Data and privacy literacy: the role of the school in educating children in a datafied society[1]

Sonia Livingstone, Mariya Stoilova und Rishita Nandagiri

Abstract

What should children be taught about their online privacy and the uses that others may make of their personal data, and why? This chapter reports on a systematic mapping of the available evidence followed by child-centered, qualitative research interviews with children aged 11-16 years old in the UK. The aim was to discover what children of different ages already know about privacy and data online, to ask them what they want to know, and then to reflect on the educational challenges posed by the answers. For its conceptual framing, the chapter distinguishes three contexts for data use online – interpersonal, institutional (including the school) and commercial. Since these are increasingly interconnected, it is argued that children should be taught about each, to gain a critical understanding of the data ecology and business models which are driving the datafication of society and, thereby, childhood. Finally, it is proposed that, if schools could themselves demonstrate best practice in data processing – explaining school policy, practice, and opportunities for redress to their students – this might prove a more effective means of improving children's understanding than via the taught curriculum.

Introduction

Of the many calls upon educators, one of the most recent is that children should be taught about their online privacy and data, given today's increasingly datafied society (Lupton/Williamson 2017: 780-794). The transforma-

1 **Acknowledgments:**
This research was funded by the UK's Information Commissioner's Office. An earlier version of this chapter was originally published in Frau-Meigs, D. et al (Eds.), *Handbook on Media Education Research*. London: Routledge.

tion of ever more human activities into data means that managing one's privacy is becoming highly complex, and ever more part of institutional practices of state control and evolving business models. People's online data selves (or 'digital footprints') are increasingly the means by which their options become determined for them by others, according to the interests of those others rather than, or at best, as well as the interests of the data subject (Zuboff 2019). Consequently, it is important to recognize the interdependence of digital media literacy (what children can and should be taught about the digital environment) and digital design and regulation (how the digital environment does, could and should address children, use their data or offer redress).

This poses a new challenge for schools already struggling to address e-safety, online identity and reputation, coding, information navigation, misinformation and "fake news," digital dimensions of sex and relationships education, screen time and mindfulness, and more, all under the loose rubric of "media literacy" (Bulger/Davison 2018). How can children be educated about commercial and state uses of their data, when this involves complexities of data protection and privacy regulation that most adults – including parents and teachers – hardly understand? Can such digital literacy education, even if implemented, manage sufficiently to empower children when companies obscure how they operate with children's data, conceal children's privacy rights, or fail to anticipate their needs in designing services? The risk is that the result may disempower children further by confusing them with quickly out-of-date complexities or inculcating the dystopian message that they can only lose control of their online privacy if they wish to participate fully in the digital age.

This chapter draws on the project, "Children's data and privacy online: growing up in a digital age" (Livingstone/Stoilova/Nandagiri 2019a), funded by the UK's data protection authority. This takes a child-centred approach, prioritising children's voices, experiences and rights within a wider framework of evidence-based policy development. The research began with a systematic evidence mapping of current research (Livingstone/Stoilova/Nandagiri 2019a), followed by 28 workshop-style focus group discussions with children of secondary school age (11-16 years old) and, separately, interviews with parents and educators (for a detailed description of the methodology see Livingstone/Stoilova/Nandagiri 2019b). Both the evidence mapping and the empirical work have informed this chapter. Real-life scenarios and exemplar digital experiences were used to facilitate the discussions and to ensure that children were engaged in deliberating on the opportunities, risks, and practical dilemmas posed by the digital environment. Guided throughout by an international expert advisory board,

and working with children themselves, the project concluded by creating an online, open-access toolkit to support and promote children's data and privacy literacies.

The analysis starts by asking: what do children know, what do they want to know and what do they need to know about their privacy and data online? Then, given their professed knowledge gaps, the research considers the role of the school, asking what the teachers know and think they should teach, and considering also how the school as an institution, through its own policies and procedures, models a particular approach to children's data and privacy; this latter tends to undercut the curricular challenge by modelling an opaque approach to data protection. Finally, after hearing from students and parents what they expect of the school and from teachers on their struggles to grasp the data and privacy literacy challenge facing them, the chapter concludes by asking whether the responsibility for children's privacy be better apportioned between school, home, business, regulators and children themselves.

