Children's data and privacy online

Growing up in a digital age

An evidence review

Sonia Livingstone • Mariya Stoilova • Rishita Nandagiri

January 2019

LSE Media and Communications

ico. Information Commissioner's Office — Grant Recipient

Preferred citation:
Livingstone, S. Stoilova, M. and Nandagiri, R. (2019) Children's data and privacy online: Growing up in a digital age. An evidence review. London: London School of Economics and Political Science.

Table of contents

Cover image: Max Pixel

1. Executive summary

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. In a digital age in which many everyday actions generate data – whether given by digital actors, observable from digital traces, or inferred by others, whether human or algorithmic – the relation between privacy and data online is becoming highly complex. This in turn sets a significant media literacy challenge for children (and their parents and teachers) as they try to understand and engage critically with the digital environment.

With growing concerns over children's privacy and the commercial uses of their data, it is vital that children's understandings of the digital environment, their digital skills and their capacity to consent are taken into account in designing services, regulation and policy. Using systematic evidence mapping, we reviewed the existing knowledge on children's data and privacy online, identified research gaps and outlined areas of potential policy and practice development.

Key findings include:

- Children's online activities are the focus of a multitude of monitoring and data-generating processes, yet the possible implications of this '**datafication of children'**[1] **has only recently caught the attention** of governments, researchers and privacy advocates.

- **Attempts to recognise children's right to privacy on its own terms are relatively new** and have been brought to the fore by the adoption of the European General Data Protection Regulation (GDPR, 2018) as well as by recent high-profile privacy issues and infringements.

- In order to capture the full complexity of children's privacy online, we distinguish among: **(i) interpersonal privacy** (how my 'data self' is created,[2] 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); and **(iii) commercial privacy** (how my personal data is harvested and used for business and marketing purposes).

- The key privacy challenge (and paradox) currently posed by the internet is the simultaneous interconnectedness of voluntary sharing of personal information online, important for children's agency, and the attendant threats to their privacy, also important for their safety. While **children value their privacy and engage in protective strategies**, they also greatly appreciate the ability to engage online.

- Individual **privacy decisions and practices are influenced by the social environment**. Children negotiate sharing or withholding of personal information in a context in which networked communication and sharing practices shape their decisions and create the need to balance privacy with the need for participation, self-expression and belonging.

- Institutionalised aspects of privacy, where data control is delegated – voluntarily or not – to external agencies such as government institutions, is becoming the norm rather than the exception in the digital age. Yet there are **gaps in our knowledge of how children experience institutional privacy**, raising questions about informed consent and children's rights.

- The invasive tactics used by marketers to collect personal information from children have aroused data privacy and security concerns particularly relating to children's

[1] 'Datafication' refers to the process of intensified monitoring and data gathering in which people (including children) are quantified and objectified – positioned as objects (serving the interests of others) rather than subjects (or agents of their own interests and concerns); see Lupton, D. and Williamson, B. (2017) The datafied child: The dataveillance of children and implications for their rights. *New Media & Society* 19(5), 780-94.

[2] 'Data self' refers to all the information available (offline and online) about an individual.

ability to understand and consent to such datafication and the need for parental approval and supervision, especially for the youngest internet users. While the commercial use of children's data is at the forefront of current privacy debates, the empirical evidence related to children's experiences, awareness and competence regarding privacy online lags behind. The available evidence suggests that **commercial privacy is the area where children are least able to comprehend and manage** on their own.

- **Privacy is vital for child development** – key privacy-related media literacy skills are closely associated with a range of child developmental areas. While children develop their privacy-related awareness, literacy and needs as they grow older, even the oldest children struggle to comprehend the full complexity of internet data flows and some aspects of data commercialisation. The child development evidence related to privacy is insufficient but it undoubtedly points to the need for a tailored approach which acknowledges developments and individual differences amongst children.

- Not all children are equally able to navigate the digital environment safely, taking advantage of the existing opportunities while avoiding or mitigating privacy risks. The evidence mapping demonstrates that **differences among children (developmental, socio-economic, skill-related, gender- or vulnerability-based) might influence their engagement with privacy online**, although more evidence is needed regarding the consequences of differences among children. This raises pressing questions for media literacy research and educational provision. It also invites greater attention to children's voices and their heterogeneous experiences, competencies and capacities.

- Privacy concerns have intensified with the introduction of digital technologies and the internet due to their capacity to compile large datasets with dossiers of granular personal information about online users. **Children are perceived as more vulnerable than adults to privacy online threats** due to their lack of digital skills or awareness of privacy risks. While issues such as online sexual exploitation and contact with strangers are prominent in current debates, more research is needed to explore potential links between privacy risks and harmful consequences for children, particularly in relation to longer-term effects.

- No longer about discipline and control alone, surveillance now contains facets of 'care' and 'safety', and is promoted as a reflection of responsible and caring parents and is thus normalised. **Risk aversion, however, restricts children's play, development and agency**, and constrains their exploration of physical, social and virtual worlds.

- While the task of balancing children's independence and protection is challenging, evidence suggests that **good support can make an important difference to children's privacy online**. Restrictive parenting has a suppressive effect, reducing privacy and other risks but also impeding the benefits of internet use. Enabling mediation, on the other hand, is more empowering in allowing children to engage with social networks, albeit also experiencing some risk while learning independent protective behaviours.

- While the evidence puts parental enabling mediation at the centre of effective improvement of children's privacy online, platform and app features often prompt parental control via monitoring or restriction rather than active mediation. **Media literacy resources and training for parents, educators and child support workers** should be considered as the evidence suggests important gaps in adults' knowledge of risks and protective strategies regarding children's data and privacy online.

- The evidence also suggests that **design standards and regulatory frameworks are needed which account for children's overall privacy needs across age groups**, and pay particular attention and consideration to the knowledge, abilities, skills and vulnerabilities of younger users.

2. Acknowledgements

We are grateful to the Information Commissioner's Office (ICO) for funding this project. In particular, we would like to thank the team – Robert McCombe, Lisa Atkinson, Adam Stevens, Lisa O'Brien and Rachel Bennett – for their support.

We are thankful to our expert advisory group members for sharing valuable recommendations:

Jonathan Baggaley (PSHE Association)

Dr Ayelet Blecher-Prigat (Academic College for Law and Science)

Dr Leanne Bowler (Pratt Institute)

Dr Monica Bulger (Future of Privacy Forum and Data & Society Research Institute)

John Carr, OBE (Children's Charities' Coalition on Internet Safety)

Professor Nick Couldry (Department of Media and Communications, LSE)

Jutta Croll (Stiftung Digitale Chancen)

Julie de Bailliencourt (Facebook)

Anna Fielder (Privacy International)

Kerry Gallagher (ConnectSafely.org)

Patrick Geary (UNICEF)

Emily Keaney (Office of Communications)

Louis Knight-Webb (Who Targets Me)

Professor Eva Lievens (Law Faculty, Ghent University)

Claire Lilley (Google)

Dr Orla Lynskey (LSE Law)

Louise Macdonald (Young Scot)

Alice Miles (Office of the Children's Commissioner)

Andrea Millwood-Hargrave (International Institute of Communications)

Dr Kathryn Montgomery (School of Communication, American University)

Dr Victoria Nash (Oxford Internet Institute)

Dr Elvia Perez Vallejos (University of Nottingham)

Jen Persson (DefendDigitalMe)

Joseph Savirimuthu (University of Liverpool)

Vicki Shotbolt (Parent Zone)

Professor Elisabeth Staksrud (University of Oslo)

Dr Amanda Third (University of Western Sydney)

Josie Verghese (BBC School Report)

Dr Pamela Wisniewski (University of Central Florida

We also thank the LSE Research Division and James Deeley at the LSE Department of Media and Communications for their ongoing project support and assistance, and Heather Dawson at the British Library of Political and Economic Science for her expert suggestions and guidance with relevant databases and sources.

3. Introduction

3.1. Context

The nature of privacy is increasingly under scrutiny in the digital age, as the technologies that mediate communication and information of all kinds become more sophisticated, globally networked and commercially valuable. The conditions under which privacy can be sustained are shifting, as are the boundaries between public and private domains more generally. In public discourse, widely expressed in the mass and social media, there is a rising tide of concern about people's loss of control over their personal information, their understanding of what is public or private in digital environments and the host of infringements of privacy resulting from the actions (deliberate or unintended) of both individuals and organisations (especially state and private sector), as well as from hostile or criminal activities.

Our focus is on privacy both as a fundamental human right vital to personal autonomy and dignity and as the means of enabling all the activities and structures of a democratic society. Within this, it is the transformation in the conditions of privacy wrought by the developments of the digital age that occupy our attention in this report. These centre on the creation of data – which can be recorded, tracked, aggregated, analysed (via algorithms and increasingly, via artificial intelligence) and 'monetised' – from the myriad forms of human communication and activity which, throughout history, have gone largely unrecorded, being generally unnoticed and quickly forgotten.

The transformation of ever more human activities into data means that privacy (rather than publicity) now requires a deliberate effort, that it is far easier to preserve than remove the record of what has been said or done, that surveillance by states and companies is fast becoming the norm not the exception, and that our data self (or 'digital footprint') represents not merely a shadow of our 'real' self but rather, a real means by which our options become determined for us by others, according to their (rather than, or at best, as well as our own) interests.

The position of children's privacy in the digital environment is proving particularly fraught for three main reasons. First, children are often the pioneers in exploring and experimenting with new digital devices, services and contents – they are, in effect, the canary in the coal mine for wider society, encountering the risks before many adults become aware of them or are able to develop strategies to mitigate them. Although children have always been experimental, even transgressive, today these actions are particularly consequential, because children now act on digital platforms that both record everything and, being often proprietary, own the resulting data traces (Montgomery, 2015). The growing 'monetisation', 'dataveillance', 'datafication' and sometimes misuse or 'hacking' of children's data, and thereby privacy, is occasioning considerable concern in public and policy circles. While it is often children's transgressive or 'risky opportunities' (Livingstone, 2008) that draw attention to the added complexities of the digital environment, these raise a more general point. In the digital age, actions intended by individuals to be either *private* (personal or interpersonal) or *public* (oriented to others, of wide interest, a matter of community or civic participation) in nature now take place on digital networks owned by the *private* sector, thereby introducing commercial interests into spheres where they were, throughout history, largely absent (Livingstone, 2005).

Second, despite their facility with and enthusiasm for all things digital, children have less critical understanding of present and future risks to their wellbeing posed by the use of the digital environment than many adults. Most research attention has concentrated on teenagers, but increasingly the very youngest children are becoming regular uses of the internet (Chaudron et al., 2018). So, too, are those who are 'at risk' or in some ways vulnerable as regards their mental or physical health or their socio-economic or family circumstances. This raises new challenges regarding the demands on children's media literacy (especially its critical dimensions) as well as that of the general public (including parents and teachers). Meeting these challenges inclusively and at scale is generally seen as the remit of educators, yet the task may be too great, insofar as understanding the complexities of digital data processes and markets is proving beyond the wit of most adults.

Third, children's specific needs and rights are too little recognised or provided for by the design of the digital environment and the regulatory, state and commercial organisations that underpin it

(Livingstone et al., 2015). Here there are growing calls for regulatory intervention, again on behalf of children and also the general public, including for mechanisms even to know who is a child online and for privacy-by-design (along with safety- and ethics-by-design) to become embedded in the digital environment, so that children's specific rights and needs – including regarding their personal data – are protected (Kidron et al., 2018). The recent Recommendation from the Council of Europe (2018) on guidelines to protect, respect and fulfil the rights of children in the digital environment offers a comprehensive framework, and something of a moral compass for states, as they seek to address the full range of children's rights specifically in relation to the internet and related digital technologies. Within this, privacy and data protection are rightly prominent.

In Europe, 2018 saw the implementation of wide-ranging new legislation in the form of the General Data Protection Regulation (GDPR), incorporated into UK law by the Data Protection Act 2018. This recognises that 'personal data protection is a fundamental right in the EU' (Jourová, 2018) and seeks to return a measure of control to the individual (or internet user) regarding their privacy online. In a series of policy documents, the UK's data protection authority, the Information Commissioner's Office (ICO), explains the implications of the GDPR for UK citizens in general and for children in particular.[3] As regards the latter, Recital 38 of the GDPR sets out the imperative for regulatory provision to protect children's data:

> 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.

The ICO recently held a consultation[4] on how such protection can and should be achieved for children and a number of pressing challenges are already becoming apparent (Livingstone, 2018). In this review, our concern is less with the specifics of regulation and more with the conditions under which children use the internet, the implications of their activities (and those of others) for the personal data that is collected and analysed about them and especially, how children themselves understand and form views regarding their privacy, the uses of their data and the implications for their engagement with the digital environment – all part of their media literacy. GDPR Recital 38 makes clear reference to children's vulnerabilities, their awareness of online risks and the adverse consequences to their privacy that regulation should seek to prevent.

However, throughout the consultations and deliberations during the long build-up to the GDPR, children's views were barely included, and research with or about children was little commissioned or considered. Nonetheless, the GDPR builds on a series of assumptions regarding the maturity of children (to give their consent) and the role of parents (in requiring their consent for the use of data from under-age children), most notably in relation to GDPR Article 8.[5] It also presumes knowledge of how children can understand the Terms and Conditions of the services they use (in requiring that these be comprehensible to services users), the risks that face children (in the requirement for risk impact assessments) and more. Hence our primary question – what do children understand and think about their privacy and use of personal data in relation to digital, especially commercial, environments?

[3] For details, see *Children and the GDPR* (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/) and *Guide to the General Data Protection Regulation* (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/).

[4] See *Call for evidence – Age-appropriate design code* (https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/call-for-evidence-age-appropriate-design-code/).

[5] Parental consent is required for underage children only when data is processed on the basis of consent (rather than another basis for processing, such as contract, legal obligation, vital interests, public task or legitimate interests). For more details see: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

3.2. Aims of the project and the evidence review

With growing concerns over children's privacy online and the commercial uses of their data, it is vital that children's understandings of the digital environment, their digital skills and their capacity to consent are taken into account in designing services, regulation and policy. Our project Children's data and privacy online: growing up in a digital age seeks to address questions and evidence gaps concerning children's conception of privacy online, their capacity to consent, their functional skills (e.g., in understanding terms and conditions or managing privacy settings online) and their deeper critical understanding of the online environment, including both its interpersonal and especially, its commercial, dimensions (its business models, uses of data and algorithms, forms of redress, commercial interests, and systems of trust and governance). The project also explores how responsibilities should be apportioned among relevant stakeholders and the implications for children's wellbeing and rights.

The project takes a child-centred approach, arguing that only thus can researchers provide the needed integration of children's understandings, online affordances, resulting experiences and wellbeing outcomes (Livingstone and Blum-Ross, 2017). Methodologically, the project prioritises children's own voices and experiences within the wider framework of evidence-based policy development by conducting focus group research with children of secondary school age, their parents and educators, from selected schools around the country; organising child deliberation panels for formulating child-inclusive policy and educational/awareness-raising recommendations; and creating an online toolkit to support and promote children's digital privacy skills and awareness.

Given current regulatory decisions regarding children's awareness of and capacity to manage digital risks and their consequences for their wellbeing – manifest in policies for privacy-by-design, child protection, child and parent consent, minimum age for use of services, and so forth – the project focuses on children aged 11 to 16 (Livingstone, 2014; Kidron and Rudkin, 2017; Macenaite, 2017; UNICEF, 2018).

The aim of the evidence review is to gather, systematise and evaluate the existing evidence base on children's privacy online, particularly focusing on key approaches to the study of children's privacy in the digital environment; children's own understandings, experiences and views of privacy online; their approach to navigating the internet and its commercial practices; their experiences of online risks and harm; ways of supporting children's privacy and media literacy; and how differences in age, development and vulnerability make a difference.

4. Methodology

The research questions guiding the review are:

- How do children understand, value and negotiate their privacy online?
- What are the digital skills, capabilities or vulnerabilities with which children approach the digital environment?
- What are the significant gaps in knowledge about children's online privacy and commercial use of data?

We conducted a systematic mapping of the evidence (Grant and Booth, 2009; Gough et al., 2012; EPPI-Centre, 2018), utilising a comprehensive and methodical search strategy, allowing us to include a broad range of sources including policy recommendations, case studies and advocacy guides. Here we summarise our methodology briefly. For a detailed account of the methodology, including search terms, databases, inclusion criteria and screening and coding protocols, see Appendix 1.

Three groups of search terms were combined, to identify research about children, privacy and the digital environment (primarily the internet, but including all digital devices, content and services that can be connected to it). This demanded a particularly multidisciplinary approach to the research framing and interpretation of results.

We identified three disciplines relevant to the scope of the review – social and cultural studies, legal and regulatory studies, and technological/computer sciences (see Figure 1), with databases and search terms (children, privacy, digital) chosen to match these three areas. This review focuses on the overlap between the three areas, centring on the privacy and data literacy of children.

Figure 1: Concept mapping of three disciplines and their overlaps

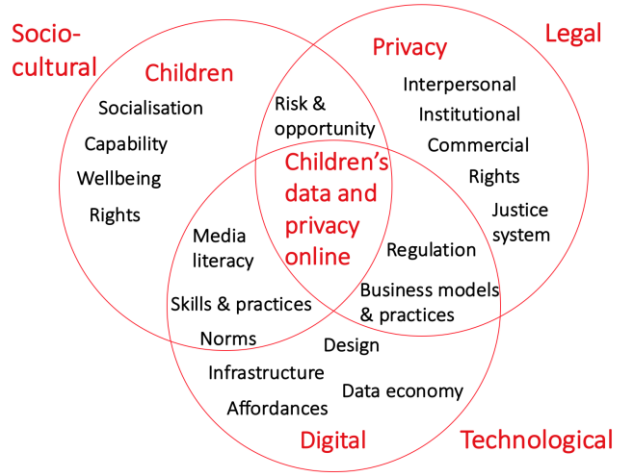


Table 1: Results by category

Category	Type	Number of studies
Type of study (*n* = 105)	Primary research	99
	Secondary data analysis	6
Methodology (*n* = 105)	Survey	33
	Mixed-methods	20
	Interviews	15
	Experimental or quasi-experimental	10
	Participatory	8
	Secondary analysis	6
	Focus group discussions	5
	Observational	4
	Other	4
Age (coded across multiple categories)	Age 0-3	2
	Age 4-7	10
	Age 8-11	46
	Age 12-15	77
	Age 16-19	64
	Could not categorise	3
Study focus (coded across multiple categories)	Behaviours and practices	67
	Attitudes and beliefs	50
	Media literacy and understandings	37
	Privacy strategies of the child	27
	Support and guidance from others	9
	Design and interface (affordances)	5
	Decision-making to use services	2
Type of privacy (coded across multiple categories)	Interpersonal	86
	Commercial	37
	Institutional	8
Data type (coded across multiple categories)	Data given	93
	Data traces	27
	Inferred data	7

The systematic evidence mapping included an extensive search of 19 databases that covered the social sciences, legal studies and computer science disciplines, resulting in 9,119 search items. We consulted our expert advisory group for additional relevant literature, adding 279 more items to our review. This gave us a total of 9,398 search results. We screened these results for duplicates and relevance, leaving a total of 6,309 relevant results. Using a predefined inclusion criteria and a two-phase process, we narrowed the results to a final sample of 105 studies (see Table 1 above and the Report Supplement for a summary of each source).

We limited the resulting sources to empirical research studies with children, including both primary and secondary data analysis studies. Summaries of these studies can be found in the Report supplement.

The primary research studies draw more on quantitative than qualitative methodologies, with a significant number using mixed-methods approaches. We also categorised the empirical studies by age, study focus and the types of privacy and data investigated. Studies tend to focus on children across different age groups, with a majority of them focusing on 12- to 19-year-olds. There is a dearth of research on 0- to 7-year-olds, and to a lesser but still significant extent for 8- to 11-year-olds. The studies focus predominantly on the behaviours and practices of young people, as well as on their attitudes and beliefs. We also categorised the types of privacy explored in our sample, finding that interpersonal privacy is, by far, the most frequently addressed. This is also reflected in the types of data investigated in our sample, where data given is the most common type of data explored.

In what follows we begin with a conceptual analysis of privacy in the digital age, moving, then, to empirical findings regarding children's understanding of privacy in relation to digital and non-digital environments.

5. Children's privacy online: key issues and findings from the systematic evidence mapping

We first explore the key areas related to children's privacy online which we identified during the systematic evidence mapping, starting with how privacy has been conceptualised in relation to the digital environment, the key dimensions that constitute child privacy and the types of data involved, and the links between privacy and child development. We then focus on how children manage (and negotiate) their privacy online and the protection strategies they employ. We also consider how differences among children might put some children in particularly vulnerable situations, and review the privacy-related risks and harm that children face. Finally, we review the evidence on privacy protection, children's autonomy and best approaches to supporting children's privacy online.

