilled, investment of appropriate resources in both educational institutions and regulatory authorities is required. But to task educators with the responsibility of mitigating harms due in large part to the structural problem of unfair or exploitative data processing is surely to misdirect scarce educational resources. While children have the right to be informed in an honest and age-appropriate way about the nature and consequences of the processing of their personal data, it is equally or perhaps more important to implement regulation that imposes and enforces requirements for data processing in children's best interests. After all, children are hardly expected to educate themselves about other complex fields akin to data processing such as financial services or pharmaceutical drugs, in place of government regulation. Hence this chapter concludes by calling for a rights-respecting architecture for digital platforms that ensures that genuine choices are available to users, who should be fully informed about these choices, as well as preventing privacy violations and commercial exploitation of children around the world. To advance in this direction, it is imperative to give children a voice to guarantee that their best interests are taken into account in shaping and evaluating both educational and regulatory initiatives, and to recognise their interdependencies.

REFERENCES

5Rights (2021) *But how do they know it is a child? Age Assurance in the Digital World.* London: 5Rights. Available at: https://5rightsfoundation.com/uploads/But_How_Do_They_Know_It_is_a_Child.pdf

Altman, I. (1975) *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*, Monterey, CA: Brooks/Cole.

Article 29 Data Protection Working Party, (2018) 'Guidelines on Transparency under Regulation 2016/679'. WP260 Rev.01. Available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

Aviram, A., Gurion, B. and Eshet-Alkalai, Y. (2006) 'Towards a theory of digital literacy: Three scenarios for the next steps', *European Journal of Open, Distance and E-Learning*. Available at: https://old.eurodl.org/materials/contrib/2006/Aharon_Aviram.pdf

Buckingham, D. (2007) 'Digital media literacies: Rethinking media education in the age of the internet', *Research in Comparative and International Education, 2*(1), 43–55. Available at: https://doi.org/10.2304/rcie.2007.2.1.43

Bulger, M. and Burton, P. (2020) *Our Lives Online: Use of Social Media by Children and Adolescents in East Asia – Opportunities, Risks and Harms*. Bangkok: UNICEF East Asia and Pacific Regional Office. Available at: www.unicef.org/eap/reports/our-lives-online

Carretero, S., Vuorikari, R. and Punie, Y. (2017) *DigComp 2.1: The Digital Competence Framework for Citizens with Eight Proficiency Levels and Examples of Use*, EUR 28558 EN. Available at: https://op.europa.eu/en/publication-detail/-/publication/3c5e7879-308f-11e7-9412-01aa75ed71a1/language-en

Chakravartty, P and Sarikakis, K. (2006) *Media Policy and Globalisation*, Edinburgh: Edinburgh University Press.

Charter of Fundamental Rights of the European Union. OJ C 326. 2012. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012P%2FTXT

De Wolf, R. and Vanden Abeele, M. (2020) 'Children's voices on privacy management and data responsibilization', *Media and Communication, 8*(4), 158–62. Available at: http://dx.doi.org/10.17645/mac.v8i4.3722

DfE (Department for Education) (2019) 'EdTech Strategy marks "new era" for schools', Press release, 3 April. Available at: www.gov.uk/government/news/edtech-strategy-marks-new-era-for-schools

Fulton, K. (1997) *Learning in a Digital Age: Insights into the Issues,* A publication of the Milken Exchange on Information Technology, Milken Family Foundation.

Gavison, R (1980) 'Privacy and the Limits of Law', *Yale Law Journal, 89(3).* Available at: https://digitalcommons.law.yale.edu/ylj/vol89/iss3/1

Goodwin, G., and Maru, V. (2014), *What do we know about legal empowerment? Mapping the Evidence*. Namati. Available at: https://namati.org/wp-content/uploads/2014/05/Evidence-Review2.pdf

Heyman, R., De Wolf, R. and Pierson, J. (2014) 'Evaluating social media privacy settings for personal and advertising purposes', *The Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media, 16*(4), 18–32. doi:10.1108/info-01-2014-0004.

ICO (Information Commissioner's Office) (2020) *Age Appropriate Design: A Code of Practice for Online Services (the Final Version).* Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services

Katyal, S.K. (2019) 'Artificial intelligence, advertising, and disinformation', *Advertising & Society Quarterly, 20*(4). doi:10.1353/asr.2019.0026

Lansdown, G. (2014) ‘25 years of UNCRC: Lessons learned in children’s participation’, *The Canadian Journal of Children’s Rights, 1*(1), 172–90. Available at: https://doi.org/10.22215/cjcr.v1i1.12

Laufer, R. and Wolfe, M. (1977) ‘Privacy as a concept and a social issue: A multidimensional developmental theory’, *Journal of Social Issues, 33*(3), 22–42. Available at: https://doi.org/10.1111/j.1540-4560.1977.tb01880.x

Leaver, T. (2015) ‘Born Digital? Presence, Privacy, and Intimate Surveillance’, in H. John and W. Qu (eds) *Reorientation: Translingual Transcultural Transmedia – Studies in Narrative, Language, Identity, and Knowledge* (pp. 149–60), Shanghai: Fudan University Press.