1. Conceptualizing data and privacy literacy

Children's digital literacy plays an important part in how children understand, manage and safeguard their privacy. Privacy involves considerably more than simply providing, guarding or withholding one's personal information. Drawing on Nissenbaum's (2004: 119–157) notion of privacy as *contextual integrity*, and recognizing that contexts emerge from the mutual interaction between people and their environments, privacy online is conceptualized in this chapter as depending, on the one hand, on the design, infrastructure and political economy of the digital environment and, on the other, on users' agency and knowledge (as data subjects, individually and collectively) regarding what they wish or judge appropriate to share within specific digital contexts. While many digital contexts can be identified, a primary distinction can be made among:

(i) interpersonal privacy (how my 'data self' is created, accessed and multiplied via my online social connections);
(ii) institutional privacy (how public agencies like government, educational and health institutions gather and handle data about me);
(iii) commercial privacy (how my personal data is harvested and used for business and marketing purposes).

Online, interactions are encoded and mediated by data, and users are learning to recognize how their social interactions are transformed into da-

ta in ways that may or may not respect their agency. The digital environment is developing too – increasingly structuring, managing and potentially exploiting users' data in ways that generally lack transparency and accountability. Three types of data can be distinguished when considering what children need to understand about their online privacy: data contributed by individuals about themselves or others (data given); the data left, mostly unknowingly, and captured via data-tracking technologies (data traces); and data derived from analyzing data given, data traces, and possibly other sources (inferred data, also referred to as 'profiling') (typology adapted from van der Hof 2016: 409-45, building on Goffman 1971).

Given the importance of these distinctions and complexities, we argue that a functional skills-based approach to the digital interface (learning practically how to navigate terms and conditions, age requirements, privacy settings, etc.) is necessary but not sufficient to protect and empower children in a datafied society. Children's autonomy and dignity as actors in the world depends on both their freedom to engage and their freedom from undue persuasion or influence. To exercise their rights as agents and citizens in a digital world, children need a deeper, critical understanding of both the digital environment (including its business models, uses of data and algorithms, forms of redress, commercial interests, systems of trust and governance) and, indeed, of social relations and interactions. Arguably this would traditionally fall within media education, but it sits uncomfortably with standard definitions focused on mediated forms of communication – such as the ability to access, analyze, evaluate and create messages across a variety of contexts (Aufderheide 1993) – because what is critical in relation to data and privacy is an understanding of the digital environment behind the interface of the screen. It is also more demanding than many media literacy curricula (McDougall/Livingstone/Sefton-Green/Fraser 2014, European Audiovisual Observatory 2016).

This may seem daunting to teachers, and understandably so, given the technological complexities, rapid pace of innovation, regulatory challenges and relative unaccountability of digital businesses, not to mention the crowded curriculum, limited opportunities for in-service training and many other pressures on teachers (National Literacy Trust 2018). However, critical approaches to media education have long urged that children are taught not only about mediated representations and influences but also about the production context and political economy of the media and the consequences for power, profit and possibilities of resistance (Kellner/Share 2007: 59-69, Hartley 2011, Buckingham 2015: 21-35). In the light of today's growing digital challenges, one might wish that this task had been begun by schools earlier.

2. Children's understanding of data and privacy online

Children's capacity to manage their privacy in the digital environment depends on many factors. Educators, regulators and parents are particularly keen to know when and how data and privacy online should be addressed – in the curriculum, in framing regulation - for children of different ages (Livingstone 2018: 18-23, Livingstone/Ólafsson 2018, Livingstone/Blum-Ross/Zhang 2018). While cautioning that most research focuses on adolescents to the exclusion of younger children, and that differences within as well as across age groups can be substantial, findings for children aged 5-7, 8-11 and 12-17 years old were grouped together based on the age groups used most often in the available research.

Table 1 provides a summary of the results of the systematic evidence mapping of recent empirical research on children's understanding of their privacy online (Livingstone/Stoilova/Nandagiri 2019a). It suggests that children give considerable thought to interpersonal privacy, although they may struggle with how to negotiate sharing or withholding personal information in networked contexts which demand they trade privacy for opportunities for participation, self-expression and belonging (Micheti/Burkell/Steeves 2010: 130-43, Hasselbalch Lapenta/Jørgensen 2015).