5.1. Conceptualising privacy in the digital age

Definitions of privacy can be difficult to apply in the digital environment, as are efforts to measure privacy empirically (Solove, 2008). From Westin (1967: 7) we find the classic conceptualisation of privacy: 'the claim of individuals, groups, or institutions to determine themselves when, how and to what extent information about them is communicated to others'. The tensions Westin identified between privacy, autonomy and surveillance apply strongly in the contemporary digital environment, even though his work was written much earlier. Recent theoretical approaches also tend to define privacy online in terms of individual control over information disclosure and visibility (Ghosh et al., 2018), but they seek ways of acknowledging how this control depends on the nature of the social and/or digital environment.

Thus contextual considerations are increasingly important in discussions of privacy. Nissenbaum's (2004) theory of *privacy as contextual integrity* refers to the negotiation of privacy norms and cultures. For her, information sharing occurs in the context of politics, convention and cultural expectations, guided by norms of appropriateness, distribution of information and violation. Hence these norms must be examined and taken into account when making judgements about privacy and privacy-related actions.

Another approach, *communication privacy management theory*, focuses on the relational context, framing privacy as a process of boundary negotiation within specific interpersonal relationships. Thus privacy emerges from (or is infringed by) the negotiation over the social rules over what information is shared, when and with whom, and how these rules are agreed with others (Petronio, 2002). Increasingly it is argued that privacy is better understood in relational rather than in individual terms (Solove, 2015; Hargreaves, 2017). Rather than focusing on an individual's intent to control their information, it can be more productive to understand how privacy-related actions – for instance, to keep or tell a secret, to disclose sensitive information to others, to collaborate with others to establish social norms for information sharing – depend on and are meaningful within the specific relationships (and their contexts, norms and boundaries) to which individuals are party. These actions are embedded in a context of norms, legal and policy regulations, and rights (O'Hara, 2016).

To conceptualise privacy in the digital age, we start by observing how the nature of the digital environment adds complexity to the social environment, especially with the widespread adoption of social media. boyd and Marwick (2011) use the notion of *networked privacy* to refer to the public-by-default nature of personal communications in the digital era, thus affecting the decisions of individuals about what information to share or withhold. They outline four key affordances (or socially designed features of the digital environment) of networked technologies: persistence, replicability, scalability and searchability. These affordances mean that people must contend with dynamics not usually encountered in daily life before, over and above the established demands of social interaction. These include the imagined audience for online posts/performances, the collapse and collision of social contexts, the blurring of public and private spheres of activity, and the nature of network effects (notably, the ways in which messages spread within and across networks).

One consequence is that where social interactions used to be private-by-default, they are increasingly becoming public-by-default, with privacy achieved 'through effort' rather than something to be taken for granted. Another is that where social interactions used to be typically (although not necessarily) ephemeral, they are increasingly digitally recorded through digital traces that are themselves amenable to further processing and analysis, whether for individual or organisational (public or commercial) benefit. Yet another is that, because of the affordances of online environments (including the conditions of identifiability or anonymity, as well as the effects of particular regulation or design), people tend to act differently online than offline.

Studies suggest that the mediated nature of social network communication facilitates greater self-disclosure of personal information than face-to-face interaction (Xie and Kang, 2015). The importance of online self-representation and identity experiments to youthful peer cultures also fuels online sharing of personal information. In these contexts teenagers may prioritise what to protect more than what to disclose, with exclusions carefully considered (boyd and Marwick, 2011). Steeves and Regan (2014) identify four different understandings of the value of privacy by young people: contextual, relational, performative and dialectical. Contextual understandings relate to how privacy is guided by certain norms and values, often complicated by evolving environment and disagreements with what these norms are, especially with adults. Relational understandings associate privacy with forming relationships which need to be based on transparency, mutuality and trust, but some online relationships that young people have (with school boards, marketers, potential employers or law enforcement agencies) are one-dimensional, Steeves and Regan (2014) suggest.

In such a context, the idea of consenting to online privacy terms and conditions does not involve reciprocity; it forms a one-way relationship allowing the monitoring of the consent-giver who has no other option but to agree or be refused the benefit. These one-way relationships are purely instrumental, do not involve a process of negotiation, and jeopardise autonomy when the online environment allows the instrumental and commercial invasion of privacy. Finally, dialectical understanding of privacy points to the tension between the public and the private spheres which have collapsed online, which means that young people can seek both privacy and publicity online at the same time necessitating the constant negotiation of privacy and consent which cannot be given away irreversibly (Steeves and Regan, 2014).

So, while the dynamics of the online context can threaten and potentially violate privacy, children also experience its affordances as supporting their identity, expressive and relational needs by enhancing their choice and control over personal information and thus, their privacy online (Vickery, 2017). Online spaces, while technically public, can be experienced as offering greater 'privacy' because they are parent-free compared with, for example, what a child can say or do at home (boyd and Marwick, 2011). Hence, while children, like anyone else, are influenced by social as well as digital environments, their privacy perceptions and practices might be different from how adults (parents, educators, policy-makers) envision them or wish them to be. For example, a 13-year-old girl participating in the ethnographic study of London-based schoolchildren by Livingstone and Sefton-Green (2016) explained that she considered Facebook to be public and Twitter private, because her cohort's social norms dictated that they were all on Facebook, making any posting visible to everyone she knew (even though her profile was set to private), whereas few of her friends used Twitter so she could have a conversation there which was visible only to a select few.

Similarly, a study of Finish children aged 13 to 16 creating own online blogs expereinced them as intimate spaces affording welcome opportunities for making new connections, rather than spaces where information is shared publicly (Oolo and Siibak, 2013). A final example is the study of a youth online platofrm for anonymous sharing of experiences of online hurtful behaviour (MTV Over the Line) by Zizek (2017), who describes that communicating with strangers in this context carries trust and closeness – characteristics that are usually ascribed to children's relationships with family or friends. This shifts privacy from traditionally shared in non-public circles to being shared in a public space – creating a new way of dealing with what is seen as public and private (Zizek, 2017). This means that one cannot simply determine contextual norms from a formal knowledge of the digital environment but rather, empirical research including the views and experiences of children is vital.

5.2. Dimensions of children's online privacy

In this review, we follow Nissenbaum's definition of privacy as 'neither a right to secrecy nor a right to control, but a right to appropriate flow of personal information' (Nissenbaum, 2010: 3). This embeds the notion of privacy as relational and contextual (relationships being a specific, and crucial, part of any social context) in the emphasis on 'appropriate' (as judged by whom? Or negotiated how?) and 'flow' (from whom to whom or what?).That is, it does not assert the right to control as solely held by the individual but rather, construes it as a matter of negotiation by participants. But what kinds of relationships, in what kinds of context, and as part of what power imbalances are pertinent for children's privacy in the digital age?

A recent UNICEF report on children's privacy online and freedom of expression distinguishes several dimensions of privacy affected by digital technologies – physical, communication, informational and decisional privacy (UNICEF, 2018). Physical privacy is violated in situations where the use of tracking, monitoring or live broadcasting technologies can reveal a child's image, activities or location. Threats to communication privacy relate to access to posts, chats and messages by unintended recipients. Violation of information privacy can occur with the collection, storage and processing of children's personal data, especially if this occurs without their understanding or consent. Finally, disruptions of decisional privacy are associated with the restriction of access to useful information which can limit children's independent decision-making or development capacities (UNICEF, 2018). Consequently, the report pays particular attention to children's right to privacy and protection of personal data, the right to freedom of expression and access to information diversity, the right to freedom from reputational attacks, the right to protection attuned to their development and evolving capacities and the right to access remedies for violations and abuses of their rights – as specified in the UN Convention on the Rights of the Child (1989).

Such attempts to recognise children's right to privacy on its own terms are relatively new and have been brought to the fore by the recent more comprehensive focus on privacy (and its violations) in the light of the discussions prompted by the adoption of the GDPR across Europe. Until then, the privacy discourse tended to be developed mainly in relation to adults' privacy, undervaluing the privacy of children, and also tended to see children's privacy as managed by responsible adults (like family members) who had children's best interests at heart

(Shmueli and Blecher-Prigat, 2011).[6] For our systematic mapping of the current debate and emerging research regarding children's privacy online, its dimensions and relevant actors, we find the distinction between interpersonal, institutional and commercial privacy helpful. This means that, while we have the questions of rights firmly in mind (UNICEF, 2018), to grasp the import of the available empirical research we focus more pragmatically on the nature of the relationships and contexts in which children act in digital environments and on how they understand the implications for their privacy (i.e., to their 'appropriate flow of personal information'). Specifically, we distinguish three main types of relationship (or context) in which privacy is important: between an individual and (i) other individuals or groups ('interpersonal privacy'); (ii) a public or third sector (not-for-profit) organisation ('institutional privacy'); or (iii) a commercial (for-profit) organisation ('commercial privacy').

Interpersonal privacy

We found that the predominant amount of attention to children's privacy online relates to the interpersonal dimension, and most of the existing studies demonstrate that individual privacy decisions and practices are influenced by the social environment – how individuals handle sharing with or withholding information from others, how existing networks, communication and sharing practices influence individual decisions, and how desire for privacy is balanced with participation, self-expression and belonging. Issues related to peer pressure, offline privacy practices and concerns and parental influences also form important connections to the social dimension of privacy (Xu et al., 2008; Heirman et al., 2013). Children's online practices are shaped by their interpretation of the social situation, their attitudes to privacy and publicity and their ability to navigate the technological and social environment and development of strategies to achieve their privacy goals. These practices demonstrate privacy as a social norm, achieved through an array of social practices configured by social conditions (boyd and Marwick, 2011; Utz and Krämer, 2015).

For example, a qualitative study of UK children aged 13-16 and their use of social media found that teenagers form 'zones of privacy' using different channels for disclosure of personal information in a way that allows them to maintain intimacy with friends but sustain privacy from strangers and sometimes, parents (Livingstone, 2008). Their behaviour on social media demonstrated the shaping role of social expectations in the peer group and their own understanding of friendship and intimacy on privacy norms and behaviours. Privacy decisions are also influenced by factors such as the privacy settings of one's friends, the intensity of social media use, gender, types of contacts on one's social media profile, privacy concerns, wanting to be in control of one's personal information, prior negative experiences of sharing personal information or parental mediation (Youn, 2008; Abbas and Mesch, 2015).

Institutional privacy

In digital societies, the collection of children's data begins from the moment of their birth and often includes large amounts of information collected even before they reach the age of two (UNICEF, 2018). Institutionalised aspects of privacy where data control is delegated to external agencies, such as government institutions, is becoming the norm rather than the exception in the contemporary digital era (Young and Quan-Haase, 2013). Still, the discussion of institutional privacy in relation to children was much less prominent in the literature, and when discussed it was mostly seen as a legitimate effort to collect data, not raising the same critical concerns that we see in relation to either children's own privacy practices or commercial practices. The main attention was focused on the technical solutions related to institutional privacy, the improvement of safety features and techniques to restrict unauthorised access (Al Shehri, 2017), but not on what the purpose of this data gathering is, how it is shared with others and what the longer-term consequences might be.

Amongst the criticisms of institutional privacy are the contribution of governments and local authorities to the increase in personal data gathering and their ability to request individual data from industry, for example, in an attempt to predict

[6] Linked to questions of the child's right to privacy is a debate, inflected differently in different countries and cultures, regarding the parent's rights over their child, including the parent's right to manage (or invade) their child's privacy. Archard, D. (1990) Child Abuse: parental rights and the interests of the child. *Journal of Applied Philosophy* 7(2), 183-94, Shmueli, B. and Blecher-Prigat, A. (2011) Privacy for children. *Columbia Human Rights Law Review* 42, 759-95.

criminal or terrorist behaviour (Solove, 2015; DefendDigitalMe, 2018). There is also the potential of institutional administrative data, collected in circumstances in which one would expect confidentiality, to be shared across intra- and inter-governmental, public and commercial institutions, for purposes described as for 'public benefit', such as fraud prevention, health and welfare or education.

Still, existing studies show that individuals care about how their personal data is collected and processed by public section organisations and what this means for their privacy. For example, Bowyer et al. (2018) explore how families perceive the storage and handling of their data (personal data, relationships, school records and academic results, social support and benefits, employment, housing, criminal records, general practitioner and medical records, library usage) by state welfare and civic authorities, using game-based interviews. The study found that families often consider their data as 'personal' and want to be in control of it, especially in relation to information perceived to be 'sensitive'. This was often prompted by recognised risks (of a criminal, medical, welfare, social and psychological nature) and fear of the consequences of mishandling or misuse of the data (Bowyer et al., 2018). This study, however, did not focus on children; it considered them as part of the family. Similar findings are discussed by Culver and Grizzle (2017) who did a global survey with children and young people (aged 14-25, no distinction made by age groups) and found that 60% of the survey respondents disagreed that governments have the right to know all personal information about them and 50% agreed that the internet should be free from governments' and businesses' control. However, 38% thought that governments have the right to know this information if it would keep them safe online and 55% said that their security was more important than their privacy (Culver and Grizzle, 2017).

Other research looked at institutionalised privacy in relation to young adults (e.g., students and online learning and monitoring platforms), but there was little discussion of a parallel, institutionalised privacy for children (e.g., digital learning platforms, fingerprint access to school meals, profiling of attendance and academic performance). In fact, these new approaches to digital learning are often presented as 'revolutionary' and transformational to parents, even though they raise many questions in relation to the merging of for-profit platforms and business models with public education (Williamson, 2017).

The potential risks behind institutional privacy are demonstrated by a study of American schools exploring the use of third-party applications and software to monitor and track students' social media profiles and use during and after school (Shade and Singh, 2016; Bulger et al., 2017). The research demonstrated that, while the monitoring is justified by school governors as an attempt to tackle bullying, violence and threats by and directed at students, the business imperatives raise ethical concerns about young people's right to privacy under a regime of commercial data monitoring. Some of the examples included in the study comprised monitoring and analysing public social media posts made by students aged 13+ and reporting on a daily basis posts flagged as a cause for concern to school administrators. The reports included screenshots of flagged posts, whether they were posted on/off campus, time and date and user's name and highlighted posts reflective of harmful behaviour to students, as well as actions that are harmful to schools themselves – shifting from an interest in the safety of youth to the protection of the school. It was unclear if the businesses cross-reference their data with other records or information available, creating an assemblage of surveillance (Shade and Singh, 2016). While this demonstrates the potential risks, more research is needed to fill in the gaps related to how children and teenagers experience institutional privacy, so as to draw further attention to the management of informed consent and children's rights in settings such as schools and health services (Lievens et al., 2018).

Commercial privacy

The means for processing children's data are advancing and multiplying rapidly, with commercial companies gathering more data on children than even governments do or can collect (UNICEF, 2018), pushing commercial data collection to the top of the privacy concerns. Marketers employ many, often invasive, methods to turn children's activities into a commodity (Montgomery et al., 2017), monitoring of online use and profiling via cookie-placing, location-based advertising and behavioural targeting. They also encourage young consumers to disclose more personal information than necessary

in exchange for enhanced online communication experiences (Bailey, 2015; Shin and Kang, 2016), or as a trade-off for participation and access to the digital services and products provided (Micheti et al., 2010; Lapenta and Jørgensen, 2015). The invasive tactics used by marketers to collect personal information from children aiming to reach and appeal to them as a designated target audience have led to rising data privacy and security concerns (Lupton and Williamson, 2017). These particularly relate to children's ability to understand and consent to such data collection and the need for parental approval and supervision, particularly in relation to children under the age of 13 (or higher in some countries in Europe)[7] (Livingstone, 2018).

While the commercial use of children's data is at the forefront of current privacy debates, the empirical evidence lags behind, with very few studies examining children's awareness of commercial data gathering and its implications. The majority of research on young people in this area is based on young adults (18+) or older teenagers (16+), and demonstrates that even these more mature online users have substantial gaps in their privacy knowledge and awareness. Some of the barriers that have been identified by the existing research on children's understanding of commercial privacy relate to the incomprehensibility of how their online data is being collected and used (Emanuel and Fraser, 2014; Acker and Bowler, 2018), how it flows and transforms – being stored, shared and profiled (Bowler et al., 2017), and to what effect and future consequence (Murumaa-Mengel, 2015; Bowler et al., 2017; Pangrazio and Selwyn, 2018). While the research demonstrates that some commercial privacy concerns exist (related to being tracked online, that all the data is stored permanently, the inability to delete one's data), children generally display some confusion of what personal data means and a general inability to see why their data might be valuable to anyone (Lapenta and Jørgensen, 2015).

The existing evidence also suggests that children may also provide personal data passively and unconsciously when using online services like social media, provoked by the platform design and configuration (De Souza and Dick, 2009; Madden et al., 2013; Pangrazio and Selwyn, 2018; Selwyn and Pangrazio, 2018). Generally, children are more concerned about not being monitored by parents (Shin et al., 2012; Third et al., 2017) or about breach of privacy by friends and by unknown actors (such as hackers, identity thieves and paedophiles), and less so about the re-appropriation of their data by commercial entities.

Children also struggle with privacy statements due to their length and complicated legal language or the inefficient management of parental consent by children's websites (Children's Commissioner for England, 2017b) which either overlook, detour or avoid parental consent. Some children may feel obliged to agree with the Terms and Conditions and they see targeted advertising as a default part of contemporary life (Lapenta and Jørgensen, 2015). The evidence also suggests that children do not feel that they can change their behaviour much, feel unable to invest the time needed to constantly check the privacy settings, and are not sure how to avoid data profiling (Lapenta and Jørgensen, 2015; Pangrazio and Selwyn, 2018). As a result, they experience a contradiction between their desire to participate and the wish to protect their privacy, in a way that might cause a sense of powerlessness (Lapenta and Jørgensen, 2015; Pangrazio and Selwyn, 2018; Selwyn and Pangrazio, 2018).

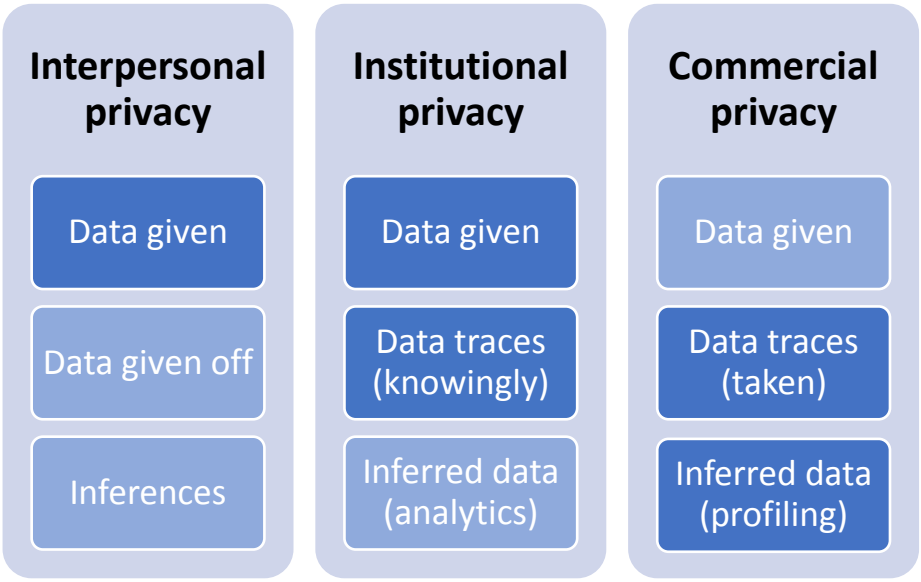
There is some evidence that commercial privacy is related to different behaviours than interpersonal privacy resulting from the different type of follow-up engagement: while individuals examine the reaction of friends towards their posts on social media, they do not often deliberately communicate with commercial entities, so the consequences of their data being used may remain unknown to them, making them less concerned about commercial than interpersonal privacy (Lapenta and Jørgensen, 2015). Better knowledge of commercial privacy, however, can be associated with a greater desire to have control over the display of advertising content. A study of 363 adolescents aged 16-18 from six different schools in Belgium showed that as their level of privacy concern increased, so did their sceptical attitudes towards advertisement targeting, resulting in lower purchasing intention: 'This demonstrates that adolescents adopt an advertising coping response as a privacy-protecting strategy when they are more worried about the way advertisers handle their online personal information for commercial purposes' (Zarouali et al., 2017: 162). This demonstrates the importance of exploring commercial privacy in relation to children,

[7] Parental consent is required for underage children only when data is processed on the basis of consent.

particularly with a developmental (Fielder et al., 2007) and educational/media literacy focus as so far we lack sufficient up-to-date research.