Livingstone, S. (2020) ‘“It’s None of Their Business!” Children’s Understanding of Privacy in the Platform Society’, in B. Kidron (ed.) *Freedom Security Privacy: The Future of Childhood in the Digital World* (pp.126-133), London: 5Rights Foundation. Available at https://freedomreport.5rightsfoundation.com/its-none-of-their-business-childrens-understanding-of-privacy-in-the-platform-society

Livingstone, S., Ólafsson, K. and Staksrud, E. (2013) ‘Risky social networking practices among “underage” users: Lessons for evidence-based policy’, *Journal of Computer-Mediated Communication, 18*(3), 303–20. doi:10.1111/jcc4.12012.

Livingstone, S., Stoilova, M. and Nandagiri, R. (2019) *Talking to Children about Data and Privacy Online: Research Methodology*, London: London School of Economics and Political Science. Available at: www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Talking-to-children-about-data-and-privacy-online-methodology-final.pdf

Livingstone, S., van Couvering, E. and Thumim, N. (2008) ‘Converging Traditions of Research on Media and Information Literacies: Disciplinary, Critical and Methodological Issues’, in J. Coiro, M. Knobel, C. Lankshear and D.J. Leu (eds) *Handbook of Research on New Literacies* (pp. 103–32), Mahwah, NJ: Lawrence Erlbaum Associates.

Milkaite, I. and Lievens, E. (2019) ‘Children’s rights to privacy and data protection around the world: Challenges in the digital realm’, *European Journal of Law and Technology, 10*(1). Available at: https://ejlt.org/index.php/ejlt/article/view/674

Milkaite, I. and Lievens, E. (2020) ‘Child-friendly transparency of data processing in the EU: From legal requirements to platform policies’, *Journal of Children and Media, 14*(1), 5–21. Available at: https://doi.org/10.1080/17482798.2019.1701055

Nascimbeni, F. and Vosloo, S. (2019) *Digital Literacy for Children: Exploring Definitions and Frameworks*. Scoping Paper No. 01. New York: UNICEF. Available at: www.unicef.org/globalinsight/media/1271/file/%20UNICEF-Global-Insight-digital-literacy-scoping-paper-2020.pdf

Nissenbaum, H. (2010) *Privacy in Context. Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.

OECD (2019), "Fostering digital literacy and well-being", in Burns, T. and F. Gottschalk (eds.), *Educating 21st Century Children: Emotional Well-being in the Digital Age*, OECD Publishing, Paris, https://doi.org/10.1787/23ac808e-en

Pangrazio, L. and Selwyn, N. (2019) '"Personal data literacies": A critical literacies approach to enhancing understandings of personal digital data', *New Media & Society, 21*(2), 419–37.

Park, Yong Jin. (2013). Digital Literacy and Privacy Behavior Online. *Communication Research*, 40, 215-236.

Raffaghelli, J.E. (2020) 'Is data literacy a catalyst of social justice? A response from nine data literacy initiatives in higher education', *Education Sciences, 10*, 233–53. doi:10.3390/educsci10090233

Sarikakis, K. and Winter, L. (2017) 'Social media users' legal consciousness about privacy', *Social Media + Society*, January–March, 1–14. Available at: https://doi.org/10.1177/2056305117695325

Stoilova, M., Livingstone, S. and Nandagiri, R. (2019) *Children's Data and Privacy Online: Growing Up in a Digital Age*, London: London School of Economics and Political Science. Available at: www.lse.ac.uk/my-privacy-uk/Assets/Documents/Childrens-data-and-privacy-online-report-for-web.pdf

Stoilova, M., Livingstone, S. and Nandagiri, R (2020) 'Digital by default: Children's capacity to understand and manage online data and privacy', *Media and Communication, 8*(4). Available at: www.cogitatiopress.com/mediaandcommunication/article/view/3407

UN (United Nations) (1989) *United Nations Convention on the Rights of the Child,* Geneva. Available at: https://www.ohchr.org/en/professionalinterest/pages/crc.aspx

UN (United Nations) Committee on the Rights of the Child (2021) *General Comment No. 25 (2021) on Children's Rights in Relation to the Digital Environment*, CRC/C/GC/25. Available at https://undocs.org/CRC/C/GC/25

UNICEF (United Nations Children's Fund) (2014) *25 Years of the Convention of the Rights of the Child – Is the World a Better Place for Children?* New York: UNICEF.

US Congress (2011) S.Res.99 – 112th Congress (2011–2012). Available at www.congress.gov/bill/112th-congress/senate-resolution/99

van Dijk, J.V. and Hacker, K. (2003) 'The digital divide as a complex and dynamic phenomenon', *The Information Society, 19*, 315–26. Available at: https://doi.org/10.1080/01972240309487