By contrast, children are generally less aware of how institutions or commerce operate in the digital environment, and so they may reveal personal data without recognizing the potential for data breaches on the one hand or exploitative practices by businesses on the other. It can be noted, however, that most research considers only interpersonal contexts, whereas this research had to combine the limited findings from institutional and commercial contexts for privacy, notwithstanding the important difference between organizations acting in the public and private interest (see table 1 for summary of answers).

Table 1: Children's developing data and privacy literacy

	Interpersonal privacy	Institutional and commercial privacy
5- to 7-year-olds	• A developing sense of ownership, fairness and independence • Learning about rules but may not follow, and don't get consequences • Use digital devices confidently, for a narrow range of activities • Getting the idea of secrets, know how to hide, but tend to regard tracking/monitoring by a trusted adult as helpful	• Limited evidence exists on understanding of the digital world • Low risk awareness (focus on device damage or personal upset) • Few strategies (can close the app, call on a parent for help) • Broadly trusting
8- to 11-year-olds	• Starting to understand risks of sharing but generally trusting • Privacy management means rules not internalized behavior • Still see monitoring by a parent or other trusted adult positively, to ensure their safety • Privacy risks linked to 'stranger danger' and interpersonal harms • Struggle to identify risks or distinguish what applies offline/online	• Still little research available • Gaps in ability to decide about trustworthiness or identify adverts • Gaps in understanding privacy terms and conditions • Interactive learning shown to improve awareness and transfer to practice
12- to 17-year-olds	• Online as 'personal space' for expression, socializing, learning • Concerned about parental monitoring yet broad trust in parental and school restrictions • Aware of/attend to privacy risks, but mainly seen as interpersonal • Weigh risks and opportunities, but decisions influenced by desire for immediate benefits	• Privacy tactics focus on online identity management not data flows (seeing data as static and fragmented) • Aware of 'data traces' (e.g., ads) and device tracking (e.g., location) but less personally concerned or aware of future consequences • Willing to reflect and learn but do so retrospectively • Media literacy education is most effective if adolescents can use their knowledge to make meaningful decisions in practice

The focus groups with children aged 11 to 12, 13 to 14 and 15 to 16 years old confirmed this finding. The research began with an open discussion of privacy, and how children use and think about the internet. It then sought to focus their discussion on the privacy and data practices of the commercial apps and services they use and, later, on the practices of their school and other institutions such as health or transport services. But over and again, children responded in interpersonal terms, even when institutional or commercial practices were really at issue (Stoilova/Livingstone/Nandagiri 2020). They discussed the people running Instagram or Snapchat, and their teachers, notwithstanding that these are organizational relationships. This may partly be due to their greater familiarity with interpersonal contexts, and the ways in which privacy in that domain is managed and valued. It may also be because, in interpersonal contexts, privacy is largely mediated by the personal information people choose to reveal to the those they know or meet, involving practices with which children are familiar.

Yet this is not, by and large, how privacy works online, especially in relation to institutions and commerce, where the relation between user agency and digital design can be very different, mediated by data protection regulation, on the one hand, and the data economy or business of "datafication," on the other hand (O'Hara 2016: 86-91, Lupton/Williamson 2017: 780-794).

3. What children want to know about data and privacy online

Towards the end of each session, the children were asked what they wanted to know, and what they thought companies should do differently (see Table 2 for summary of answers). Their primary concern, irrespective of age – and admittedly after a lively discussion of their data and privacy online – is: who has got their data, what is done with it, and why. Few had a good understanding of how data profiling is conducted or the data economy of which profiling is a part. When the researchers explained something of this to them, many were both puzzled and outraged – "it's none of their business" was a common response to learning about the widespread collection of their personal data although, ironically, it is precisely the companies' business model (Zuboff 2019).

The tabulated responses provide some interesting hints about how children of different ages approach the problem – younger children are concerned with the privacy options provided by apps, for instance, while older children are beginning to think also about data governance. Also, younger

children think of personal information in terms of phone numbers and other data given, while older children are more aware of data taken (via facial recognition technology, for instance), and of different kinds of data (sensitive, biometric, profiled). The youngest group wants more protections while those in the middle age group are "naughtier" (asking about the dark web, hacking, etc.). From the focus group discussions, a growing awareness of all three data types seemed roughly linked to age, with the younger children focusing most on data given, and the teenagers increasingly aware of data taken and inferred– though all had some awareness of profiling, because all had had the experience of searching for something and later receiving related advertising.