Types of digital data

Figure 2: Dimensions of privacy and types of data



With digital media now being embedded, embodied and everyday (Hine, 2015), the contemporary digital world has become 'data-intensive, hyper-connected and commercial' as an increasing amount of data is being collected about online users, including children (van der Hof, 2016: 412; Winterberry Group, 2018). To capture this comprehensive collection of data and to think about what children know and expect in relation to different types of data, we adapted a typology from privacy lawyer Simone van der Hof (2016) to distinguish:

- **Data given** – the data contributed by individuals (about themselves or about others), usually knowingly though not necessarily intentionally, during their participation online.
- **Data traces** – the data left, mostly unknowingly– by participation online and captured via data-tracking technologies such as cookies, web beacons or device/browser fingerprinting, location data and other metadata.
- **Inferred data** – the data derived from analysing data given and data traces, often by algorithms (also referred to as 'profiling'), possibly combined with other data sources.

Each of these types of data may or may not be 'personal data', that is, 'information that relates to an identified or identifiable individual', as defined by the ICO and GDPR.[8]

The different dimensions of privacy incorporate different types of data (see Figure 2) and therefore, represent different degrees of 'invasiveness' (indicated by the intensity of the colour of the boxes), especially having in mind that only one type of data is actively contributed by individuals – the 'data given'

When considering privacy online, do children think mostly about their individual privacy and the data they or others (friends or family) share about them online? How knowledgeable are they about the data traces they leave and about how these can be used to profile them (inferred data) for commercial purposes?

[8] For more on 'personal data' see *What is personal data?* (https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/).

5.3. Privacy and child development

Research shows that children of different ages have different understanding and needs. The truth of this claim does not mean it is easy to produce age groupings supported by evidence, nor that children fall neatly into groupings according to age; they do not. Any age group includes children with very different needs and understandings. Even for a single child, there is no magic age at which a new level of understanding is reached. The academic community has, by and large, moved beyond those early developmental psychology theories which proposed strict 'ages and stages'. But nor does it consider children to be equivalent from the age of 5 and 15, for instance. Rather, developmental psychology, like clinical psychology and, indeed, the UN Convention on the Rights of the Child, urges that children are treated as individuals, taking into account their specific needs, understandings and circumstances.

While children develop their privacy-related awareness and literacy as they grow older, their development is multifaceted and complex; it does not fall neatly into simple stages or change suddenly once they pass their birthday. In addition, children's development can be very different based on their personal circumstances. For example, a 15-year-old from a low socio-economic status (SES) home (DE) might have similar knowledge and digital literacy as a 11-year-old from a high SES home (AB), as we show here (Livingstone et al., 2018a). Hence, we urge that consideration of age groups and age transitions considers cognitive, emotional and social/cultural factors. For instance, in the UK, around the age of 11, most children move from smallish, local primary schools to large, more distant secondary schools. Many risky practices – online and offline – occur at this transition point, because children are under pressure quickly to fit into a new and uncertain social context. They are likely, then, for social and institutional (rather than cognitive) reasons, to access many new apps and services, to feel pressured to circumvent age restrictions, to provide personal information not provided before, and so forth. To give another instance, children who suffer risks or hardships or disabilities in their day-to-day world are likely to experience different pressures to join in online, again meaning that consideration of their age alone would fail to fulfil their best interests.

However, child development theory and some existing evidence points to the diverse understandings and skills that children acquire, test and master at different ages and its subsequent influence on their online interactions and negotiations. The evidence suggests that design standards and regulatory frameworks must account for children's overall privacy needs across age groups, and pay particular attention and consideration to the knowledge, abilities, skills and vulnerabilities of younger users. Chaudron et al.'s (2018) study of young children (aged 0-8) across 21 countries found that most children under 2 in developed countries have a digital footprint through their parents' online activities. Children's first contact with digital technologies and screens was at a very early age (below the age of 2) often through parents' devices, and they learn to interact with digital devices by observing adults and older children, learning through trial and error and developing their skills. They did not have a clear understanding of privacy or know how to protect it. The Global Kids Online study observed clear age trends in four countries, where older children were more confident in their digital skills than their younger counterparts. Young children (aged 9-11) in particular showed less competence in managing their online privacy settings than teens (aged 12-17) (Byrne et al., 2016).

Privacy is vital for child development – key privacy-related media literacy skills are closely associated with a range of child developmental areas – autonomy, identity, intimacy, responsibility, trust, pro-social behaviour, resilience, critical thinking and sexual exploration (Peter and Valkenburg, 2011; Raynes-Goldie and Allen, 2014; Pradeep and Sriram, 2016; Balleys and Coll, 2017). Online platforms provide opportunities for development (while also introducing and amplifying risks) that children can use to build the skill entourage that they need for their growth (Livingstone, 2008). There is also solid evidence that understanding of privacy becomes more complex with age and that the desire for privacy also increases (Shin et al., 2012; Kumar et al., 2017; Chaudron et al., 2018).

Despite the relationship between child development and privacy functioning and competencies, the evidence on this is patchy. How do children understand and manage privacy based on their age and development? What is the most suitable age to start learning about privacy online, and how should

this learning expand as children grow up and develop? These are important questions, which the systematic evidence mapping could not answer sufficiently. Due to the nature of the existing research, it is difficult to provide robust evidence to support strictly identified age brackets and to cover the full age spectrum under 18 years. A large number of studies focus on 12- to 18-year-olds, paying much less attention to younger cohorts and studies rarely disaggregate findings amongst the different age groups (Livingstone et al., 2018b). Further difficulties arise from the fact that current evidence on children's privacy concerns, risks and opportunities utilises a range of age brackets and applies them inconsistently.

Attempting to overcome the above difficulties and boiling the research down to its essence, we mapped the development of children's understanding of privacy by age, with the caveat that the differences within as well as across age groups can be substantial. We identified three groups of evidence (see Table 2 below): children aged 5-7, 8-11 and 12-17. Hence, we think that there is little evidence to support the more nuanced differences in the age groups at present.

Table 2: Child development and types of privacy

	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 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 internalised behaviour • Still see monitoring positively, as ensuring 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, socialising, 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 focused 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 best if teens can use new knowledge to make meaningful decisions

5- to 7-year olds

Starting with the youngest group we identified – **the 5- to 7-year-old children** – we found that there is limited evidence on their understanding of privacy, but the existing studies suggest that children of this age are already starting to use services which collect and share data - for example, 3% of the UK children aged 5-7 have a social media profile and 71% use YouTube (Ofcom, 2017b). Children of this age gradually develop a sense of ownership and independence, as well as the ability to grasp 'secrecy' that is necessary for information management abilities and privacy (Kumar et al., 2017). While children are confident internet users, they engage in a narrow range of activities and have low risk awareness (Bakó, 2016). They do not demonstrate an understanding that sharing information online can create privacy concerns (Kumar et al., 2017), and their perception of risks arising from technology use is associated mainly with physical threats (e.g., mechanical damage to the device) which are easier to comprehend, while abstract notions such as 'privacy' and 'safety' are hard to grasp (Chaudron et al., 2018). For example, when playing with internet-connected toys, the children do not necessarily realise that these devices record and share their data (McReynolds et al., 2017).

At this young age children have little clear understanding of how to engage in online privacy protection (Chaudron et al., 2018), and rely on adults to advise them and create rules. Their strategies at this age include mainly closing the app or website, providing fake information and asking trusted adults for help (Kumar et al., 2017). Children of this age can identify some information as sensitive – and might want to hide it from parents to avoid getting into trouble (Kumar et al., 2017) – but they often do not see monitoring of their activities or tracking their devices as a cause for concern or breach of privacy (Gelman et al., 2018).

8- to 11-year olds

While over one in five UK **children aged 8-11** (21%) have a social media profile (Ofcom, 2017b), even though they are officially below the required age to use these platforms, children at this age still struggle to identify risks or distinguish what applies offline/online. They have gaps in their ability to decide about trustworthiness of the sources and content or identify commercial content (e.g., adverts) (Ofcom, 2017b). Children start to understand that sharing can create some risks for them (Kumar et al., 2017), but associate privacy hazards mainly with 'stranger danger' (Weeden et al., 2013; Raynes-Goldie and Allen, 2014; Children's Commissioner for England, 2017b). Children aged 8-11 approach privacy management based on rules and not internalised behaviour, hence they find it hard to apply their knowledge to practical situations (Kumar et al., 2017) and they still have gaps in understanding privacy terms and conditions which are unclear and inaccessible to them.

Children's sharing of personal data at this stage is guided by parental advice (Livingstone, 2008), and those whose parents are actively mediating their internet use are sharing less personal information online (Miyazaki et al., 2009). Children of this age also see monitoring more positively than adults (e.g., that it might be for the benefit of their own safety), but they also start to develop a desire for independence (Livingstone, 2008) and might come up strategies to bypass parental monitoring, supervision or surveillance when it is undesirable (Barron, 2014). The effects of warning signs on websites notifying children of age-inappropriate content can have the opposite effect – children are more likely to share their data than on sites where there is no warning as they become curious (Miyazaki et al., 2009). The research also demonstrated that there are some effective examples of interactive learning approaches used with children of this age which are shown to improve awareness and transfer to practice (Zhang-Kennedy et al., 2017).

12- to 17-year olds

For the oldest group of children – **children between 12 and 17 years of age** – we found they are by now aware of privacy risks: they engage in careful consideration of information disclosure (Wisniewski et al., 2015) and balance their desire to protect themselves with the need to participate and socialise (Oolo and Siibak, 2013; Betts and Spenser, 2016; Dennen et al., 2017; Third et al., 2017). They also weigh risks and opportunities but their decisions are often influenced by the immediacy of and desire for benefits, more than distant and uncertain risks in the future (Youn, 2009; Yu et al., 2015). Yet their decisions are based on their still

partial understanding of the nature and operation of the internet and its uses of personal data.

The older children become, the more actively they use the internet, and the more technical skills they acquire (Madden et al., 2013). For example, 46% of UK children aged 12-15 know how to delete the history records of the websites they have visited (27% have done it), 36% know how to use a browser in incognito mode (20% have used it), 18% know how to unset filters preventing them from visiting websites (and 6% have done it), and 7% know how to use a proxy server (3% have used one) (Ofcom, 2017b). These technical skills, however, are not necessarily paired with good knowledge of privacy risks or with effective privacy protection strategies. With greater internet use comes higher exposure to online risks, including those related to privacy – older teens share more personal information, to more people, and across a larger number of platforms (Madden et al., 2013; Xie and Kang, 2015).

Children of this age (12-17) have a good understanding of online restrictions and monitoring by the school (Cortesi et al., 2014; Acker and Bowler, 2018) – for example, they know their online activities are monitored when using a school computer and the content they can access is restricted. Children also demonstrate some awareness of the 'data traces' they leave online (e.g., in relation to seeing advertisements following their earlier searches) (Zarouali et al., 2017) and of device tracking (e.g., that some apps use their geo-location) (Redden and Way, 2017), but find it hard to make a personal connection – how their data is being collected and to what effect (Emanuel and Fraser, 2014; Acker and Bowler, 2018). Yet even at this age, children have little knowledge of data flows and infrastructure – they mostly see data as static and fractured (e.g., located on different platforms) (Bowler et al., 2017), which can create a false sense of security. They have little awareness of future implications of data traces, particularly related to distant future, which is hard to predict or conceive (Murumaa-Mengel, 2015; Bowler et al., 2017; Pangrazio and Selwyn, 2018).

The online environment at this stage is seen as a 'personal space' for self-expression and socialising, and children are often concerned about parental intrusion of their privacy (boyd and Marwick, 2011; Redden and Way, 2017; Martin et al., 2018). The sense of control over one's personal information, which such online identity management provides, can actually increase the extent of children's self-disclosure (Peter and Valkenburg, 2011), making children more likely to share personal information (Emanuel and Fraser, 2014). At this age, privacy risk functions mostly as a 'learning process' – children are mostly engaged in retrospective behaviour, trying to rectify the past, and hold expectations that they are able to retract their online activities (Wisniewski et al., 2015; Wisniewski, 2018).

A major gap in children's understanding of privacy is that they associate it mainly with interpersonal sharing of data and rarely consider the commercial or institutional use of their data (Davis and James, 2013; Steijn and Vedder, 2015; Livingstone et al., 2018b). Hence, their privacy strategies are mainly limited to management of their online identity – for example, withholding or providing fake information, or creating multiple identities, removing content, tags or withdrawing from the internet, managing privacy settings or friendship circles (Livingstone, 2008; Almansa et al., 2013; Emanuel and Fraser, 2014; Weinstein, 2014; Mullen and Hamilton, 2016). At the same time, children can be quite trusting of online platforms, choosing to accept the default privacy settings based on the belief that the site designers and developers have already considered privacy issues, and built adequate privacy protections into the site's architecture (Davis and James, 2013) – thus undermining their own initiative in relation to privacy.

Children struggle with some aspects of privacy – while they know rather well what type of personal information they have disclosed online, they are less certain who has access to this information, and often struggle to name the privacy setting of their disclosed contents (Moll et al., 2014). Children are both overestimating and underestimating how private their profile content is, sugesting an overall confusion rather than a tedency to underrate the privacy risks. They tend to overestimate the privacy of information such as favourite music and their school, but underestimate the privacy of their email address or birthday (Moll et al., 2014). While this evidence is insufficient to answer all the questions about child development, it undoubtedly points to the need for a tailored approach that acknowledges developments and individual differences amongst children. It also demonstrates that data and evidence pertaining to design standards and regulatory frameworks based on disaggregated age groups are low and merit further investigation.

5.4. Children's negotiation of privacy and information disclosure

There is a widespread consensus in the literature that children are seen as showing less concern about privacy online and their conceptions of 'privacy' and 'the private' differ from that of adults (Steijn et al., 2016). Based on such comparisons, children are criticised for sharing too much personal information online, lacking maturity in their decisions and missing the capacity to judge about the repercussions their actions. Yet the evidence demonstrates that children are not oblivious to the privacy consequences of their online behaviour. They are constantly negotiating between the risks and opportunities of communicating in networked publics (Livingstone, 2008), and are attuned to the tensions between their desire to engage, to protect themselves and their responsibility to others (Lapenta and Jørgensen, 2015; Third et al., 2017).

Children use extensively digital media for self-disclosure and, while aware of the privacy risks, they weigh these against the opportunities involved (such as online self-expression and identity, creating intimacy via confiding in others, and establishing new relationships) (Aslanidou and Menexes, 2008; De Souza and Dick, 2009; Lapenta and Jørgensen, 2015; Livingstone and Sefton-Green, 2016; Balleys and Coll, 2017). In certain cases personal data can become an asset to children and their means of part-taking and participation. Garbett et al. (2018: 9) demonstrate this in their study of a wellbeing system aiming to encourage primary schoolchildren to reflect on their own personal activity data. Using an avatar, children could compare their results to others and contribute to the success of their fitness and wellbeing teams. They could also 'socially negotiate access to their identity' (Garbett et al., 2018: 9) by revealing their identity to selected others based on friendships and judgements of trust.

Young people's understanding of privacy is less focused on personal information than adults' and they are less concerned about risks related to data mining, profiling or identity theft because dealing with bankers, future employers and authorities seems distant and less relevant (Steijn and Vedder, 2015; Steijn et al., 2016). Therefore, it is not surprising that they report less concern about privacy and are more active on social media, which provides both personal and social benefits. While children might enjoy self-exposure to known and unknown audiences on a range of social platforms, they also hold a complex set of norms associated with who should access their information and how they should react to it and feel discomfort when these norms are not being followed (Steeves and Regan, 2014).

Some children also experience a tension between the desire to withhold information and peer pressure to share and be popular online (have more 'likes' or followers), and their online choices (tailoring messages to audiences, choosing different platforms based on audiences or purposes) are influenced by their privacy concerns (Livingstone, 2008; De Souza and Dick, 2009; Betts and Spenser, 2016; Hofstra et al., 2016). In such cases, decisions about self-disclosure seem to be influenced by the immediacy and greater certainty of benefits over the more distant and potential nature of risks (Yu et al., 2015; Betts and Spenser, 2016). Children also see privacy as embedded in the context – of who is present and what is then socially appropriate given their presence and the context (boyd and Marwick, 2011). The desire for privacy, however, is not about 'hiding' but rather about asserting control (boyd and Marwick, 2011), which children try to do via managing their online representation – for example, by meticulously staging profile pictures (Almansa et al., 2013) or negotiating content posted by others, such as friends or family members (Lapenta and Jørgensen, 2015).

Children, however, are often confronted by their lack of complete control over what others share about them – sites allowing tagging or @-ing in responses, for example, exacerbate the public-by-default nature of networked publics and force children to consider what they wish to obscure or remove retrospectively (boyd and Marwick, 2011; Betts and Spenser, 2016; Pangrazio and Selwyn, 2018). As a result, children might demonstrate a 'pragmatic non-concern' about things they cannot control – such as what friends might post or how commercial entities might use their data, exhibiting an 'intellectual detachment', having a vague awareness that they are affected by data profiling but remaining intellectually disengaged from this process due to the overwhelming and uncontrollable misuse of their data (Pangrazio and Selwyn, 2018). Children's control over their representation online is also challenged by the tension between parents' practices (e.g., 'sharenting') and children's privacy.

For example, an online survey with 331 parent–child pairs (children aged 10-17) in the USA demonstrated that parents and children disagree on the permission-seeking process when it comes to posting information online (Moser et al., 2017). Children believe that parents need to ask permission more than their parents think they should, and also objected to the sharing of content reflecting negatively on the child's self-preservation, content perceived as 'embarrassing', unflattering or overtly revealing (Moser et al., 2017). While the research demonstrates that parents do consider their children's privacy when posting information about them online (Blackwell et al., 2016), the issue of privacy decision-making remains problematic. Parents shape children's digital identity through sharenting, and these disclosures can sometimes follow them into adulthood (Moser et al., 2017). This information sharing, sometimes without children's consent, makes them narrators of their children's lives and stories and gatekeepers of their children's personal information. This can give rise to a potential conflict of interest in the future, as children's digital identities evolve and they come to resent their parents' disclosures. While a lot of research focuses on how children make decisions about sharing content online and how they negotiate this with others, much less attention is paid to the commercial dimensions of such 'volunteered' content, and more information is needed on the extent to which children feel competent and able to negotiate institutional and commercial privacy, or, in fact, if they would like to.

5.5. Children's privacy protection strategies

Internet privacy has attracted attention due to the large-scale collection of personal information, making it easy to copy, tag, search, replicate or decontextualise. There seems to be a contradiction between willingly volunteering personal information online and the expressed concern for privacy online – identified as the privacy paradox (Barnes, 2006; Norberg et al., 2007). However, the existing evidence demonstrates that children deploy a range of privacy protection strategies – from selective use of platforms based on the privacy they provide, to withholding or providing fake information, to removing content, tags or withdrawing from the internet, to managing privacy settings or friendship circles (Almansa et al., 2013; Feng and Xie, 2014). This implies that children value their privacy and engage in protective strategies but the disclosure forms part of a trade-off that teens engage in – so as research shows, they weigh up what they might lose or gain or what the risk and reward may be.

Children might engage in withholding strategies (reflecting and deciding not to share content considered to be inappropriate), proactive strategies (actively selecting channels, settings, altering content) or might not have any strategies, for example, when they are not aware of different privacy options or risks (Davis and James, 2013). When using proactive strategies, children select amongst the multiple communication channels afforded to them, opting for private dyad communication channels (like text messaging or private messenger) to discuss more intimate and personal matters, while reaching out to social media platforms to reconnect with older friends or access information that may be otherwise hard to come by (Heirman et al., 2016; Mullen and Hamilton, 2016; Dennen et al., 2017). Other strategies involve content modification (such as changing textual descriptions, removing tags or altering images); management of audiences and boundaries, for example, by segmenting friend groups within services and between them or removing and blocking people (Madden et al., 2013; Mullen and Hamilton, 2016); or using social steganography (as a form of privacy management this involves children [de]coding messages for their intended audience or using language and specific references for their intended audiences) (boyd and Marwick, 2011).

A major point of interest in relation to privacy protection management is the role of privacy concerns on children's strategies. If children are concerned about their privacy, are they more careful with their sharing practices? If they are concerned about privacy, does it mean that they are more aware of the potential risks and better able to mitigate them? Are children's privacy concerns a reliable predictor of actual privacy protective behaviours, and if so, of what types of behaviour? It seems intuitive to expect that better awareness of privacy risks and higher concerns would produce more effective privacy protection strategies, and a substantial body of work has sought to explore this connection. The evidence, however, has demonstrated a very mixed picture and the impact of privacy concerns on privacy protective behaviours is varied.

Some of the research demonstrates the paradox of people sharing information even though they have

disclosure worries with privacy concerns not being associated with information-disclosing behaviour (Shin and Kang, 2016). For example, warning safeguards notifying children of unsuitable content or minimum age requirements can have the opposite effect – they can increase personal information disclosure as they seem to create curiosity rather than awareness or concern (Miyazaki et al., 2009). Other existing studies demonstrate some connection between a higher level of privacy concern and strategies to handle privacy risks, such as higher likelihood of changing privacy settings, reading privacy messages, providing less personal information, reporting unsolicited emails or responding negatively to them, or expecting negative consequences from information disclosure (Moscardelli and Divine, 2007; Youn, 2008; Chai et al., 2009; Madden et al., 2013; Chi et al., 2018).