More striking, however, was that across the age range, a strong assumption of fairness pervaded what the children said: companies *should* explain better, improve services, be age-appropriate, provide options that users want, respond to users' concerns, and treat users well. They did not really question whether it is in companies' interest to act in this way; if practices are judged by children as unfair, then something should be done. Similarly, if an organization is trusted (whether a big brand or their school) then it was assumed that they would treat children's data fairly. Here the logic of interpersonal contexts is at work, with which children are familiar, being extended to the institutional and, especially, commercial contexts, with which they often have little experience (Stoilova/Livingstone/Nandagiri 2020).

Indeed, since interpersonal lives are now often conducted in proprietary environments, each interaction has a double significance – sharing an image with a friend on Instagram means also sharing that image with Instagram. Thus, the interpersonal and commercial contexts – traditionally so different, become blurred, confusing not only children but also the adults who try to guide them. Confusions arose from the use of terms from interpersonal or everyday contexts being used for technical processes – how can companies still know all about you if you've put your "privacy" settings on or dissemble your name, age or gender; why aren't things you "deleted" truly deleted; why are companies who have no personal relation with you so interested in your 'personal' life? The tendency to extend interpersonal expectations into commercial contexts was also evident when things go wrong – children express frustrations about companies proving unresponsive to their reports or complaints; they would expect family or friends to respond, after all, so why not the companies?

Table 2: Children's views of how their data and privacy online should be addressed: what they want to know, and what they think should be changed (entries paraphrased and summarized)

	What children want to know about their data and privacy online	What children think companies should do differently
All ages	• Who has got my personal data, how long do they keep it and what do they do with it • Why do they collect, share and sell my information • Where does deleted data go, is it really gone	• Make deleted apps or information permanently gone • Provide more and better privacy, security and safety options • Make accounts private, turn off geo-location and disable cameras by default • Don't share my data with other sites or services • Better responsiveness to user concerns and complaints • Make Terms and Conditions understandable, short and visual
11-to 12-year olds	• Why do apps need to know your phone number • Who controls the websites • Who can find out about my information • Why do they set age restrictions so high (e.g. WhatsApp) • Why don't companies remove scamming sites • Why is reporting stuff so hard • Why do they make mistakes about who you are	• Let under 13s use social media but keep their account private • Make online content more appropriate for our age • Take down hostile content (e.g. fat shaming)

	What children want to know about their data and privacy online	What children think companies should do differently
13-to 14- year olds	• Who can see what I search • Can people see me through my camera or hear my voice • What social media sites do with your information • What happens when you get hacked • What happens to your data when you die • What is the dark web • What do they do with your face when you use facial recognition	• Allow paid-for but private apps • Not sell our data • Not show me what I'm not interested in • Make it easier to erase your account
15-to 16-year olds	• Where is data kept, how does it travel across the internet, and what is shared with other companies • Why do they need to know so much about me (e.g. my gender) • Is sensitive data shared	• Leave me alone • Keep biometric data safely • Delete our data after a certain time (e.g. two years) • Only ask for information when relevant • Allow you to opt out of data collection • Better checks on age restrictions • Explain to you what information they have about you

4. The role of the school in teaching children about data and privacy online

Institutional practices related to privacy (e.g., digital learning platforms, fingerprint access to meals or buildings, profiling of attendance and performance) are often presented as "revolutionary" and transformational to parents (Williamson 2017: 59-82). But one study in American schools found that commercial monitoring software, instituted to tackle bullying, monitored public social media posts made by students aged 13+ when both on and also off campus, with reports flagged to school administrators (Shade/Singh 2016: 1-12). Not only does this mean that efforts professing to protect children can both infringe their privacy and position them as perpetrators, but it is often unclear to schools whether the businesses providing educational services also cross-reference their data with other records or information available, creating an assemblage of surveillance which may exceed what parents or children believe they have consented to and which may have adverse consequence they do not anticipate.

Several parents and teachers in the research project expressed concern about this reliance on commercial business models and for-profit platforms for educational purposes, echoing the concerns of critical scholars regarding the risk to and exploitation of student data (Shade/Singh 2016: 1-12, Bulger/McCormick/Pitcan 2017, Lievens/Livingstone/McLaughlin/O'Neill /Verdoodt 2018: 1-27). A father mentioned parent concerns over school use of children's thumbprints (to pay for lunch), noting ruefully that the school implemented this use of biometric data notwithstanding:

> Well, the thing is information is collected everywhere even if you're not aware it's being collected, isn't it, nowadays? So, when a child's at school, I know the school has those biometric [thumb prints] ... There was a bit of hoo-ha about it, but it still went ahead. So that information's collected, isn't it? Someone's got the thumb print somewhere stored.

Such concerns are motivated – perhaps also reinforced– by the increasing sponsorship of schools by big companies (in the UK, the pressing decision is, as it is colloquially expressed, whether to become a "Google" or a "Microsoft" school).

In general, however, the children, parents and teachers interviewed were very confident of their interpersonal privacy management – asking permission before taking or posting photos of the students, for instance; and fairly confident of their institutional privacy management (describing the GDPR (General Data Protection Regulation) training and procedures, assuring us of the school's trustworthy approach to storing sensitive data

on special educational needs or family problems or student grades). They were also excited about the involvement in education of big companies, seeing this as a way of preparing for the "digital future," hoping to benefit from the latest opportunities rather than being stuck behind the times.

But their accounts faltered when they were asked about commercial privacy management – as one parent noted, when discussing the tracking that might occur when iPads are provided to students, "our kids are the guinea pig generation." Parents and teachers seemed uncertain, for instance, about the use of student data for tracking and learning analytics by Capita SIMS or ClassDojo or Show My Homework or cloud storage services or any of the commonly used software – at first telling the researchers confidently that student data never leaves the school, then realizing they might, then looking worried as they have no answer to questions about third party sharing ("that's not at our level," one told the researchers). One school's "technical learning officer" admitted that he was not aware of what kind of data are being gathered about the children or how identifiable they are but expects that data are both detailed and shared with the council, researchers and companies (in this case, Google). Children in his school are, as he put it, "tracked all the time," and he was optimistic that the school will gain better intelligence it can use to the benefit of the students. More commonly, a sense of fatalism regarding the data economy pervaded the interviews, with the exception of one business studies teacher who pushes back robustly that it is how the economy works:

> I'm just looking at it from a business point of view. I don't see why that is a concern […] It just drives the economy forward. We've been doing this for 50 years in a sense of after cartoons, there's toy adverts… So it's not. No real difference. It's just a clever, more advanced way of doing it.

The recent and widespread success of introducing e-safety into British schools, however, combined with the tendency to conceive of privacy primarily in interpersonal terms, means that children – and, indeed, parents and teachers, are tempted to think that privacy and data literacy could be incorporated within existing lessons about personal safety online. Ironically, it is not until one recognizes the existence and complexity of the political economy and commercial infrastructure of the emerging digital environment that the need for a critical knowledge of it is fully appreciated. Again, this is the case with most curriculum subjects, and why a pedagogic solution which goes beyond what children may initially ask for is needed.

The findings suggest that such a solution will be welcome. In focus groups, children were keen to discuss the tech news they hear through the

mass media – often the scandals involving the major platforms, the latest data breach or tragic suicides linked to social media, but also news about emerging innovations – smart devices, robots, and developments in artificial intelligence. The message was clear: they consider themselves the generation that will live their lives in and through technology, so they want to understand it. But their enthusiasm for discussing the latest tech news, sharing stories of what went wrong or figuring out for themselves how things work is often a world away from how they talk about lessons. In a rapidly changing digital environment children often feel that the curriculum is lagging behind and educational interventions at school happen mainly when something goes wrong. Much less involved in using the apps and devices, parents and teachers have limited knowledge, at best, and children often prefer to learn by trial and error on their own.