Children might become more concerned about their privacy following the misuse of their data, realising the accessibility to sensitive information, or deciding that risks outweigh the benefits. The differences in the findings might be related to the ways privacy concerns and privacy protective behaviours are measured, or to considering additional factors, such as internet use, digital skills, trust or socio-cultural norms. For example, factors such as the sense of control over one's personal information and who can access it can influence what and how much children disclose online (Davis and James, 2013). The expected attitudes of parents and friends also influence children's intention to share personal information (van Gool et al., 2015) – if children expect that their parents and friends would disapprove, they tend to share less.

Hence, a related question arises – whether trust has any effect on sharing information online – and the evidence is again mixed. While trust appears to be an important influencer of self-disclosure, including sensitive information, because it minimises the perceived risk (Xie and Kang, 2015), it does not explain fully children's privacy protection strategies. Some studies suggest that trust in their social networks makes children more likely to disclose personal information and less likely to engage in protective behaviours (Steeves and Webster, 2008; S-O'Brien et al., 2011; Abbas and Mesch, 2015). A study using a nationally representative survey with 800 USA teenagers aged 12 to 17 also found that trust was associated with disclosure of contact information (such as phone number and email address). However, trust did not predict disclosure of insensitive information (school name, relationship status and personal interests) and personal identification information (photo and real name) (Xie and Kang, 2015). Interestingly, the same study did not find any relationship between regret of posting personal information and privacy settings or self-disclosure, but discovered that children who were more frequent users had larger network sizes, and were in contact with people they did not know, and were more likely to regret posting information online. Still, the rationale behind children's privacy behaviours is still unclear and the findings are mixed.

While there was substantial evidence to show that children care about their privacy and engage in a range of protective behaviours, many questions remain unanswered when it comes to how children choose their protective behaviour, which privacy-protection strategies are more efficient, and why some children are more protective of their privacy than others. Yet, the evidence demonstrates important gaps in children's practices – their privacy protection strategies are more focused on the interpersonal than the commercial domain, suggesting important gaps in their understanding of privacy risks and abilities to handle the commercialisation of their personal data. It is also likely that some explanation of the mixed evidence on children's protection strategies might be offered by looking at media literacy and whether children have the necessary digital skills to protect their online privacy.

5.6. Media literacy

Children's media literacy plays an important part in how children understand, manage and safeguard their privacy, prompting substantial research attention into this area. Privacy skills cannot be researched or taught in isolation from general media literacy and even digital citizenship – to manage privacy online one needs to understand the internet itself (Culver and Grizzle, 2017).

As David Buckingham (2015) argues, 'the increasing convergence of contemporary media means that we need to be addressing the skills and competencies – the multiple literacies – that are required by the whole range of contemporary forms of communication.' He identifies four areas of online media literacy competence: representation,

language, production and audience. 'Production' involves knowing the parties involved in online interactions and the reasons for communicating, including awareness of commercial influences which are often invisible to children.

Hence, media literacy involves an understanding of how media and information are created, analysed, distributed, applied, used and monestised (Oolo and Siibak, 2013; Culver and Grizzle, 2017). For example, the recent draft statutory guidance on teaching Relationships Education, Relationships and Sex Education (RSE) and Health Education by the Department for Education includes several references to online data and privacy as part of knowledge about relationships, online media, internet safety and harm. The guidance suggests that education should teach children how information is shared and used online both in interpersonal relationships and commercial contexts:

> Pupils should have a strong understanding of how data is generated, collected, shared and used online, for example, how personal data is captured on social media or understanding the way that businesses may exploit the data available to them. (Department for Education, 2018: 21)

The guidance also suggests that the concept of personal privacy and permission-seeking should be taught from the beginning of primary school.

Livingstone (2014) similarly suggests that (social) media literacy needs to encompass competences across several areas: affordances (including privacy-related), the communication (creating and decoding it), and the social interactions (e.g., relationships, privacy, anonymity). The development of this (social) media literacy is related to children's cognitive and social development and privacy competences play an important part in it (Livingstone, 2014). Media literacy also needs to include children's understanding of their data worlds, digital traces and data flows, as well as the analytical skills needed for personal data management involved in the curating and obfuscating digital data lives (Walrave and Heirman, 2013; Acker and Bowler, 2017; Bowler et al., 2017), as well as the ability to demand one's right to privacy (Culver and Grizzle, 2017).

The evidence on children's privacy-related media literacy includes evaluation of withholding and proactive strategies children use (Davis and James, 2013), as well as their knowledge and competence in this area. For example, a UK-based representative study of internet users aged 12 to 15 demonstrated that a third (34%) knew how to delete their browsing history, one in four (24%) knew how to amend settings to use a web browser in privacy mode, one in ten (10%) knew how to disable online filters or controls and 6% knew how to use a proxy server to access particular sites or apps. The proportion of children who said that they had done these things in the past year was much smaller (ranging from 11% who had deleted their search history to only 1% who had unset any filters or controls or used a proxy server) (Ofcom, 2017a). The privacy skills of children seem also to be improving over time – a longitudinal European study of children aged 9-16 found that there was an increase in the proportion of children who know how to change their privacy settings (43% of 11- to 13-year-olds in 2010 and 55% in 2014) and those who know how to delete their browsing history (37% in 2010 and 53% in 2014) (Livingstone et al., 2014).

However, while many children know how to change their privacy settings, many choose not to. There was an increase in the number of children who have a public social media profile between 2010 and 2014: from 11% to 19% in the UK compared to the European average of 25% in 2010 and 29% in 2014 (Livingstone et al., 2014). This demonstrates that being able to do something does not necessarily translate into a privacy protective behaviour ((Ofcom, 2017b; Ogur et al., 2017). The same study also found that around one-quarter of 11- to 16-year-olds in Europe talk about private things online, with over a third saying they talk about different things online compared to face-to-face interactions, and that they find it easier to be themselves online (Livingstone et al., 2014). Still, the proportion of children who discuss private issues online decreased over the period of four years. Children in the UK and Ireland were overall better off that their peers in other European countries (Belgium, Denmark, Italy, Romania and Portugal) – they start using social media later and when they do, they have fewer online contacts and are more likely to have a private profile. Still the study found that many children lack sufficient media literacy skills and their overall awareness of privacy risks might need improvement. In addition, technical architectures can additionally complicate privacy protection with shifting setting defaults and inconsistent levels between different

platforms, making it difficult to maintain a consistent privacy level (Oolo and Siibak, 2013; Bailey, 2015).

While the evidence related to commercial privacy is scarce, it demonstrates that this is an area of media literacy which children find particularly challenging (Bowler et al., 2017; Coleman et al., 2017; Acker and Bowler, 2018). In a qualitative USA-based study of young people aged 11-18, Bowler et al. (2017) found that teens have varying interpretations of the nature of data and a broad understanding of the lifecycle of data. However, most respondents found it difficult to connect with data at a concrete and personal level, with the notion of a personal data dossier either non-existent or proving too abstract a concept. Some were able to connect data to 'digital traces' but seemed to imagine data as static, held in a single place and had little knowledge of data flows and infrastructure. While aware of the security issues related to social media, they have spent little time thinking more broadly about the digital traces of their data and implications for their future selves (Bowler et al., 2017).

There is evidence that children's understanding of commercial privacy increases with age – for example, a New Zealand study of children and young people aged 8 to 21 found that the younger groups had much less understanding of different privacy-related security issues, such as allowing apps to access camera, contacts and personal information (name, address, mobile number) – only 2% of the 8- to 12-year-olds reported awarenss compared to 18% of the 13- to 17-year-olds and 24% of the over-18s. Similarly, small proportions knew that installed apps can access information not required for its operation and may use this information for other purposes such as online advertisements, but this improved with age: 1% of 8- to 12-year-olds, 15% of 13- to 17-year-olds and 26% of 18- to 21-year-olds (Tirumala et al., 2016).

Children are seen as particularly susceptible to digital advertising, and even though young internet users are faced with large quantities of online advertising, the evidence related to their influence on children is scarce. Some of the key issues related to children's exposure to online advertising arise from their inability to distinguish between website content and advertisements, difficulty in understanding the relationship between website content provider and the advertiser, and issues related to collecting children's data (van Reijmersdal et al., 2017). For example, a study of Dutch children aged 9-13 found that they process advertising in a non-critical manner, and seeing adverts which were close to their interests and hobbies was effective in creating a positive attitude towards the brand and consequently increases intentions to buy the products (van Reijmersdal et al., 2017). This is also demonstrated by a recent Ofcom (2017b) study of the media practices and competences of children aged 3 to 11, which discovered that children find it difficult to identify online advertisements that have evolved into a complex advertising and marketing environment. Children reported knowledge of personalised online advertising and brand ambassador advertising (e.g., via vloggers), but were not always able to identify this in practice, especially when it is designed to work similarly to other social media content. The study also found that children understand advertising revenue through sponsored ads, but many are unable to identify it accurately (even when the word 'ad' appears), and believe Google as an authenticating and trustworthy source (Ofcom, 2017b).

Teaching children about privacy can also prove challenging, as a participatory experimental study of Australian children aged 13 to 17 demonstrated (Selwyn and Pangrazio, 2018). The study found that while children are active on social media and consider themselves relatively safe, many are uncertain about what information others can see about them and are concerned about the permanence of their online posts. After using a specific app designed to demonstrate the gathering of personal data, the children became more aware of geolocation data (perceived as creepy, unsettling and invasive). They also found the data analysis inaccurate (assuming different interests, nationality, visited places), which the children found reassuring – as a sign that the internet does not know everything about them. As part of the experiment the children were able to adopt different response tactics – check the Terms and Conditions, research and report back on the commercial background of social media platforms, run ad-blocking, tracking and geo-spoofing software, or alter their selfies in a way that aims to confuse facial recognition and photo analysis. The first two activities enabled them to become more aware of data use and sharing, the business model and ownership of the services, while the latter two were seen as uninteresting or ineffective. The authors describe the experiment as relatively ineffective in provoking the participants to change their personal data practices due to the

perceived lack of effectiveness of any alternative actions combined with lack of time and expertise (Selwyn and Pangrazio, 2018). The children also did not object to being targeted by advertising which was perceived as an acceptable element of mobile media use. While children were generally interested and concerned about online privacy, they also felt overwhelmed and annoyed but did not feel empowered to make changes, and nor did they feel in control of their privacy, leading the authors to argue in favour of changes to the business model which would not only make personal data use more transparent, but would also enable children to engage more actively and agenticly with the online platforms raising their critical awareness (Selwyn and Pangrazio, 2018).

While there is concern about children's online privacy, more evidence is needed in order to identify the effective media literacy education approaches. Some of the existing evidence suggests that privacy-related education can increase children's awareness of technological solutions or tighter privacy settings as coping and threat-mitigating strategies (Chai et al., 2009; Youn, 2009). Still, most initiatives (government legislation, educational programmes or parental control applications) are based on adult perspectives and do not facilitate the development of children's autonomous understanding of privacy (Raynes-Goldie and Allen, 2014). Steeves and Regan (2014) point out that most educational programmes (e.g., EU's Ins@fe initiative, the myprivacy.mychoice.mylife campaign by the Privacy Commissioner of Canada and the US government's Kids.gov) refer to privacy as information control, advise children on the dangers of disclosing personal information, and associate the lack of disclosure with safety. This not only creates the image of the online environment as dangerous and unsafe, but also does not correspond to children's own concerns (Steeves and Regan, 2014).

Privacy literacy skills need to be enacted by children, rather than taught as external rules, and need to reflect the actual concerns and experiences of children (Raynes-Goldie and Allen, 2014). Most positive effects are observed when children are able to make more autonomous decisions about effectively protecting themselves online, can gain experience in coping with unexpected or undesired situations, and are able to learn from mistakes (Youn, 2009; Feng and Xie, 2014; Wisniewski et al., 2015; Wisniewski, 2018). While a substantial number of studies explored children's strategies to protect their privacy and the occasions when they fail to do this, we did not find a comprehensive framework that discusses the different dimensions of privacy skills that children need in order to protect effectively their privacy online and to remain safe from harm. A much better understanding of what digital skills are needed in the area of privacy is needed, which not only distinguishes between awareness and behaviour and conceptualises privacy skills as part of more comprehensive media literacy, but also takes into account the difference between risks and harm – what is detrimental for one child might be harmless for another.

5.7. Differences among children

Not all children are equally able to safely navigate the digital environment, taking advantage of the existing opportunities while avoiding or mitigating risks. The evidence mapping demonstrates that differences between children might influence their engagement with privacy online, and while ideally the evidence base would be more robust, there is certainly an argument to be made for the benefits of child-focused perspectives which give recognition to children's voices and explore their heterogeneous experiences, competencies and capacities.

Socio-economic inequalities

Socio-economic inequalities are under-researched in relation to privacy, but some of the existing evidence suggests that effects related to device ownership and use, as well as parental practices, might cause disadvantages to some children (Dennen et al., 2017; Acker and Bowler, 2018). A comparative European study found that socio-economic status (as well as age and gender) made a difference in relation to online privacy. Children from lower SES were much less likely to have a public social media profile or to share personal data, such as their address or phone number (Livingstone et al., 2010). While UK children were much more likely to guard their privacy online than their European peers (by having a private profile, starting to use social media when older, having fewer online contacts, sharing incorrect age), socio-ecnomic inequalities still make an important difference (Livingstone et al., 2010; Livingstone et al., 2014).

Similarly, Feng and Xie (2014)'s study of socialisation and privacy-protection strategies of US children

aged 12 to 17 found that teens whose parents have higher educational levels tend to be more concerned about their online privacy, which may be attributed to more active mediation strategies by parents. There was a signifcant relationship observed between children's level of privacy concern and their privacy-setting strategies – they were more likely to set their profile to private or partially private if they are concerned with privacy, and children with better educated parents were better off in this regard. We discuss the impact of parenting on children's privacy skills in more detail later on in this report (see section 5.10).

The importance of socio-economic inequalities was also highlighted by a qualitative research exploring the privacy strategies of low-income and minority ethnic US youth aged 14 to 19 (Vickery, 2015). The study found that young people from this group want to control the context in which their information is shared and who has access to it. Yet, they often have limited access to technology and experience more strongly the need to share devices which may disturb their privacy and create the need for constant negotiation: 'the boundaries of sharing and privacy are constantly renegotiated at the intersection of localized social norms, economic and social capital, and the technical affordances of particular platforms and devices' (Vickery, 2015: 282). This leads to a blur of what constitutes a private or shared device. Furthermore, young people from low-income backgrounds were found to be subject to greater surveillance through different activities and obligations.

In this context, the mobile phone served as a status symbol and a gateway to greater independence and freedom, but some teens also chose to disconnect as a way of maintaining privacy and reverse typical power dynamics. Others split their online activities across different platforms in a fluid and disconnected manner which was a 'deliberate privacy strategy intended to resist the ways social media industries attempt to converge identities, practices, and audiences' (Vickery, 2015: 289). Different contextual norms of privacy underpinned the different platforms, and young people navigated away from the ones they felt more closely monitored. Young people from low-income backgrounds also experienced the misinterpretation of their identities and communicative practices by majority peers, which created a complicated need to navigate across cultural contexts and the feeling of lack of privacy when these contexts collapsed. While all young peeople balance strategies for protection with opportunities for participation, some marginalised groups also feel the need for self-censorship and disconnection, which silence them further (Vickery, 2017). While there was substantial evidence to demonstrate that socio-economic inequalities play an important role in relation to children's privacy, more research is needed to explain the actual effects.

Gender differences

Most of the research on online behaviour in highly internet-penetrated countries shows little gender differences in internet use and online risks, yet some of the existing evidence in relation to privacy demonstrates important gender differences in privacy risk perception, the level of concern and protection behaviours. A study of Canadian girls (aged 15-17) and young women's (aged 18-22) experiences with social media and their perspectives in policy-makers' debates found that girls are overlooked within policy and policy responses, relying on gender-neutral language and ignoring the socio-cultural norms that play out in online spaces (Bailey, 2015). Girls also experience the impacts of stereotypical notions of female beauty and technological architectures that simultaneously enabled and limited control over their fully integrated online/offline lives. The perceived gendered risks of loss of control over data or appropriation of their data made privacy exceptionally important to girls (Moscardelli and Divine, 2007; Bailey, 2015; Malik et al., 2015). In some contexts such gender stereotypes can affect girls' access to technologies and freedom of online participation, for example, due to tighter parental regulations and more intense monitoring (Badri et al., 2017).

Several studies found that girls are less likely to reveal personal information, to accept requests from unknown people, and more likely to engage in protective behaviours than boys (Steeves and Webster, 2008; Mullen and Hamilton, 2016; Öncü, 2016). For example, a survey of children aged 9-18 from Australia, Japan, Indonesia, Korea and Taiwan found that girls in these countries were overall much less likely to take 'provocative pictures' than boys, while evidence from Ireland showed that girls are more likely to be online friends with their parents (Mullen and Hamilton, 2016). Still, there was some

evidence that girls face more risks – survey data from 395 high school students in the USA aged 14 to 18 show that girls are more likely to experience misuse of personal information and receive unwanted emails (Youn and Hall, 2008). Girls also perceive privacy risks to be more serious than boys, which includes feeling more uncomfortable about privacy risks and reporting higher likelihood of conflicts with parents or teachers about such risks. Boys, on the other hand, are more likely to read unsolicited emails and to provide their information to websites, but are also more likely to send complaints about spam (Youn and Hall, 2008).

However, not all studies find gender significant in influencing privacy behaviour, and some studies show the opposite. For example, a survey of USA children aged 12 to 16 found that girls are more likely to contact strangers online and to have a social media profile earlier on (Martin et al., 2018), while a Croatian survey of children aged 14 to 18 found no differences based on gender and age (Velki et al., 2017). More evidence is needed to explain the different conclusions and explore gender differences throughout child development. It is possible that gender differences vary between cultural contexts, and some gaps are bigger at a younger age and diminish later in life.

Vulnerability

We did not find robust evidence on vulnerable children which explores effects on privacy in relation to the digital environment. There was an acknowledgement that the existing privacy protection model which has a parent-centred approach reinforces existing privileges and leaves out the most vulnerable groups of children, such as foster children (Wisniewski, 2018). There was also some evidence that children who thought they could rely on their family for support when needed were less likely to share personal information with a large number of online friends, while those who relied more on support from friends and significant others were more likely to have more contacts online (Öncü, 2016). However, studies looking at the impact on vulnerable children were mostly missing.

During the literature search we came across a number of studies on vulnerable young adults, which remained outside the scope of the final review. Some of the excluded examples – related to posting more frequently and experiences of loneliness (Al-Saggaf and Nielsen, 2014) and experiences of stigma towards disclosing sensitive information about illness and medication (Zhang, 2012) – are worth mentioning here as they demonstrated some connection between vulnerability and online privacy behaviours. They suggest that more evidence is needed to explore if there are any similar effects at a younger age and to establish if perceived vulnerabilities might influence privacy-protective behaviours. It is necessary to identify if such impacts are significant, if they lead to higher likelihood of experiencing harm and what types of vulnerabilities are at play. On the other hand, digital technologies can be used to create new opportunities and improve digital skills of vulnerable children. For example, a number of studies in the sample demonstrated that designing interactive technologies for children with special needs can offer new opportunities for support and participation, addressing the freedoms and rights of these children (Alper et al., 2012). Hence, the positive effects and opportunities of digital technologies on living with vulnerability have been explored in much greater depth, while the evidence on any possible negative effects on children's privacy is lacking.

5.8. Privacy-related risks of harm

Privacy concerns have intensified with the introduction of digital technologies and the internet due to their ability to compile large datasets with dossiers of granular personal information about online users (Selwyn and Pangrazio, 2018). A substantial body of literature discusses privacy online risks that children face: these are related, on the one hand, to the technological affordances and digital ecology, and on the other, to children's own online practices. Key issues that have come to the fore include online marketing and commercial activities, awareness of and willingness to provide personal information online, the effects of privacy disclosures (including reputational damage, blackmailing, stalking or identify theft), issues related to participation on social networking sites, and unawareness of the privacy online policies of platforms. Children are perceived as more vulnerable than adults to privacy online threats, such as re-identification, due to their lack of digital skills or awareness of privacy risks (Children's Commissioner for England, 2017a). There is also a link between the amount of time spent online and involvement in social networking sites, which is positively associated with online information

disclosure (Steeves and Webster, 2008; Shin and Kang, 2016). This trend, however, is not new, as existing research on children's internet use demonstrates that more time spent online is linked to more opportunities and more risks (Livingstone and Helsper, 2010).