Parents, however, both trust and rely on the school to teach their children data and privacy literacy, not least because their own knowledge is hugely variable. One mother had been hacked, found it terrifying, and had relatives engaged in an online privacy-related court case; yet when asked how the school protected sensitive data regarding her autistic son, she said "I don't know" and "I haven't really thought about it." A father who worked in the digital sector knew so much that, after regaling us with all the risks – cybercrime, fraud, identity theft, etc. – he concluded that there is nothing really to be done, "that's just the nature of the internet" and it's a scary world. Another father, who had "worked in the internet since it started," wants data profiling and discrimination taught in citizenship classes as it would be unfair and unequal to demand that parents understand such things:

> I think that should be part of citizenship, that they're learning in schools about how all of this impacts. Because, I don't know much about profiling, to be honest.

Certainly, some parents know very little: one mother was unaware of privacy-protecting tactics such as incognito browsing or deleting one's search history but had a daughter with good digital privacy skills.

Existing research shows that, while most teachers (99%) believe they have the greatest responsibility for helping children develop online literacy skills, more than half (54%) think that the national curriculum does not teach children the digital literacy skills they need, and over a third (35%) feel that the digital literacy skills taught in schools are not transferable to the 'real world' (National Literacy Trust 2018). The teachers interviewed were ambivalent about teaching data and privacy literacy – they felt they keep telling the students to be careful and sensible but found repeating the

same message over and again ineffective. They are keen that parents should take more responsibility to bring up their children to be aware, critical and cautious about the digital environment, and that secondary school (in the UK, from 11 years old) is already late to begin educating tomorrow's "digital citizens."

At the same time, teachers are critical of parents – seeing them as too disengaged, or unaware, or panicky. They also worry about being overwhelmed by parental demands when they use messaging systems to communicate with parents, while children told us they distrust this form of tracking or that their parents are reluctant to download the apps in the first place. As regards social media use, teachers tended to be critical of the children also, disapproving of their fascination with selfies, susceptibility to online persuasion and peer pressure, dishonesty in lying about their age or setting up fake profiles, foolishness for posting indecent images, naivety about the future consequences of their actions, and overconfidence in thinking they know it all.

Still, both parents and teachers recognized that children need to discover how to behave online, to be allowed the freedom to make mistakes and learn from them, and not to be overburdened by expectations to understand a very complicated, and generally not child-friendly, digital environment. Parents and teachers trusted the children to know what they are doing and to seek help when they need it and wanted to create a learning environment where children are active and independent agents.

4. Conclusion

The main purpose of this chapter has been to identify what children understand about their data and privacy online, in order to frame the educational challenge for teaching data and privacy literacy, whether within the media education curriculum or elsewhere – for instance, in the computing or citizenship curricula. From the systematic evidence mapping and primary research with children, parents and teachers, it can be argued first, that it is not enough for children to gain functional skills to consider what personal data they provide, manage their privacy settings or respond to data protection options provided by online services. To enact their rights as agents and citizens in a complex datafied society, they also need some measure of critical understanding of the networked data economy which is fueled not only by data given but also data traces and inferred or profiled data.

Improving children's data and privacy literacy is a demanding media education task in its own right. It is made more complex by the fact that children are already familiar with interpersonal privacy contexts, with younger children especially tending to assume that values and practices appropriate to interpersonal relations also apply in institutional and commercial contexts, even though this is often inappropriate and results in misunderstandings. However, the workshops with children revealed that they are keen to deepen their understanding of data and privacy online, wanting to know who has their data, what they do with it and why. None of these questions can be answered by simple answers, awareness-raising campaigns or other quick fixes. Add to this the complexity involved in answering the other questions children ask, and it is clear that an educational strategy is needed. In other words, children implicitly recognize this as an expert domain which they should be taught something about.

Although many are tempted to assimilate data and privacy literacy to the now-familiar teaching of e-safety, the knowledge required, and the implications for the curriculum, are distinctive and, therefore, best addressed separately. However, the very complexity of today's data economy places limits on what teachers can be trained and resourced to teach. Nor can either parents or teachers be burdened with ensuring children understand a digital environment which governments, regulators and businesses are all struggling to manage.

A second purpose of this chapter, therefore, has been to call attention to the complementary obligations and responsibilities of others, especially businesses and regulators. Children not only want to know more but they want changes from the digital environment and, reasonably so, whether or not such changes are feasible or forthcoming. Media literacy is always co-dependent on the nature of the media environment – if the latter is opaque or "illegible" (Livingstone 2008: 51-62), the task of media educators is made all the more difficult. Conversely, the more the media environment adjusts to meet the needs and rights of its users, the more media education can focus on empowerment rather than harm mitigation.

By conceptualizing privacy in contextual terms, this argument can be extended directly to the present case. In short, to the extent that the commercial digital environment is opaque and unaccountable or even exploitative in its treatment of users' data (Norwegian Consumer Council 2018), the more knowledge and support users will require to maintain the privacy necessary to human agency and dignity in the digital age. Thus, at a policy level, the provision of digital literacy in schools must be considered hand in hand with questions of data protection regulation.

In the process of researching this question through fieldwork in schools highlights the unique position of the school in this regard, being an institution tasked both with educating its students and managing their personal data. Just as with citizenship education, in relation to data protection the school is not only the site of education but also a microcosm of the wider society: if children are not treated as independent rights-holders at school, the teachers will lack credibility in teaching them about democracy (Frau-Meigs/Hibbard 2016). Similarly, unless schools are transparent and accountable in their processing of student data, they can hardly teach data and privacy literacy to those same students. Put positively, it is open to schools as institutions with considerable data protection responsibilities to become beacons of good practice, thereby demonstrating to children and parents how their privacy rights can be realized in the digital environment and influencing their expectations for other, usually commercial contexts. This would surely ease the increasingly important task of providing data and privacy literacy education for children.

References

Aufderheide, Patricia (1993): *Media Literacy: A Report of the National Leadership Conference on Media Literacy*. Aspen Institute, Communication and Society Program. Retrieved from: https://files.eric.ed.gov/fulltext/ED365294.pdf (last accessed on October 1, 2020).

Buckingham, David (2015): *Defining Digital Literacy – What do young people need to know about digital media?* In: Nordic Journal of Digital Literacy 10, S. 21–35.

Bulger, Monica / McCormick, Patrick / Pitcan, Mikaela (2017): *The Legacy of inBloom*. Retrieved from: https://datasociety.net/pubs/ecl/InBloom_feb_2017.pdf (October 1, 2020).

Bulger, Monica / Davison, Patrick (2018): *The Promises, Challenges, and Futures of Media Literacy*. Retrieved from: https://datasociety.net/pubs/oh/DataAndSociety_Media_Literacy_2018.pdf (October 1, 2020).

European Audiovisual Observatory (2016): *Mapping of Media Literacy Practices and Actions in EU-28*. Strasbourg: European Audiovisual Observatory. Retrieved from: https://rm.coe.int/0900001680783500 (October 1, 2020).

Frau-Meigs, Divina / Hibbard, Lee (2016): *Education 3.0 and Internet Governance: A new global alliance for children and young people's sustainable digital development*. London: Chatham House. Retrieved from: https://www.cigionline.org/sites/default/files/gcig_no27web_0.pdf (October 1, 2020).

Goffman, Erving (1971): *The Presentation of Self in Everyday Life*. Harmondsworth: Penguin. Retrieved from: https://monoskop.org/images/1/19/Goffman_Erving_The_Presentation_of_Self_in_Everyday_Life.pdf (October 1, 2020).

Hartley, John (2011): *The Uses of Digital Literacy*. New Jersey: Rutgers.

Hasselbalch Lapenta, Gry / Jørgensen, Rikke Frank (2015): *Youth, Privacy and Online Media: Framing the right to privacy in public policy-making*. In: First Monday 20(3). Retrieved from: https://journals.uic.edu/ojs/index.php/fm/article/view/5568/4373 (October 1, 2020).

Kellner, Douglas / Share, Jeff (2007): *Critical Media Literacy Is Not an Option*. In: Learning Inquiry 1(1), S. 59-69.

Lievens, Eva / Livingstone, Sonia / McLaughlin, Sharon / O'Neill, Brian / Verdoodt, Valerie (2018): *Children's Rights and Digital Technologies*. In: U. Kilkelly / T. Liefaard (Hg.): International Human Rights of Children. Singapore: Springer Singapore, S. 1-27.