The technology-related privacy risks are linked to features such as GPS-enabled tracking, potentially creating threats to anonymisation due to coarse-grained location data or undesirable tracking, or ecology-based features such as the ease of obtaining fake social media accounts which can result in spreading malware, stealing personal information, spying on users' activity or inflicting the digital environment with fake content. The consequential risks relate to brokers selling the data to other agents (advertisers, further education recruiters and employment agencies), fuelling large-scale and highly personalised spear-phishing attacks, and exposure to perpetrators of child sexual abuse and violence (Dey et al., 2013; Murumaa-Mengel, 2015).

Children's own online practices have been under substantial scrutiny for privacy risks. Often children's privacy is viewed from a normative adult perspective, representing them as carelessly oversharing personal information, and is entangled with issues of security and the need to face risks to physical, emotional and academic/vocational safety. What information children make publicly available has received considerable research attention, with studies pointing out that a significant amount of 'private' information (current city and school, graduation year, inferred year of birth and list of school friends, favourite activities, music, films and relationship information) can be directly available on social media, including profiles of minors registered as adults (Almansa et al., 2013; Dey et al., 2013) and even information about engagement in illegal activities (Williams and Merten, 2008).

A survey with Canadian children aged 11 to 17 found that large proportions of children were willing to disclose personal information such as real name, address or email when engaging with different online activities: signing up for a free email account (76%), creating a social media profile (76%), posting on their blog (57%), entering a contest (56%), registering for a game site (69%), participating in a chat room or discussion forum (48%) or using a dating site (39%) (Steeves and Webster, 2008). Almost half of the respondents (49%) had never read the Terms and Conditions of the sites they visit and thought it was safe to share secrets via email and online messages (45%), and nearly a third (31%) had shared passwords with friends. The risky behaviour increased with age – at the age of 17 42% of children were most willing to disclose personal information, compared to 39% of the 15-year-olds and 21% of the 13-year-olds. At the same time the older children were less likely to engage in protective behaviour – 38% of the 17-year-olds compared to 36% of the 15-year-olds and 26% of the 13-year-olds were classified as least likely to use protective behaviours. The older children were also more likely to report intentionally visiting websites with adult content (pornography) – 21% of the children aged 17, 18% of those aged 15 and 7% of those aged 13 (Steeves and Webster, 2008).

Another source for concern is to whom this information is available as some children have public profiles that might be accessed by people unknown to them. While there is no convincing evidence that such contact with 'strangers' results in experiences of harm, and some existing studies on internet use acknowledge that these perceived 'strangers' are likely to be just friends of friends (Byrne et al., 2016), the fact that children share personal information with people they might not know is automatically seen as a privacy risk. The evidence usually explores the type of information shared online and to whom it is available. For example, a qualitative study of Spanish and Columbian school students aged 12 to 15 found that children are quite generous with the personal information they share online – more so in Spain than in Colombia – and adding unknown people as friends was not uncommon (Almansa et al., 2013). This meant that unknown people had access to their personal information – about a third of the students' profiles contained personal information, such as birthday, address and school, as well as favourite activities, music, films, and about a fifth relationship information. However, other studies which looked at regret of posting did not find that privacy settings or self-disclosure increased the likelihood of regretting sharing the information (Xie and Kang, 2015). Therefore, 'stranger danger' seems to be more of a normative perception of what privacy risks are rather than evidence-based observation about increased harm.

In spite of the substantial focus on privacy online risks, much less attention is paid to children's experiences of harm from the risks, making the evidence on any negative consequences from

privacy breaches rather scarce. While studies on the negative effects from privacy risks on young adults exist (see for example Alkis et al., 2017 about the effects of unintended disclosure of personal information on anxiety), more research is needed to explore any potential links between privacy risks and harms and their effects on children. Some evidence on how teenagers approach risk demonstrates that they seem to perceive privacy risks 'as a learning process' (Wisniewski, 2018: 87), taking measures when risks have escalated to a potentially harmful situation. Hence, the ability to handle these risks is an important part of the learning and development process, and foreclosing these risks would limit children's autonomy and ability to develop.

5.9. Privacy protection and children's autonomy

Surveillance, globally, is becoming the norm in public spaces, even when occupied by children. Mobile phones have brought surveillance and monitoring into the realm of personal relationships, normalising the perception that all children should be accountable and accessible at any time and place, with parental surveillance gaining increased prominence. No longer about discipline and control alone, surveillance now contains facets of 'care' and 'safety', and is promoted as a reflection of 'responsible and caring parents' and is thus normalised (Barron, 2014).

However, child surveillance raises a number of problems – first, in relation to the practice itself; second, due to the underlying assumptions about risk, safety and childhood; and finally, in relation to breaches to children's rights to autonomy and independence. Efforts to create a 'risk-free environment' are unrealistic and unachievable (Barron, 2014). The existing research evidence demonstrates that with greater presence in the digital environment, children face greater risks but also more opportunities (Livingstone and Helsper, 2010). While working to reduce online risks and maximise opportunities is an excellent approach to creating the optimal online environment for children, it is important to remember that every child will be exposed to risks at some point, and a risk-free environment is unfeasible, both online and offline. Risk aversion also restricts children's play, development and agency, and constrains their exploration of physical, social and virtual worlds (Barron, 2014). Surveillance can have negative effects by limiting independence, reducing pro-active risk management (Wisniewski, 2018) and undermining children's right to participation. It might obstruct children's development of important skills, such as learning to be 'street smart', and it could affect negatively the trust relationship between the parent and the child.

Finally, the existing evidence demonstrates that surveillance creates resistance in children and deployment-evasive tactics to avoid or circumvent monitoring or discovery of rule-breaking. The strategies involve pretending the mobile was in a silent mode, it ran out of credit, or had a flat battery, giving false information, deleting texts or using specific characteristics or codes in texts that are likely to make them hard to read by adults (Barron, 2014). Children's engagement in online spaces can serve a social role – allowing them to make sense of the world and their relationship to society, to explore their own identities and interests in relation/resistance to the norm – in ways that are less significantly influenced or controlled by adults compared to physical spaces (boyd and Marwick, 2011). The social space of networked publics takes on greater significance and critical value – it functions as a communication channel, and also as the space holding an 'imagined community' (boyd and Marwick, 2011).

5.10. Supporting children

While the task of managing a healthy balance between children's independence and protection is challenging, there is a substantial amount of evidence demonstrating that the right support makes an important difference to children's privacy online. The existing evidence focuses predominately on the role of parents, while other sources of support such as educators and child support workers need more exploration. Friends are, alongside parents, amongst the most important sources of both information and support (Byrne et al., 2016; Walker et al., 2016) but again, this is rarely evaluated in relation to prvacy. Parental mediation research focuses on the role of parents as socialisation agents in adolescents' media consumption and the strategies that they employ to control and supervise media use. In relation to privacy, the studies explore the role of parents in children's privacy online concerns and information-disclosing behaviour.

The notion that children are at risk online due to their poor decisions related to privacy and information disclosure is prevalent in the litarature. While restrictive online practices reduce privacy risks, they also reduce the online benefits and do not teach children to effectively protect themselves online (Wisniewski, 2018). For example, parental supervision can reduce children's willingness to disclose personal information and can increase children's privacy protective strategies (Steeves and Webster, 2008).

Still, it is not sufficient to fully protect children's online privacy as it only reduces privacy risk-taking but does not eliminate it. Some of the behaviours that can be seen as risky (sharing passwords, pretending to be someone else online, posting personal information) can be explained by children's perception of the online environment as a place for socialising and the importance of sharing information for maintaining friendships – predominantly with people they already know and trust. In such cases parental supervision is not effective because it is incompatible with children's social needs and expectations (Steeves and Webster, 2008). Even when effective in reducing privacy risk-taking, parental supervision cannot remove risks – even children with the highest level of parental supervision who are amongst the most active in social interaction are less likely to display privacy-protective behaviour than those with low levels of engagement in social interaction (Steeves and Webster, 2008). Furthermore, children's understanding of online privacy-protection practices does not necessarily translate into reduced privacy risk-taking (Steeves and Webster, 2008).

It can be argued that privacy-protection strategies, such as adjusting privacy settings, should be seen as a form of resilience behaviour (Rimini et al., 2016). Resilience, understood as 'an individual's ability to thrive in spite of significant adversity or negative risk experiences' (Wisniewski, 2018: 87), can be increased by modifying emotions and behaviours, for example, via self-monitoring, impulse control (prioritising long-term consequences over short-term desires) and risk coping (addressing an encountered problem in a way that reduces harm, which is influenced by children and parents' risk perception). In fact, privacy-protective behaviours are linked to stronger self-efficacy and exposure to information from verious sources (Moscardelli and Divine, 2007; Chai et al., 2009). Experiential learning allows risk-taking behaviours to act as learning opportunities and contribute to the development of risk-coping behaviours (risk acting as a learning process) (Jia et al., 2015). When faced with privacy risks, children tend to attempt to manage low-level risks on their own and turn to external support for higher-level risks, which ties in to their developmental learning processes. Hence, exposure to privacy risk and subsequent coping mechanisms should be viewed as a part of children's learning processes and development as competent digital users (Jia et al., 2015).

Earlier research on children's internet use demonstrated that there are different styles and approaches of parenting mediation, which have, in turn, different effects on children's online behaviour and competence. Restrictive mediation (control-based) refers to parents' limiting access to media or rule-setting about appropriate media context or exposure. Enabling mediation (autonomy-supportive) refers to parents' explaining or discussing undesirable aspects of media consumption and suggesting proper ways in which to use and engage with it. The existing evidence suggests that enabling mediation, by virtue of its critical discussion and engaging in dialogue, is more effective. Restrictive mediation can be effective in reducing risks associated with children's online use, but can cause boomerang effects by limiting children's online opportunities. The research on parenting and privacy online uses the same parenting mediation model to explore the effects on children's privacy online.

In their study of the effects of parenting styles on children's privacy (including secondary analysis of the 2012 Pew Research Center's privacy management survey of 588 USA-based teenagers aged 12 to 17 and one of their parents), Wisniewski et al. (2015) found that 81% of parents were worried about their child's privacy online. Parents who were more concerned engaged more in privacy measures, but the different strategies they used had different effects on their children's behaviour. The authors identified two types of parental mediation strategies: (i) direct parental mediation (reflecting technical and restrictive mediation and including the use of parental controls, setting the child's privacy settings); or (ii) active parental mediation (instructive or monitoring behaviours including talking about posting practices and reviewing or commenting on existing posts). The study also

identified two types of children's privacy behaviour on social media: (i) privacy risk-taking, which included sharing of basic information (such as photos, name, date of birth and relationship status) or more sensitive information (videos of themselves, mobile number, email address) and taking part in risky interactions (e.g., talking to online strangers, regretting posting online content, automatic location sharing); and (ii) privacy risk-coping involving seeking advice or engaging in safety behaviours such as posting fake information, deleting content, blocking or deleting contacts, and deactivating one's account (Wisniewski et al., 2015).

The study found that children whose parents engaged in a more direct intervention were less likely to disclose basic information online and more likely to seek advice but were also less likely to engage in safety behaviours. Parental active mediation was linked to higher likelihood of disclosure of sensitive information and engagement in safety behaviour, meaning that children made more autonomous decisions and were encouraged to learn from mistakes. Children whose parents were more concerned about privacy also showed a higher level of concern and were, in turn, more likely to seek advice and engage in safety behaviours. Children who engaged in one type of risky behaviour (e.g., sharing basic data) were also more likely to engage in others (sharing sensitive information). Children associated only risky interventions with higher privacy risk, which was, in turn, linked to advice seeking and coping behaviours, while sensitive information was associated only with coping behaviours and basic information was not linked to either perceptions of higher privacy risk or coping behaviour.

Based on this, the authors suggests that children have mainly retrospective behaviour when it comes to privacy risks (Wisniewski et al., 2015). Controlling parents had the most suppressive effect – reducing privacy risk, corrective behaviours but also frequency of use of social networks and the network complexity of their children. Active mediation was found to be more empowering as children engaged with social networks more, experienced some risk, but also engaged in coping behaviours. This was observed particularly strongly for the children of highly engaged parents who had high engagement and complex social networks, despite the restriction from direct parental intervention. None of the parent styles were effective in reducing contact with strangers, possibly because the children did not disclose this to their parents.

A number of other studies also demonstrate the better outcomes of enabling parental mediation in relation to privacy (Moscardelli and Divine, 2007). A survey with 395 secondary school students from a public school in the USA found that family communication patterns affect children's perceptions of privacy-related parental mediation, their privacy concerns and the formulation of privacy protection measures (Youn, 2008). Rule-making did not create higher privacy concern, but co-using the internet with parents and discussions about privacy resulted in higher privacy concern, suggesting that children had developed a better privacy risk awareness. The children who were more concerned about privacy also supported government regulation, school education and wanted the right to be forgotten (name removal request) (Youn, 2008). Similarly, in a survey with 746 children in Singapore aged 12-18, Shin and Kang (2016) found that enabling mediation was more effective in reducing privacy risks – it was negatively associated with intention to disclose personal information and also with actual disclosure. Adolescents who frequently talked to their parents also had heightened privacy concerns, which may indicate heightened awareness.

While this evidence puts enabling mediation at the centre of effective improvement of children's privacy online, platform and app features often prompt technical solutions. A study of 75 commercially available mobile apps on Android Play found that an overwhelming majority of features (89%) within these apps supported parental control via monitoring or restriction rather than active mediation. In addition, many of the apps were 'extremely privacy invasive, providing parents granular access to monitor and restrict teenagers' intimate online interactions with others, including browsing history, the apps installed on their phones and the text messages teens sent and received' (Wisniewski, 2018: 88). In the analysis of the reviews of these apps, Wisniewski found that children evaluate the apps much less positively than parents, and experience them as restrictive and invasive. The possible solutions can involve encouraging children to self-regulate their behaviour, designing apps based on children's needs and safety features which do not compromise privacy (e.g., by giving parents access only to meta-level information and not the

granular details) (Wisniewski, 2018). Most importantly, children's privacy needs to be facilitated by enabling parental mediation, and channels of further support through education need to be explored.

Privacy online training for parents, educators and child support workers should also be considered as the evidence suggests important gaps in adults' knowledge of privacy online risks and the best protective mechanisms (Chaudron et al., 2018). Parents and educators alike lack the understanding of third party gathering and use of personal information, and may fail to recognise the privacy risks of online educational activities (Walker et al., 2016). Parents also struggle to moniotor what children do online, find it hard to understand the privacy protocols, are sometimes unaware of the minimum age requirements of apps, and struggle to support children sufficiently in relation to privacy (Walker et al., 2016; Ofcom, 2017b). They might also fail to comprehand the full extent of commercial risks for children's privacy. For example, an ethnographic study of children aged 7-18 and their parents showed that parents understand children's privacy risks as external threats (from predators, adult content and spyware) and risks from inadvertent revealing of personal information by children, but lack sufficient comprehension of commercial risks (Rode, 2009).

Even when parents are aware of the privacy implications of their children's internet use, they might be unable to monitor this sufficiently. For example, a qualitative study with parent–child pairs in the USA focusing on the exploration of parents and children's perceptions of the privacy of internet-connected toys discovered that the parents were sensitive to the issues surrounding the constant child data recording and how this data would be retained and used by the companies. Still, they doubted that they would have the time to listen to the recordings and check what data the company has on their child (McReynolds et al., 2017). Quite often parental mediation strategies include monitoring of children's actions with or without technological aids, using blocking technology for certain activities deemed risky or threatening, encouraging self-restraint and discussing safe behaviour (Rode, 2009). While these strategies are important for children's online safety, the gaps related to commercial and institutional use of children's data are symptomatic. Hence, a really comprehensive system supporting both children and adults around all types of privacy and online data is necessary for developing privacy-related media literacy.

6. Recommendations

- **Introducing a comprehensive approach to privacy online**

While a substantial amount of research is focused on children's interpersonal privacy, much less attention is paid to institutional and commercial privacy, even though the evidence demonstrates that children struggle to fully comprehend and manage the commercial use of their personal data. A more comprehensive approach which tackles all dimensions of privacy in developing awareness and capabilities is needed to address these gaps.

- **A balance of protection and autonomy**

A healthy balance between children's independence and protection can foster their development, agency and exploration of the physical, social and virtual worlds. Policy and educational measures to ensure children's privacy online and safety should also facilitate their autonomy, pro-active risk management and right to participation.

- **A child-focused approach**

With growing concerns over children's privacy online and the commercial uses of their data, it is vital that children's understandings of the digital environment, their digital skills and their capacity to consent are taken into account in designing services, regulation and policy. A child-focused approach can give recognition to children's voices and facilitate and support their heterogeneous experiences, competencies and capacities. It can also create opportunities of peer-to-peer support and a more inclusive and tolerant online environment.

- **Banning discrimination or less favourable treatment based on personal data**

Getting access to personal data can result in future discrimination or less favourable treatment (e.g., in relation to education, employment, credit or insurance opportunities). Data provided during childhood can 'follow' individuals through their adult life due to the longevity of the traces left online. Therefore, policy attention needs to be focused on preventing less favourable treatment and discrimination based on harvesting personal data and using it in ways that go beyond its original intention, especially if this data is collected from a person under the age of 18. 'Rights by design' is vital so a child could check, contest, rectify, erase or edit information about themselves.

- **Digital skills and privacy education at an early age**

Children start facing privacy decisions and risks as soon as they enter the digital environment, long before their media literacy prepares them to make decisions in their own best interests. Some studies demonstrate the effectiveness of interactive learning materials to introducing privacy-related issues (such as protection of personal information, online trust, location sharing, cyberbullying and passwords, digital trail) to children as young as 7 (Zhang-Kennedy and Chiasson, 2016; Zhang-Kennedy et al., 2017). Privacy proficiency tests show significant improvement in children's privacy knowledge and privacy-conscious behaviour retention after one week, highlighting the great potential of digital and privacy skills education at an early age (Zhang-Kennedy and Chiasson, 2016; Zhang-Kennedy et al., 2017). In addition, media literacy and privacy-related skills need to be enacted by children, rather than taught as external rules, and need to reflect the actual concerns and experiences of children (Raynes-Goldie and Allen, 2014). Children need to be able to make more autonomous decisions about effectively protecting themselves online, to gain experience in coping with unexpected or undesired situations, and to learn from mistakes (Youn, 2009; Feng and Xie, 2014; Wisniewski et al., 2015; Wisniewski, 2018).

- **Focus on individual differences and psychological factors**

Individual differences and psychological factors should be at the centre of privacy policy and evidence gathering, rather than technological factors, as they are the most influential in explaining children's privacy awareness, experiences and behaviours. A better understanding of what personal and environmental influences contribute to children's effective management of their privacy online can facilitate a more efficient approach to privacy literacy. The current evidence suggests that existing vulnerabilities and social marginalisation (Marwick and boyd, 2018), child development (Kumar et al., 2017) and values towards privacy and trust (Steeves and Webster, 2008; Youn, 2009) are important ways of accessing and explaining the differences between children – a starting point

towards designing better privacy protection and media literacy education.

- Supporting children by supporting adults

Adults are often left feeling 'behind' digital developments and struggling to identify the best ways to support children. A comprehensive system supporting both children and adults around them – parents, educators and child support workers – is a prerequisite for developing effective media literacy. Rather than focusing predominantly on parental mediation, a wider approach which engages children's support networks in their full breadth can allow children in different circumstances to receive the support they need.

- Improving the privacy affordances of the online environment

The available evidence also suggests that children are not fully aware of the threats coming from commercial entities that collect, record and aggregate data on their platforms, and nor do they fully understand how their data is used for economic profit by targeting ads or customising content. Further work is needed to increase the transparency of data collection, improve privacy control navigation, enable granular control over privacy settings to match the elaborate data-harvesting techniques and create better industry standards around user empowerment. Ease of use, ubiquitous functions and user-friendly features of the privacy setting interface may reinforce children's privacy protection behaviours.

Children cannot be expected to be solely responsible for handling the complex commercial environment. This makes necessary the changes to the business model which would not only make personal data use more transparent, but would also enable children to engage more actively and agentically with the online platforms, raising their critical awareness (Selwyn and Pangrazio, 2018). Some possible changes include:

  - The principle of data minimisation by default is crucial in ensuring that children's data is gathered only when it is service-critical and is not shared with third parties, reducing the fake 'voluntary' data sharing by children.
  - 'Default' settings can be improved by switching data harvesting and profiling off by default safeguard children's personal data more efficiently, protecting particularly children who do not know how to change their settings.
  - Hidden paid-for activities including in-app purchases are hard for children to identify and can lead to unintended exposure to commercial content, sometimes unsuitable for the child's age. Transparency and age verification are needed to redress these issues.
  - Designing age-appropriate content needs to be an ongoing process that takes into account the wider digital ecology and children's changing knowledge, needs and competences within the dynamic internet environment.
  - Location of responsibility should lie within the industry, rather than children, their parents and educators. The focus should fall on the overall design of online environment and its ecology, rather than enforcement of regulatory measures.
  - A close working collaboration between government, industry, educators and child representatives for creating a sense of shared ethical responsibility for delivering high-quality services to children is needed.

- Better evidence base

The evidence mapping identified substantial gaps in existing knowledge in relation to all dimensions of privacy online, but particularly with reference to institutional and commercial uses of data. More research is needed to improve our understating of how children's developmental needs affect privacy risks and related media literacy; what skills are needed to protect online privacy and how best to teach these skills to children; what support strategies are most efficient in helping children to take advantage of the existing opportunities, avoid harm and foster resilience and self-efficacy; and what policies and regulations are best equipped to mitigate privacy risks and foster a safe online environment for children.

Appendices

Appendix 1: Detailed methodology

Approach

We expected the body of literature focusing directly on children's interactions with online commercial environments would be sparse, and so adopted an inclusive approach to the literature search, recognising that research might be published across the psychological and social sciences, including media studies, legal studies and computer science.

We applied the following inclusion criteria in searching for evidence:

- Relating to children's online privacy – interpersonal, institutional or commercial.
- On children's privacy protection strategies, media literacy and digital skills.
- Exploring children's perspectives and experiences of privacy, online environments and digital skills (expanded to include adults if relevant to children's experiences or when children are included, for instance, in research on families or parents).
- From any country but published in English.
- Published since 2007 to ensure relevance for current contexts and current technological advances.
- Preferably published in peer-reviewed journals, although policy or advocacy-related publications from non-governmental organisations (NGOs), government reports, industry sources and other relevant grey literature that meet quality requirements were included.
- Deriving from high-quality, methodologically robust research, both in terms of the systematic evidence mapping and in terms of the sources analysed.

A systematic evidence review approach, seen as 'the classical' evidence review (Gough et al., 2012), was considered. However, in seeking to include a wide range of literature to capture the complexity of online privacy in relation to commercial use and its implications for children, the team applied a systematic mapping of evidence (Grant and Booth, 2009; Gough et al., 2012; EPPI-Centre, 2018).

Thus, the search strategy included a broad range of sources such as end-of-year reports, policy recommendations, conference papers, advocacy tools, methodological guides and case studies. To capture the depth of complexity and insights available in the disciplines, the team requested input from a range of experts on recommended literature and research sources, which added to the comprehensiveness of the results (see the Acknowledgements). This allowed us to describe the nature of the research field and facilitated the interpretation of the findings, informing our final synthesis.

Search terms and outcomes

In consultation with the LSE academic support librarian Heather Dawson, the team selected 19 databases based on their suitability to the review's scope and aims. These cover the social sciences, legal studies, computer science studies, government publications, legal documents and grey literature.

We categorised the search terms into three groups: (i) child terms, (ii) technology terms and (iii) privacy terms. Search testing was conducted to ensure validity, optimal coverage and efficiency. The terms were discussed, conceptually mapped and reviewed by the team for reliability, before fine-tuning them to produce the final search combination:

- Group 1, **child** terms: child* OR youth OR teen* OR adolescen* OR minor OR kid OR girl OR boy OR student OR pupil
- Group 2, **technology** terms: digital* OR mobile* OR internet OR online
- Group 3, **privacy** terms: priva*

The search included title AND abstract AND keywords (where keyword search was available). For some databases, search options restricted us to abstracts, metadata, keywords or title only. In the initial search testing, Group 2 included the term 'data' but this returned a large number of extraneous results. In Group 3 we attempted including 'data' and 'secur*' but this produced a large number of irrelevant sources and were therefore removed. The search produced 9,119 sources (see Table 3). The expert recommendations and grey literature additions bring the total to 9,398 sources in all.

Table 3: Databases, search protocol and results

Database	Search words	Period	Search areas	Language filter	Number of results
Web of Science Core Collection	Groups 1, 2, 3	2007-18	Topic	English	2,365
Scopus	Groups 1, 2, 3	2007-18	Title and abstract	English	2,865
International Bibliography of the Social Sciences (IBSS)	Groups 1, 2, 3	2007-18	Title and abstract	English	216
Communication & Mass Media (via EBSCO)	Groups 1, 2, 3	2007-18	Title and abstract	English	210
ERIC (via EBSCO)	Groups 1, 2, 3	2007-18	Title and abstract	English	848
Child Development & Adolescent Studies (via EBSCO)	Groups 1, 2, 3	2007-18	Title and abstract	N/A	66
British Education Index (via EBSCO)	Groups 1, 2, 3	2007-18	Title and abstract	English	62
SocINDEX (via EBSCO)	Groups 1, 2, 3	2007-18	Title and abstract	English	173
IEEE/IET electronic library	Groups 1 and 3	2007-18	Metadata	N/A	1,440
ACM Digital Library	Child* and Priva*	2007-18	Abstract	N/A	71
CORE's Open Access	Child* and Priva*	2007-18	Title and abstract	N/A	0
PAIS International	Groups 1, 2, 3	2007-18	Anywhere but full text	English	147
Criminal Justice Abstracts (via EBSCO)	Groups 1, 2, 3	2007-18	Title and abstract	English	96
HeinOnline	Groups 1, 2, 3	2007-18	Title (no abstract search)	English	32
Index to Foreign Legal Periodicals (IFLP) via HeinOnline	Groups 1, 2, 3	2007-18	Keyword	N/A	1
Westlaw UK	Search within results of Group 1 adding Group 3	2007-18	All	N/A	35
Lexis Library	Search within results of Group 1 adding Group 3	NA	All	N/A	11
SSRN Papers	Search within results of Group 1 adding Group 3	NA	Title, abstract, key words	N/A	481
BALII	Search within results of Group 1 adding Group 3	2007-18	All	N/A	0
Experts	N/A	2007-18	N/A	English	279
				TOTAL search results	9,398
				TOTAL search results without duplicates	6,309
				Final sample after screening	105

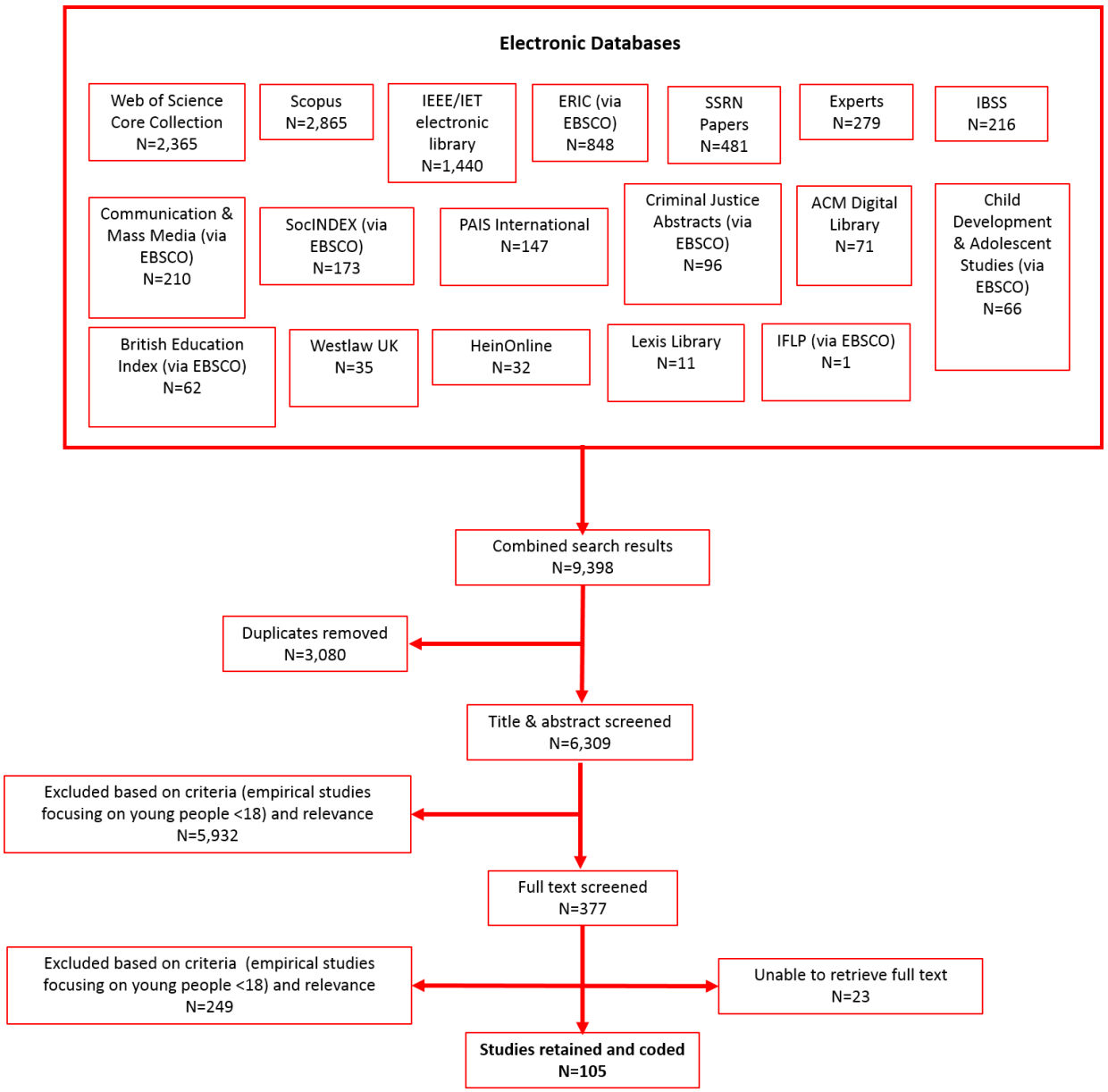
Databases searched

Database	Description
Web of Science Core Collection	Provides access to articles covering all aspects of the sciences, social sciences and humanities
Scopus	Covers a wide range of science and social science subject areas including gender studies, women's studies and LGBT issues
International Bibliography of the Social Sciences (IBSS)	Includes over 3 million bibliographic references dating back to 1951
Communication & Mass Media (via EBSCO)	Full text and cover-to-cover indexing and abstracts for journals on communication, mass media, linguistics, rhetoric, language, logic and closely related fields
ERIC (via EBSCO)	The Education Resources Information Centre (ERIC) is an authoritative database of indexed and full-text education literature and resources. Sponsored by the Institute of Education Sciences of the US Department of Education
Child Development & Adolescent Studies (via EBSCO)	This bibliographic database is a key source for the current and historical literature related to the growth and development of children up to age 21
British Education Index (via EBSCO)	Provides information on research, policy and practice in education and training in the UK and some international literature. Covers all aspects of education from preschool to higher education; sources include education and training journals
SocINDEX (via EBSCO)	This bibliographic database provides high-quality indexing and abstracts for journals covering the broad spectrum of sociological study
IEEE/IET electronic library	Contains almost one-third of the world's current literature in electrical engineering, communications and computer science
ACM Digital Library	The world's most comprehensive database of full-text articles and bibliographic literature covering computing and information technology
Core Open Access Search	Aggregates all open access research outputs from repositories and journals worldwide
PAIS International	Produced by the Public Affairs Information Service, this indexes the content (often with abstracts) of over 1,000 journals, as well as some books, theses and government documents, on the subjects of public affairs, international relations, social policy and other social science subjects. Coverage is from 1972 onwards
Criminal Justice Abstracts (via EBSCO)	This bibliographic database provides records selected from the most notable sources in the criminal justice field. It covers journals from around the world, reflecting the increasing globalisation of criminology studies
HeinOnline	Premier online database containing more than 155 million pages and 200,000 titles of legal history and government documents in a fully searchable, image-based format, provides comprehensive coverage from inception of over 2,500 law-related periodicals and contains entire databases dedicated to treaties, constitutions, case law, world trials, classic treatises, international trade, foreign relations and more
Index to Foreign Legal Periodicals (IFLP) via HeinOnline	Preeminent multilingual index to articles and book reviews in over 500 legal journals published worldwide. It provides in-depth coverage of public and private international law, comparative and foreign law and the law of all jurisdictions
Westlaw UK	Easily searchable source of case law, legislation, news, legal journals, commentary, current awareness alerts and EU legal materials

Lexis Library	A legal database which provides access to selected full text case law, legislation and journal articles from the UK, EU, US and other selected jurisdictions worldwide
SSRN Papers	Research repository that spans across multiple disciplines
BALII	British and Irish Legal Information Institute covers British and Irish case law and legislation, European Union case law, Law Commission reports and other law-related British and Irish material
Expert Literature	We included 279 sources recommended by experts in the field in the systematic review, retaining 26 in the final scoping

Screening

Figure 3: The screening process



The collection of 9,398 sources ('search results') was cleaned by removing duplicates, which reduced the search results to 6,309 sources (see Figure 3). These were screened for relevance through two stages:

1. The results were screened on the basis of titles, abstracts and executive summaries and the results which did not meet the inclusion criteria were removed.

2. The full texts were screened, applying the same criteria for relevance and a new requirement for methodological rigour. Results where the full text was not available were also removed.

This produced a final set of 105 sources to be read and coded. Summaries of the 105 sources are available in the Report supplement.[9]

Most exclusions were due to:

- 'Priva*' capturing the 'private sector', thus discussing technological developments but not focusing on privacy-related issues, for example: software development (e.g., apps for children); ICT education and digital skills generally, without a specific focus on privacy; not relevant to the digital environment (some databases which did not allow the cross-over of all three search groups).

- Search terms relating to digital* OR mobile* OR internet OR online that focused on technical aspects such as engineering or IT skills,

- 'Child' present but study relates to adults not children (e.g., child custody; childbirth; adult children).

- Studies using adult 'student' samples and not children. In cases where the literature on children (aged under 18) was particularly scarce, some of the studies on young adults were left in the sample to help us identify potential areas of research interest.

- Studies not substantially related to privacy (e.g., focused on online purchase choices).

- Robustness of the research methodology: unconvincing description of the methodology or terminology/key research terms.

- The search also produced databases of conference proceeding (rather than individual papers) which were removed due to low relevance of the individual sources.

- Similar outputs by the same author (e.g., conference paper and a journal article) – the most recent or reliable source was retained.

Coding

The final results were coded via a coding template developed for the purpose of the systematic evidence mapping and constructed to that it meets the review requirements. The coding involved recording key information about: the approach to and definitions of privacy; key findings related to children's experiences of online privacy; and research methodology and context (type of study, methods and type of data, age groups, research questions and geographic scope, study value and reliability, limitations). Summaries of the codes studies can be found in the Report supplement.

[9] See http://www.lse.ac.uk/media-and-communications/assets/documents/research/projects/childrens-privacy-online/Background-report-final-Supplement.pdf

Appendix 2: List of coded sources

Abbas, R. and Mesch, G.S. (2015) Cultural values and Facebook use among Palestinian youth in Israel. *Computers in Human Behavior* 48, 644-53.

Acker, A. and Bowler, L. (2017) What is your Data Silhouette? Raising teen awareness of their data traces in social media. Proceedings of the 8th International Conference on Social Media & Society. Toronto, Canada: Association for Computing Machinery, 1-5.

Acker, A. and Bowler, L. (2018) Youth data literacy: Teen perspectives on data created with social media and mobile devices. 51st Hawaii International Conference on System Sciences. Hawaii, USA, 1923-32.

Ahn, J., Subramaniam, M., Fleischmann, K.R., et al. (2012) Youth identities as remixers in an online community of storytellers: Attitudes, strategies, and values. Proceedings of the American Society for Information Science and Technology 49, 1-10.

Almansa, A., Fonseca, O. and Castillo, A. (2013) Social networks and young people. Comparative study of Facebook between Colombia and Spain. *Scientific Journal of Media Education* 40, 127-34.

Aslanidou, S. and Menexes, G. (2008) Youth and the internet: Uses and practices in the home. *Computers & Education* 51, 1375-91.

Badri, M., Alnuaimi, A., Al Rashedi, A., et al. (2017) School children's use of digital devices, social media and parental knowledge and involvement – the case of Abu Dhabi. *Education & Information Technologies* 22, 2645-64.

Bailey, J.E. (2015) A perfect storm: How the online environment, social norms and law shape girls' lives. In V. Steeves and J.E. Bailey (eds) *eGirls, eCitizens*. Ottawa, Canada: University of Ottawa Press, 21-53.

Bakó, R.K. (2016) Digital transition: Children in a multimodal world. *Acta Universitatis Sapientiae, Social Analysis* 6, 145-54.

Balleys, C. and Coll, S. (2017) Being publicly intimate: Teenagers managing online privacy. *Media, Culture & Society* 39, 885-901.

Barron, C.M. (2014) 'I had no credit to ring you back': Children's strategies of negotiation and resistance to parental surveillance via mobile phones. *Surveillance and Society* 12, 401-13.

Betts, L.R. and Spenser, K.A. (2016) 'People think it's a harmless joke': Young people's understanding of the impact of technology, digital vulnerability and cyberbullying in the United Kingdom. *Journal of Children and Media* 11, 20-35.

Bowler, L., Acker, A., Jeng, W., et al. (2017) 'It lives all around us': Aspects of data literacy in teen's lives. 80th Annual Meeting of the Association for Information Science & Technology. Washington, DC, USA, 27-35.

Bowyer, A., Montague, K., Wheater, S., et al. (2018) Understanding the family perspective on the storage, sharing and handling of family civic data. Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. Montreal, QC, Canada: ACM, 1-13.

boyd, d. and Marwick, A.E. (2011) Social privacy in networked publics: Teens' attitudes, practices, and strategies. A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society. Oxford, UK, 1-29.

Byrne, J., Kardefelt-Winther, D., Livingstone, S., et al. (2016) *Global Kids Online research synthesis, 2015-2016*. Available at www.globalkidsonline.net/synthesis [accessed 29 June 2018]. UNICEF Office of Research-Innocenti and London School of Economics and Political Science, 1-75.

Chai S, Bagchi-Sen S, Morrell C, et al. (2009) Internet and online information privacy: An exploratory study of preteens and early teens. *Ieee Transactions on Professional Communication* 52: 167-82.

Chaudron, S., Di Gioia, R. and Gemo, M. (2018) *Young children (0-8) and digital technology. A qualitative study across Europe*. JRC Science for Policy Report. Luxembourg: Publications Office of the European Union, 1-259.

Chi, Y., Jeng, W., Acker, A., et al. (2018) Affective, behavioral, and cognitive aspects of teen perspectives on personal data in social media: A model of youth data literacy. In G. Chowdhury, J. McLeod, V. Gillet, et al. (eds) *Transforming Digital Worlds. iConference 2018. Lecture Notes in Computer Science*. Cham, Switzerland: Springer, 442-52.

Children's Commissioner for England (2017) *Life in 'likes': Children's Commissioner report into social media use among 8-12 year olds*. London, UK: Children's Commissioner for England, 1-42.

Coleman, S., Pothong, K., Perez Vallejos, E., et al. (2017) *The internet on our own terms: How children and young people deliberated about their digital rights*. London: 5Rights, 1-68.

Cortesi, S., Haduong, P., Gasser, U., et al. (2014) *Youth perspectives on tech in schools: From mobile devices to restrictions and monitoring.* Berkman Center Research Publication 2014-3, 1-18.

Culver, S.H. and Grizzle, A. (2017) *Survey on privacy in media and information literacy with youth perspectives*. UNESCO Series on Internet Freedom. Paris, France: UNESCO, 1-125.

Davis, K. and James, C. (2013) Tweens' conceptions of privacy online: Implications for educators. *Learning, Media and Technology* 38, 4-25.

De Souza, Z. and Dick, G.N. (2009) Disclosure of information by children in social networking – Not just a case of 'you show me yours and I'll show you mine'. *International Journal of Information Management* 29, 255-61.

Dennen, V.P., Rutledge, S.A., Bagdy, L.M., et al. (2017) Context collapse and student social media networks: Where life and high school collide. Proceedings of the 8th International Conference on Social Media & Society. Toronto, Canada: Association for Computing Machinery, 1-5.

Dey, R., Ding, Y. and Ross, K.W. (2013) Profiling high-school students with Facebook: How online privacy laws can actually increase minors' risk. Proceedings of the 2013 Conference on Internet Measurement. Barcelona, Spain: ACM, 405-16.

Emanuel, L. and Fraser, D.S. (2014) Exploring physical and digital identity with a teenage cohort. IDC '14 Proceedings of the 2014 Conference on Interaction Design and Children. New York, USA: Association for Computing Machinery, 67-76.

Feng, Y. and Xie, W. (2014) Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors. *Computers in Human Behavior* 33, 153-62.

Foucault, B. and Markov, A. (2009) Teens and communication technology: The coconstruction of privacy and friendship in mediated communication. Annual Meeting of the International Communication Association. Chicago, IL, USA: International Communication Association, 1-27.