Livingstone, Sonia (2008): *Engaging with Media – A matter of literacy?* In: Communication, Culture & Critique 1(1), S. 51-62.

Livingstone, Sonia (2018): *Children: a special case for privacy?* In: Intermedia 46(2), S. 18-23. Retrieved from: http://eprints.lse.ac.uk/89706/ (October 1, 2020).

Livingstone, Sonia / Ólafsson, Kjartan (2018): *When do Parents Think Their Child is Ready to Use the Internet Independently?* In: Department of Media and Communications, The London School of Economics and Political Science: Parenting for a Digital Future: Survey Report 2., Retrieved from: http://eprints.lse.ac.uk/87953/ (October 1, 2020).

Lupton, Deborah / Williamson, Ben (2017): *The datafied child: The dataveillance of children and implications for their rights.* In: New Media & Society 19(5), S. 780-794.

Livingstone, Sonia / Blum-Ross, Alicia / Zhang, Dongmiao (2018): *What Do Parents Think, and Do, about Their Children's Online Privacy?* In: Department of Media and Communications, The London School of Economics and Political Science: Parenting for a Digital Future: Survey Report 3. Retrieved from: http://eprints.lse.ac.uk/87954/ (October 1, 2020).

Livingstone, Sonia / Stoilova, Mariya / Nandagiri, Rishita (2019a): *Children's Data and Privacy Online: Growing up in a digital age. An evidence review*. London: London School of Economics and Political Science. Retrieved from: http://eprints.lse.ac.uk/101283/1/Livingstone_childrens_data_and_privacy_online_evidence_review_published.pdf (October 1, 2020).

Livingstone, Sonia / Stoilova, Mariya / Nandagiri, Rishita (2019b): *Talking to Children about Data and Privacy Online: Research methodology*. London: London School of Economics and Political Science. Retrieved from: http://eprints.lse.ac.uk/101284/ (October 1, 2020).

McDougall, Julian / Livingstone, Sonia / Sefton-Green, Julian / Fraser, Sharon P (2014): *Media and Information Literacy Policies in the UK*. In: Report for the COST (Transforming Audiences, Transforming Societies) initiative, Mapping Media Education Policies. Retrieved from: http://eprints.lse.ac.uk/57103/ (October 1, 2020).

Micheti, Anna / Burkell, Jacquelyn / Steeves, Valerie (2010): *Fixing Broken Doors: Strategies for drafting privacy policies young people can understand*. In: Bulletin of Science, Technology and Society 30(2), S. 130-43.

National Literacy Trust (2018): *Fake news and critical literacy: The final report of the Commission on Fake News and the teaching of critical literacy in schools.* London: National Literacy Trust. Retrieved from: https://literacytrust.org.uk/research-services/research-reports/fake-news-and-critical-literacy-final-report/ (October 1, 2020).

Nissenbaum, Helen (2004): *Privacy as contextual integrity*. In: Washington Law Review 79, S. 119–157.

Norwegian Consumer Council (2018): *Deceived by Design: How tech companies use dark patterns to discourage us from exercising our rights to privacy*. Oslo: Forbrukerrådet. Retrieved from: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf (October 1, 2020).

O'Hara, Kieron (2016): *The Seven Veils of Privacy*. In: IEEE Internet Computing 20, S. 86-91.

Shade, Leslie Regan / Singh, Rianka (2016): *'Honestly, We're Not Spying on Kids': School surveillance of young people's social media.* In: Social Media and Society 2, S. 1-12.

Stoilova, Mariya / Livingstone, Sonia / Nandagiri, Rishita (2020): *Digital by default: children's capacity to understand and manage online data and privacy*. Media and Communication, 8(4), DOI: http://dx.doi.org/10.17645/mac.v8i4.3407.

van der Hof, Simone (2016): *I Agree, or Do I? A rights-based analysis of the law on children's consent in the digital world*. In: Wisconsin International Law Journal 34(2), S. 409-45.

Williamson, Ben (2017): *Learning in the 'Platform Society': Disassembling an educational data assemblage*. In: Research in Education 98(1), S. 59-82.

Zuboff, Shoshana (2019): *The Age of Surveillance Capitalism: The fight for a human future at the new frontier of power*. London: Profile Books.