Garbett, A., Chatting, D., Wilkinson, G., et al. (2018) ThinkActive: Designing for pseudonymous activity tracking in the classroom. Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. Montreal, QC, Canada: ACM, 1-13.

Gelman, S.A., Martinez, M., Davidson, N.S., et al. (2018) Developing digital privacy: Children's moral judgements concerning mobile GPS devices. *Child Development* 89, 17-26.

Ghosh, A.K., Badillo-Urquiola, K., Guha, S., et al. (2018) Safety vs. surveillance: What children have to say about mobile apps for parental control. Conference on Human Factors in Computing Systems. Montreal, Canada: ACM, 1-14.

Heirman, W., Walrave, M. and Ponnet, K. (2013) Predicting adolescents' disclosure of personal information in exchange for commercial incentives: An application of an extended theory of planned behavior. *Cyberpsychology, Behavior, and Social Networking* 16, 81-7.

Heirman, W., Walrave, M., Vermeulen, A., et al. (2016) An open book on Facebook? Examining the interdependence of adolescents' privacy regulation strategies. *Behaviour & Information Technology* 35, 706-19.

Hofstra, B., Corten, R. and van Tubergen, F. (2016) Understanding the privacy behavior of adolescents on Facebook: The role of peers, popularity and trust. *Computers in Human Behavior* 60, 611-21.

Ji, Y., Wang, G.J., Zhang, Q., et al. (2014) Online social networking behaviors among Chinese younger and older adolescent: The influences of age, gender, personality, and attachment styles. *Computers in Human Behavior* 41, 393-402.

Jia, H.Y., Wisniewski, P., Xu, H., et al. (2015) Risk-taking as a learning process for shaping teens' online information privacy behaviors. International Conference on Computer-Supported Cooperative Work and Social Computing. Vancouver, Canada: ACM, 583-99.

Kumar, P., Naik, S.M., Devkar, U.R., et al. (2017) 'No telling passcodes out because they're private': Understanding children's mental models of privacy and security online. Proceedings of the ACM on Human-Computer Interaction 1 (CSCW), 1-21.

Lapenta GH and Jørgensen RF. (2015) Youth, privacy and online media: Framing the right to privacy in public policy-making. *First Monday* 20.

Livingstone, S. (2008) Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society* 10, 393-411.

Livingstone, S. (2014) Developing social media literacy: How children learn to interpret risky opportunities on social network sites. *Communications. The European Journal of Communication Research* 39, 283-303.

Livingstone, S. and Haddon, L. (2009) *EU Kids Online: Final report 2009*. London: London School of Economics and Political Science. Available at www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20I%20(2006-9)/EU%20Kids%20Online%20I%20Reports/EUKidsOnlineFinalReport.pdf

Livingstone, S. and Sefton-Green, J. (2016) *The class*. New York: New York University Press.

Livingstone, S., Mascheroni, G. and Murru, M.F. (2011) Social networking among European children: New findings on privacy, identity and connection. *Hermes* 59, 89-98.

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, 303-20.

Livingstone, S., Haddon, L., Görzig, A., et al. (2010) *Risks and safety for children on the internet: The UK report: Full findings from the EU Kids Online survey of UK 9-16 year olds and their parents*. London: London School of Economics and Political Science. Available at www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/National%20reports/UKReport.pdf

Livingstone, S., Mascheroni, G., Ólafsson, K., et al. (2014) *Children's online risks and opportunites: Comparative findings from EU Kids Online and Net Children Go Mobile*. London: London School of Economics and Polilcal Science.

Machold, C., Judge, G., Mavrinac, A., et al. (2012) Social networking patterns/hazards among irish teenagers. *Irish Medical Journal* 105, 151-2.

Madden, M., Lenhart, A., Cortesi, S., et al. (2013) *Teens, social media, and privacy*. Washington, DC: Pew Research Center's Internet & American Life Project.

Malik, A., Dhir, A. and Nieminen, M. (2015) Uncovering facebook photo tagging culture and practices among digital natives. *Global Media Journal* 13, 1-22.

Martin, F., Wang, C., Petty, T., et al. (2018) Middle school students' social media use. *Educational Technology & Society* 21, 213-24.

Marwick, A.E. and boyd, d. (2014) Networked privacy: How teenagers negotiate context in social media. *New Media & Society* 16, 1051-67.

McReynolds, E., Hubbard, S., Lau, T., et al. (2017) Toys that listen: A study of parents, children, and internet-connected toys. Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems. Denver, CO, USA: ACM, 5197-207.

Micheti, A., Burkell, J. and Steeves, V. (2010) Fixing broken doors: Strategies for drafting privacy policies young people can understand. *Bulletin of Science, Technology and Society* 30, 130-43.

Miyazaki, A., Stanaland, A. and Lwin, M. (2009) Self-regulatory safeguards and the online privacy of preteen children: Implications for the advertising industry. *Journal of Advertising* 38, 79-91.

Moll, R., Pieschl, S. and Brornme, R. (2014) Competent or clueless? Users' knowledge and misconceptions about their online privacy management. *Computers in Human Behavior* 41, 212-19.

Moscardelli, D.M. and Divine, R. (2007) Adolescents' concern for privacy when using the internet: An empirical analysis of predictors and relationships with privacy-protecting behaviors. *Family & Consumer Sciences Research Journal* 35, 232-52.

Moser, C., Chen, T. and Schoenebeck, S.Y. (2017) Parents' and children's preferences about parents sharing about children on social media. *Human Factors in Computing Systems*, 5221-5.

Mullen, C. and Hamilton, N.F. (2016) Adolescents' response to parental Facebook friend requests: The comparative influence of privacy management, parent–child relational quality, attitude and peer influence. *Computers in Human Behavior* 60, 165-72.

Murumaa-Mengel, M. (2015) Drawing the threat: A study on perceptions of the online pervert among Estonian high school students. *Young* 23, 1-18.

Ofcom (2017) Children and parents: Media use and attitudes report. London: Ofcom. Available at www.ofcom.org.uk/__data/assets/pdf_file/0020/108182/children-parents-media-use-attitudes-2017.pdf

Ogur, B., Yilmaz, R.M. and Göktas, Y. (2017) An examination of secondary school students' habits of using internet. *Pegem Egitim Ve Ogretim Dergisi* 7, 421-52.

Öncü, S. (2016) Facebook habits among adolescents: Impact of perceived social support and tablet computers. *Information Development* 32, 1457-70.

Oolo, E. and Siibak, A. (2013) Performing for one's imagined audience: Social steganography and other privacy strategies of Estonian teens on networked publics. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 7, article 7.

Pangrazio, L. and Selwyn, N. (2018) 'It's not like it's life or death or whatever': Young people's understandings of social media data. *Social Media and Society* 4, 1-9.

Pradeep, P. and Sriram, S. (2016) The virtual world of social networking sites: Adolescents' use and experiences. *Psychology and Developing Societies* 28, 139-59.

Raynes-Goldie, K. and Allen, M. (2014) Gaming privacy: A Canadian case study of a children's co-created privacy literacy game. *Surveillance and Society* 12, 414-26.

Redden, S.M. and Way, A.K. (2017) 'Adults don't understand': Exploring how teens use dialectical frameworks to navigate webs of tensions in online life. *Journal of Applied Communication Research* 45, 21-41.

Rimini, M., Howard, C. and Ghersengorin, A. (2016) *Digital resilience: Empowering youth online. Practices for a safer internet use. A major survey targeting Australia, Japan, Indonesia, Korea and Taiwan*. Brussels: ThinkYoung.

Rode, J.A. (2009) Digital parenting: Designing children's safety. BCS-HCI '09 Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology. Cambridge, UK: ACM Digital Library, 244-51.

Selwyn, N. and Pangrazio, L. (2018) Doing data differently? Developing personal data tactics and strategies amongst young mobile media users. *Big Data and Society* 5, 1-12.

Shade, L.R. and Singh, R. (2016) 'Honestly, we're not spying on kids': School surveillance of young people's social media. *Social Media and Society* 2, 1-12.

Shin, W. and Kang, H. (2016) Adolescents' privacy concerns and information disclosure online: The role of parents and the internet. *Computers in Human Behavior* 54, 114-23. doi:10.1016/j.chb.2015.07.062

Shin, W., Huh, J. and Faber, R.J. (2012) Tweens' online privacy risks and the role of parental mediation. *Journal of Broadcasting & Electronic Media* 56, 632-49.

S-O'Brien, L., Read, P., Woolcott, J., et al. (2011) Understanding privacy behaviors of Millennials within social networking sites. Proceedings of the ASIST Annual Meeting 48, 1-10.

Steeves, V. and Regan, P. (2014) Young people online and the social value of privacy. Journal of Information, *Communication & Ethics in Society* 12, 298-313.

Steeves, V. and Webster, C. (2008) Closing the barn door: The effect of parental supervision on Canadian children's online privacy. *Bulletin of Science, Technology and Society* 28, 4-19.

Steijn, W.M.P., Schouten, A.P. and Vedder, A.H. (2016) Why concern regarding privacy differs: The influence of age and (non-)participation on Facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 10, 1-12.

Steijn, W.M.P. and Vedder, A.H. (2015) Privacy under construction: A developmental perspective on privacy perception. *Science Technology & Human Values* 40(4), 615-37. doi:10.1177/0162243915571167

Subrahmanyam K and Greenfield PM. (2008) Online communication and adolescent relationships. *The Future of Children* 18: 119-46.

Thang, S.M., Noor, N.M., Taha, A.M., et al. (2016) Effects of social networking on Malaysian secondary school students: Attitudes, behaviours and awareness of risks. *Pertanika Journal of Social Science and Humanities* 24, 157-67.

Third, A., Bellerose, D., Dawkins, U., et al. (2014) *Children's rights in the digital age: A download from Children Around the World*. Abbotsford, VIC, Australia: Young and Well Cooperative Research Centre.

Third, A., Bellerose, D., Diniz de Oliveira, J., et al. (2017) *Young and online: Children's perspectives on life in the digital age. The State of the World's Children 2017 Companion Report*. Sydney, NSW, Australia: Western Sydney University. Available at www.westernsydney.edu.au/__data/assets/pdf_file/0006/1334805/Young_and_Online_Report.pdf

Tirumala, S.S., Sarrafzadeh, A. and Pang, P. (2016) A survey on internet usage and cybersecurity awareness in students. 2016 14th Annual Conference on Privacy, Security and Trust (PST), 223-8.

van Gool, E., van Ouytsel, J., Ponnet, K., et al. (2015) To share or not to share? Adolescents' self-disclosure about peer relationships on Facebook: An application of the Prototype Willingness Model. *Computers in Human Behavior* 44, 230-9.

van Reijmersdal, E.A., Rozendaal, E., Smink, N., et al. (2017) Processes and effects of targeted online advertising among children. *International Journal of Advertising* 36, 396-414.

Velki, T., Solic, K., Gorjanac, V., et al. (2017) Empirical study on the risky behavior and security awareness among secondary school pupils – Validation and preliminary results. In P. Biljanovic, M. Koricic, K. Skala, et al. (eds) *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics*, 1280-4.

Vickery, J.R. (2015) 'I don't have anything to hide, but…': The challenges and negotiations of social and mobile media privacy for non-dominant youth. Information, *Communication & Society* 18, 281-94.

Vickery, J.R. (2017) *Worried about the wrong things: Youth, risk, and opportunity in the digital world*. Cambridge, MA: MIT Press.

Walker, K.L., Kiesler, T. and Malone, S. (2016) *Youth-driven Information Privacy Education Campaign 2015-16: Digital Trust Foundation Final grant report*. Online submission.

Walrave, M. and Heirman, W. (2011) Cyberteens: Balancing between self-disclosure and privacy concerns? Conference Papers – International Communication Association, 1-33.

Walrave, M. and Heirman, W. (2013) Adolescents, online marketing and privacy: Predicting adolescents' willingness to disclose personal information for marketing purposes. *Children and Society* 27, 434-47.

Weeden, S., Cooke, B. and McVey, M. (2013) Underage children and social networking. *Journal of Research on Technology in Education* 45, 249-62.

Weinstein, E.C. (2014) The personal is political on social media: Online civic expression patterns and pathways among civically engaged youth. *International Journal of Communication* 8, 210-33.

Williams, A. and Merten, M. (2008) A review of online social networking profiles by adolescents: Implications for future research and intervention. *Adolescence* 43, 253-74.

Wisniewski, P. (2018) The privacy paradox of adolescent online safety: A matter of risk prevention or risk resilience? *IEEE Security and Privacy* 16, 86-90.

Wisniewski, P., Jia, H., Xu, H., et al. (2015) *'Preventative' vs. 'reactive': How parental mediation influences teens' social media privacy behaviors*. Association for Computing Machinery, Inc., 302-16.

Xie, W.J. and Kang, C.Y. (2015) See you, see me: Teenagers' self-disclosure and regret of posting on social network site. *Computers in Human Behavior* 52, 398-407.

Youn, S. (2008) Parental influence and teens' attitude toward online privacy protection. *The Journal of Consumer Affairs* 42, 362-88.

Youn, S. (2009) Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs* 43, 389-418.

Youn, S. and Hall, K. (2008) Gender and online privacy among teens: Risk perception, privacy concerns, and protection behaviors. *Cyberpsychology and Behavior* 11, 763-65.

Zarouali, B., Ponnet, K., Walrave, M., et al. (2017) 'Do you like cookies?' Adolescents' sceptical processing of retargeted Facebook-ads and the moderating role of privacy concern and a textual debriefing. *Computers in Human Behavior* 69, 157-65.

Zhang-Kennedy, L. and Chiasson, S. (2016) Teaching with an interactive eBook to improve children's online privacy knowledge. Proceedings of The 15th International Conference on Interaction Design and Children. Manchester, UK: ACM, 506-11.

Zhang-Kennedy, L., Abdelaziz, Y. and Chiasson, S. (2017) Cyberheroes: The design and evaluation of an interactive ebook to educate children about online privacy. *International Journal of Child-Computer Interaction* 13, 10-18.

Zhang, Y. (2012) College students' uses and perceptions of social networking sites for health and wellness information. *Information Research: an International Electronic Journal* 17.

Zizek, B. (2017) Digital socialization? An exploratory sequential analysis of anonymous adolescent internet–social interaction. *Human Development* 60, 203-32.

Appendix 3: Glossary

Affordances

Affordances are understood as the fundamental properties of an object that define its potential uses in an environment. The perceived uses are influenced by an individual's skills and capabilities (Gibson, 1966). In relation to the digital environment we can divide affordances into (i) design features of the internet (data permanence, remixability, identification via IP address, URL tracking, use of cookies or tags etc.); (ii) network effects of the internet (scalability, spread, difficulty of erasure, multiplicity of versions); and (iii) organisational (institutional and commercial) practices (nature of terms and conditions, minimum age, design of privacy settings, data collection and processing policy, process of redress, security features and vulnerabilities, interrelations and interdependencies among organisations, etc.). boyd and Marwick (2011) apply this notion to networked technologies, describing four different technical affordances:

(i) Persistence: online content is automatically recorded and archived
(ii) Replicability: online content is duplicated easily
(iii) Scalability: there is great potential visibility of digital content
(iv) Searchability: digital content is accessible through search engines.

Child

Following the United Nations (UN) Convention on the Rights of the Child (1989), we define a child as a person under the age of 18. We recognise that 'teenagers' (or 'young people' or 'youth') may bear adult responsibilities and may not consider themselves children, and that cultures and contexts matter in determining the significance of 'child' and 'childhood'. The primary focus of our research project is on secondary school children aged 11-16.

Media literacy

Media literacy is widely defined as the ability to access, analyse, evaluate and create messages across a variety of contexts (Aufderheide, 1993). Buckingham (2015) suggests four areas of knowledge in media literacy online:

(i) Representation: assessing and evaluating material encountered, including its biases, reliability and positionality
(ii) Language: includes understanding codes and conventions underpinning particular forms of communication, and an awareness of how media are constructed
(iii) Production: awareness of who is communicating and why
(iv) Audience: understanding how, why and to whom media are targeted and towards what interests, and the interactivity afforded by online spaces.

In relation to the internet, if media literacy is to be promoted fairly and effectively, critical attention is needed to '(i) the symbolic and material representation of knowledge, culture and values; (ii) the diffusion of interpretative skills and abilities across a (stratified) population; and (iii) the institutional, especially, the state management of the power that access to and skilled use of knowledge brings to those who are "literate"' (Livingstone, 2004: 3). Media literacy is dependent on media affordances in that an individual's ability to access, analyse, evaluate and create messages depends on the communicative affordances of the specific context, including that of the digital environment. Institutional provision to promote and support media literacy may include awareness-raising initiatives and media education provided through schools.

Parent

We use the term 'parent' synonymously with 'carer' or 'guardian' to refer to the adults most closely involved in or responsible for a child's welfare and upbringing, recognising that this may include biological parents living separately from the child or step-parents or foster parents living with the child. We make no assumptions as to the number of parents or their sexuality, and we recognise that other family members (e.g., grandparents or aunts and uncles) may care for a child (including undertaking 'parental mediation' of their internet use). We also recognise that some children receive little or no parenting, irrespective if they possess biological parents (Byrne et al., 2016).

Privacy

Privacy is a fundamental human right, recognised in the Universal Declaration of Human Rights, the International Convention on Civil and Political Rights, the European Convention on Human Rights, the UN Convention on the Rights of the Child and codified in many national laws and constitutions. It underpins many other rights, is essential for freedom and democracy and remains intrinsic to human dignity (Solove, 2008). Westin (1967) explains privacy as the right of individuals, groups or institutions to determine if, when and to what extent information about them is shared with others. Nissenbaum (2004) builds on this understanding by suggesting that privacy is provided by appropriate flows of information, which conform to contextual norms and codes. Privacy is relational (Solove, 2015; Hargreaves, 2017) and is distinguished by the type of relationship an individual has with (i) other individuals or groups, (ii) a public or third sector (not-for-profit) organisation, or (iii) a commercial organisation. Thus we distinguish three main types of privacy for the purposes of this report:

- *Interpersonal privacy*

  Interpersonal privacy arises from the relationship between one individual (or group) and another individual (or group or community). This relationship is generally founded on processes of communication or information sharing, and may reflect mutual interests or the interests of one party more than the others. The relationship may be equal or unequal in terms of power and control over use of personal data.

- *Institutional privacy*

  Institutional privacy arises from the relationship between an individual (or group or organisation) and a public or third sector (not-for-profit) organisation. Generally, the collection and use of individuals' personal data is undertaken for reasons of the public interest. Nonetheless, there is also a generally unequal power relationship between individuals and institutions, impeding individuals' ability to control the provision and use of their personal data.

- *Commercial privacy*

  Commercial privacy arises from the relationship between an individual (or group or organisation) and a commercial organisation. Often at stake here is the nature of the commercial business model by which individuals are provided with online resources by a commercial organisation which generates revenue from the collection and use of those individuals' data, especially given the generally unequal power relationship between individuals and companies, impeding individuals' ability to control the provision and use of their personal data.

Personal data

Personal data is information that can identify or help identify individuals directly, or indirectly in combination with other information; it includes pseudonymised data. Based on van der Hof (2016), we identified three types of data: data given, data traces and interred data. 'Data given' relates to the

data contributed by individuals (about themselves or about others), usually knowingly though not necessarily intentionally, during their participation online. 'Data traces' is the data left, mostly unknowingly – by participation online and captured via data-tracking technologies such as cookies, web beacons or device/browser fingerprinting, location data and other metadata. 'Inferred data' is the data derived from analysing data given and data traces, often by algorithms (also referred to as 'profiling'), possibly combined with other data sources. Each of these types of data may or may not be 'personal data', that is, 'information that relates to an identified or identifiable individual', as defined by the ICO and GDPR.

Rights

The right to privacy is included in Article 16 of the UN Convention on the Rights of the Child (1989), Article 8 of the European Convention on Human Rights (1953) and Article 12 of the Universal Declaration of Human Rights (1948). In this report we regard the right to privacy as both a fundamental human right and a means of enabling other rights, for which we refer to the full range of rights included in the UN Convention on the Rights of the Child, including to its conception of the child as an independent rights-holder. Secondarily, we take note of the emergence of so-called 'digital rights', regarding these as some of the legal and institutional means by which privacy may be protected or fulfilled in practice.

Systematic evidence mapping

This refers to a review process that systematically identifies and describes the research that exists within the boundaries of the review question (EPPI-Centre, 2018). Systematic evidence mapping (i) describes the nature of the research field, (ii) informs the conduct of a synthesis, and (ii) aids in interpretation of the findings (Grant and Booth, 2009; Gough et al., 2012; EPPI-Centre, 2018).

References

Abbas, R. and Mesch, G.S. (2015) Cultural values and Facebook use among Palestinian youth in Israel. *Computers in Human Behavior* 48, 644-53.

Acker, A. and Bowler, L. (2017) What is your Data Silhouette? Raising teen awareness of their data traces in social media. *Proceedings of the 8th international conference on social media and society.* Toronto, Canada: Association for Computing Machinery, 1-5.

Acker, A. and Bowler, L. (2018) Youth data literacy: teen perspectives on data created with social media and mobile devices. *51st Hawaii International Conference on System Sciences.* Hawaii, USA, 1923-32.

Al-Saggaf, Y. and Nielsen, S. (2014) Self-disclosure on Facebook among female users and its relationship to feelings of loneliness. *Computers in Human Behavior* 36, 460-8.

Al Shehri, M. (2017) A secure mobile learning framework based on Cloud. *International Journal of Advanced Computer Science and Applications* 8(10), 7-11.

Alkis, Y., Kadirhan, Z. and Sat, M. (2017) Development and validation of social anxiety scale for social media users. *Computers in Human Behavior* 72, 296-303.

Almansa, A., Fonseca, O. and Castillo, A. (2013) Social networks and young people. Comparative study of Facebook between Colombia and Spain. *Scientific Journal of Media Education* 40, 127-34.

Alper, M., Hourcade, J.P. and Gilutz, S. (2012) Interactive technologies for children with special needs. *Proceedings of the 11th International Conference on Interaction Design and Children.* Bremen, Germany.

Archard, D. (1990) Child Abuse: parental rights and the interests of the child. *Journal of Applied Philosophy* 7(2), 183-94.

Aslanidou, S. and Menexes, G. (2008) Youth and the Internet: Uses and practices in the home. *Computers & Education* 51(3), 1375-91.

Aufderheide, P. (1993) *Media literacy: A report of the national leadership conference on media literacy.* Aspen: Aspen Institute.

Badri, M., Alnuaimi, A., Al Rashedi, A., et al. (2017) School children's use of digital devices, social media and parental knowledge and involvement - the case of Abu Dhabi. *Education & Information Technologies* 22(5), 2645-64.

Bailey, J.E. (2015) A perfect storm: How the online environment, social norms and law shape girls' lives. In: V. Steeves and J.E. Bailey (eds) *eGirls, eCitizens.* Ottawa, Canada: University of Ottawa Press, 21-53.

Bakó, R.K. (2016) Digital transition: Children in a multimodal world. *Acta Universitatis Sapientiae, Social Analysis* 6(1), 145-54.

Balleys, C. and Coll, S. (2017) Being publicly intimate: teenagers managing online privacy. *Media, Culture & Society* 39(6), 885-901.

Barnes, S.B. (2006) A privacy paradox: social networking in the United States. *First Monday* 11(9).

Barron, C.M. (2014) I had no credit to ring you back': Children's strategies of negotiation and resistance to parental surveillance via mobile phones. *Surveillance and Society* 12(3), 401-13.

Betts, L.R. and Spenser, K.A. (2016) 'People think it's a harmless joke': Young people's understanding of the impact of technology, digital vulnerability and cyberbullying in the United Kingdom. *Journal of Children and Media* 11(1), 20-35.

Blackwell, L., Hardy, J., Ammari, T., et al. (2016) LGBT parents and social media: Advocacy, privacy, and disclosure during shifting social movements. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems.* San Jose, CA, USA: ACM, 610-22.

Bowler, L., Acker, A., Jeng, W., et al. (2017) 'It lives all around us': Aspects of data literacy in teen's lives. *80th Annual Meeting of the Association for Information Science & Technology.* Washington DC, USA, 27-35.

Bowyer, A., Montague, K., Wheater, S., et al. (2018) Understanding the family perspective on the storage, sharing and handling of family civic data. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems.* Montreal, QC, Canada.

boyd, d. and Marwick, A.E. (2011) Social privacy in networked publics: teens' attitudes, practices, and

strategies. *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society.* Oxford, UK, 1-29.
Buckingham, D. (2015) Defining digital literacy - What do young people need to know about digital media? *Nordic Journal of Digital Literacy* 10(Jubileumsnummer), 21-35.
Bulger, M., McCormick, P. and Pitcan, M. (2017) The legacy of inBloom. Working Paper. Available at https://datasociety.net/pubs/ecl/InBloom_feb_2017.pdf.
Byrne, J., Kardefelt-Winther, D., Livingstone, S., et al. (2016) Global Kids Online research synthesis, 2015-2016. Florence and London: UNICEF Office of Research-Innocenti and London School of Economics and Political Science. Available at www.globalkidsonline.net/synthesis, 1-75.
Chai, S., Bagchi-Sen, S., Morrell, C., et al. (2009) Internet and online information privacy: An exploratory study of preteens and early teens. *Ieee Transactions on Professional Communication* 52(2), 167-82.
Chaudron, S., Di Gioia, R. and Gemo, M. (2018) Young children (0-8) and digital technology. A qualitative study across Europe. *JRC Science for Policy Report.* Luxembourg: Publications Office of the European Union, 1-259.
Chi, Y., Jeng, W., Acker, A., et al. (2018) Affective, behavioral, and cognitive aspects of teen perspectives on personal data in social media: A model of youth data literacy. In: G. Chowdhury, J. McLeod, V. Gillet, et al. (eds) *Transforming Digital Worlds. iConference 2018. Lecture Notes in Computer Science.* Cham, Switzerland: Springer, 442-52.
Children's Commissioner for England. (2017a) Life in 'likes': Children's Commissioner report into social media use among 8-12 year olds. London: Children's Commissioner for England, 1-42.
Children's Commissioner for England. (2017b) Growing up digital. A report of the Growing Up Digital Taskforce. London: Children's Commissioner for England.
Coleman, S., Pothong, K., Perez Vallejos, E., et al. (2017) The internet on our own terms: How children and young people deliberated about their digital rights. London: 5Rights, 1-68.
Cortesi, S., Haduong, P., Gasser, U., et al. (2014) Youth perspectives on tech in schools: From mobile devices to restrictions and monitoring. *Berkman Center Research Publication* 2014-3, 1-18.
Council of Europe. (2018) New recommendation adopted on children's rights in the digital environment. Available at www.coe.int/en/web/children/-/new-recommendation-adopted-on-children-s-rights-in-the-digital-environment.
Culver, S.H. and Grizzle, A. (2017) Survey on privacy in media and information literacy with youth perspectives. *UNESCO Series on Internet Freedom.* Paris, France: UNESCO, 1-125.
Davis, K. and James, C. (2013) Tweens' conceptions of privacy online: Implications for educators. *Learning, Media and Technology* 38(1), 4-25.
De Souza, Z. and Dick, G.N. (2009) Disclosure of information by children in social networking - not just a case of 'you show me yours and I'll show you mine'. *International Journal of Information Management* 29(4), 255-61.
DefendDigitalMe. (2018) The state of data. Lessons for policymakers. Available at http://defenddigitalme.com/wp-content/uploads/2018/05/StateOfDataReport_policymakers_ddm.pdf.
Dennen, V.P., Rutledge, S.A., Bagdy, L.M., et al. (2017) Context collapse and student social media networks: Where life and high school collide. *Proceedings of the 8th International Conference on Social Media & Society* Toronto, Canada: Association for Computing Machinery, 1-5.
Department for Education. (2018) Relationships education, relationships and sex education (RSE) and health education: guidance for governing bodies, proprietors, head teachers, principals, senior leadership teams, teachers (draft). London: Department for Education.
Dey, R., Ding, Y. and Ross, K.W. (2013) Profiling high-school students with Facebook: how online privacy laws can actually increase minors' risk. *Proceedings of the 2013 Conference on Internet Measurement.* Barcelona, Spain.
Emanuel, L. and Fraser, D.S. (2014) Exploring physical and digital identity with a teenage cohort. *IDC '14 Proceedings of the 2014 Conference on Interaction Design and Children.* New York: Association for Computing Machinery, 67-76.
EPPI-Centre. (2018) Definitions EPPI-Centre. Available at

http://eppi.ioe.ac.uk/cms/Default.aspx?tabid=334.
Feng, Y. and Xie, W. (2014) Teens' concern for privacy when using social networking sites: An analysis of socialization agents and relationships with privacy-protecting behaviors. *Computers in Human Behavior* 33, 153-62.
Fielder, A., Gardner, W., Nairn, A., et al. (2007) Fair game? Assessing commercial activity on children's favourite websites and online environments. London: National Consumer Councill.
Garbett, A., Chatting, D., Wilkinson, G., et al. (2018) ThinkActive: designing for pseudonymous activity tracking in the classroom. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems.* Montreal QC, Canada.
Gelman, S.A., Martinez, M., Davidson, N.S., et al. (2018) Developing digital privacy: Children's moral judgements concerning mobile GPS devices. *Child Development* 89(1), 17-26.
Ghosh, A.K., Badillo-Urquiola, K., Guha, S., et al. (2018) Safety vs. surveillance: what children have to say about mobile apps for parental control. *Conference on Human Factors in Computing Systems.* Montreal, Canada.
Gibson, J.J. (1966) *The senses considered as perceptual systems.* Westport, CT: Greenwood Press.
Gough, D., Thomas, J. and Oliver, S. (2012) Clarifying differences between review designs and methods. *Systematic Reviews* 1, 1-9.
Grant, M. and Booth, A. (2009) A typology of reviews: an analysis of 14 review types and associated methodologies. *Health Information and Libraries Journal* 26, 91–108.
Hargreaves, S. (2017) Relational privacy and tort. *William and Mary Journal of Women and the Law* 23(3), 433-76.
Heirman, W., Walrave, M. and Ponnet, K. (2013) Predicting adolescents' disclosure of personal information in exchange for commercial incentives: An application of an extended theory of planned behavior. *Cyberpsychology, Behavior, and Social Networking* 16(2), 81-7.
Heirman, W., Walrave, M., Vermeulen, A., et al. (2016) An open book on Facebook? Examining the interdependence of adolescents' privacy regulation strategies. *Behaviour & Information Technology* 35(9), 706-19.
Hine, C. (2015) Ethnography for the internet: embedded, embodied and everyday. London and New York: Bloomsbury Publishing
Hofstra, B., Corten, R. and van Tubergen, F. (2016) Understanding the privacy behavior of adolescents on Facebook: The role of peers, popularity and trust. *Computers in Human Behavior* 60, 611-21.
Jia, H.Y., Wisniewski, P., Xu, H., et al. (2015) Risk-taking as a learning process for shaping teen's online information privacy behaviors. *International Conference on Computer-Supported Cooperative Work and Social Computing.* Vancouver, Canada: ACM, 583-99.
Jourová, V. (2018) Keynote speech by Commissioner Jourová. *General Data Protection Regulation conference, 25 May.* European Commission. Available at http://europa.eu/rapid/press-release_STATEMENT-18-3949_en.htm.
Kidron, B. and Rudkin, A. (2017) Digital childhood: Addressing childhood development milestones in the digital environment. London: 5rights.
Kidron, B., Evans, A. and Afia, J. (2018) Disrupted chidhood. The cost of persuasive design. London: 5Rights.
Kumar, P., Naik, S.M., Devkar, U.R., et al. (2017) 'No telling passcodes out because they're private': Understanding children's mental models of privacy and security online. *Proceedings of the ACM on Human-Computer Interaction* 1 (CSCW), 1-21.
Lapenta, G.H. and Jørgensen, R.F. (2015) Youth, privacy and online media: Framing the right to privacy in public policy-making. *First Monday* 20(3).
Lievens, E., Livingstone, S., McLaughlin, S., et al. (2018) Children's rights and digital technologies. In: U. Kilkelly and T. Liefaard (eds) *International human rights of children.* Singapore: Springer Singapore, 1-27.
Livingstone, S. (2004) Media literacy and the challenge of new information and communication technologies. *The Communication Review* 7(1), 3-14.
Livingstone, S. (2005) In defence of privacy: mediating the public/ private boundary at home. In: S.

Livingstone (ed) *Audiences and publics: when cultural engagement matters for the public sphere* Bristol: Intellect Press, 163-85.
Livingstone, S. (2008) Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society* 10(3), 393-411.
Livingstone, S. (2014) Developing social media literacy: How children learn to interpret risky opportunities on social network sites. *Communications. The European Journal of Communication Research* 39(3), 283–303.
Livingstone, S. (2018) Children: a special case for privacy? *Intermedia* 46(2), 18-23.
Livingstone, S. and Helsper, E. (2010) Balancing opportunities and risks in teenagers' use of the internet: the role of online skills and internet self-efficacy. *New Media & Society* 12(2), 309-29.
Livingstone, S. and Sefton-Green, J. (2016) *The class.* New York: New York University Press.
Livingstone, S. and Blum-Ross, A. (2017) Researching children and childhood in the digital age. In: A. James and P. Christensen (eds) *Research with children.* 3rd ed. London: Routledge, 54-70.
Livingstone, S., Carr, J. and Bryne, J. (2015) One in three: The task for global internet governance in addressing children's rights. *Global Commission on Internet Governance: Paper Series.* London: CIGI and Chatham House.
Livingstone, S., Ólafsson, K. and Maier, G. (2018a) If children don't know an ad from information, how can they grasp how companies use their personal data? *Media Policy Project.*
Livingstone, S., Stoilova, M. and Nandagiri, R. (2018b) Children's data and privacy online: reviewing the existing evidence. London: London School of Economics and Political Science.
Livingstone, S., Haddon, L., Görzig, A., et al. (2010) *Risks and safety for children on the internet: the UK report: full findings from the EU Kids Online survey of UK 9-16 year olds and their parents*. Available at: www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/National%20reports/UKReport.pdf.
Livingstone, S., Mascheroni, G., Ólafsson, K., et al. (2014) Children's online risks and opportunites: comparative findings from EU Kids Online and Net Children Go Mobile. London: London School of Economics and Polilcal Science.
Lupton, D. and Williamson, B. (2017) The datafied child: The dataveillance of children and implications for their rights. *New Media & Society* 19(5), 780-94.
Macenaite, M. (2017) From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation. *New Media & Society* 19(5), 765-79.
Madden, M., Lenhart, A., Cortesi, S., et al. (2013) Teens, social media, and privacy. Washington, D.C: Pew Research Center's Internet & American Life Project.
Malik, A., Dhir, A. and Nieminen, M. (2015) Uncovering facebook photo tagging culture and practices among digital natives. *Global Media Journal* 13(24), 1-22.
Martin, F., Wang, C., Petty, T., et al. (2018) Middle school students' social media use. *Educational Technology & Society* 21(1), 213-24.
Marwick, A.E. and boyd, d. (2018) Understanding privacy at the margins. *International Journal of Communication* 12, 1157–65.
McReynolds, E., Hubbard, S., Lau, T., et al. (2017) Toys that listen: a study of parents, children, and internet-connected toys. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems.* Denver, CO, USA.
Micheti, A., Burkell, J. and Steeves, V. (2010) Fixing broken doors: strategies for drafting privacy policies young people can understand. *Bulletin of Science, Technology and Society* 30(2), 130-43.
Miyazaki, A., Stanaland, A. and Lwin, M. (2009) Self-regulatory safeguards and the online privacy of preteen children: implications for the advertising industry. *Journal of Advertising* 38(4), 79-91.
Moll, R., Pieschl, S. and Brornme, R. (2014) Competent or clueless? Users' knowledge and misconceptions about their online privacy management. *Computers in Human Behavior* 41, 212-9.
Montgomery, K.C. (2015) Youth and surveillance in the Facebook era: Policy interventions and social

implications. *Telecommunications Policy* 39(9), 771.
Montgomery, K.C., Chester, J. and Milosevic, T. (2017) Children's privacy in the Big Data Era: Research opportunities. *Pediatrics* 140(s2), s117-s21.
Moscardelli, D.M. and Divine, R. (2007) Adolescents' concern for privacy when using the internet: an empirical analysis of predictors and relationships with privacy-protecting behaviors. *Family & Consumer Sciences Research Journal* 35(3), 232-52.
Moser, C., Chen, T. and Schoenebeck, S.Y. (2017) Parents' and children's preferences about parents sharing about children on social media. *Human Factors in Computing Systems*, 5221-25.
Mullen, C. and Hamilton, N.F. (2016) Adolescents' response to parental Facebook friend requests: The comparative influence of privacy management, parent-child relational quality, attitude and peer influence. *Computers in Human Behavior* 60, 165-72.
Murumaa-Mengel, M. (2015) Drawing the threat: a study on perceptions of the online pervert among Estonian high school students. *Young* 23(1), 1-18.
Nissenbaum, H. (2004) Privacy as contextual integrity. *Washington Law Review* 79, 1119-158.
Nissenbaum, H. (2010) *Privacy in context. Technology, policy, and the integrity of social life.* Stanford: Stanford University Press.
Norberg, P., Horne, D. and Horne, D. (2007) The privacy paradox: personal information disclosure intentions versus behaviours. *Journal of Consumer Affairs* 41(1), 100-26.
O'Hara, K. (2016) The seven veils of privacy. *IEEE Internet Computing* 20, 86-91.
Ofcom. (2017a) Report on internet safety measures. https://www.ofcom.org.uk/__data/assets/pdf_file/0020/31754/Fourth-internet-safety-report.pdf: Ofcom.
Ofcom. (2017b) Children and parents: media use and attitudes report. London: Ofcom. Available at: www.ofcom.org.uk/__data/assets/pdf_file/0020/108182/children-parents-media-use-attitudes-2017.pdf.
Ogur, B., Yilmaz, R.M. and Göktas, Y. (2017) An examination of secondary school students' habits of using internet. *Pegem Egitim Ve Ogretim Dergisi* 7(3), 421-52.
Öncü, S. (2016) Facebook habits among adolescents: Impact of perceived social support and tablet computers. *Information Development* 32(5), 1457-70.
Oolo, E. and Siibak, A. (2013) Performing for one's imagined audience: Social steganography and other privacy strategies of Estonian teens on networked publics. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 7(1), article 7.
Pangrazio, L. and Selwyn, N. (2018) 'It's not like it's life or death or whatever': young people's understandings of social media data. *Social Media and Society* 4(3), 1-9.
Peter, J. and Valkenburg, P. (2011) Adolescents' online privacy: toward a developmental perspective. In: S. Trepte and L. Reinecke (eds) *Privacy online.* Heidelberg: Springer, 221-34.
Petronio, S.S. (2002) *Boundaries of privacy: dialects of disclosure.* New York: SUNY Press.
Pradeep, P. and Sriram, S. (2016) The virtual world of social networking sites: Adolescent's use and experiences. *Psychology and Developing Societies* 28(1), 139-59.
Raynes-Goldie, K. and Allen, M. (2014) Gaming privacy: a Canadian case study of a children's co-created privacy literacy game. *Surveillance and Society* 12(3), 414-26.
Redden, S.M. and Way, A.K. (2017) 'Adults don't understand': exploring how teens use dialectical frameworks to navigate webs of tensions in online life. *Journal of Applied Communication Research* 45(1), 21-41.
Rimini, M., Howard, C. and Ghersengorin, A. (2016) Digital resilience: Empowering youth online. Practices for a safer internet use. A major survey targeting Australia, Japan, Indonesia, Korea and Taiwan. Brussels: ThinkYoung.
Rode, J.A. (2009) Digital parenting: Designing children's safety *BCS-HCI '09 Proceedings of the 23rd British HCI Group Annual Conference on People and Computers: Celebrating People and Technology* Cambridge, UK: ACM Digital Library, 244-51.
S-O'Brien, L., Read, P., Woolcott, J., et al. (2011) Understanding privacy behaviors of Millennials within social networking sites. *Proceedings of the ASIST Annual Meeting* 48, 1-10.
Selwyn, N. and Pangrazio, L. (2018) Doing data differently? Developing personal data tactics and

strategies amongst young mobile media users. *Big Data and Society* 5(1), 1-12.
Shade, L.R. and Singh, R. (2016) 'Honestly, we're not spying on kids': School surveillance of young people's social media. *Social Media and Society* 2(4), 1-12.
Shin, W. and Kang, H. (2016) Adolescents' privacy concerns and information disclosure online: the role of parents and the internet. *Computers in Human Behavior* 54, 114-23.
Shin, W., Huh, J. and Faber, R.J. (2012) Tweens' online privacy risks and the role of parental mediation. *Journal of Broadcasting & Electronic Media* 56(4), 632-49.
Shmueli, B. and Blecher-Prigat, A. (2011) Privacy for children. *Columbia Human Rights Law Review* 42, 759-95.
Solove, D.J. (2008) *Understanding privacy.* Cambridge, MA: Harvard University Press.
Solove, D.J. (2015) The meaning and value of privacy. In: B. Roessler and D. Mokrosinska (eds) *Social dimensions of privacy: interdisciplinary perspectives.* Cambridge: Cambridge University Press.
Steeves, V. and Webster, C. (2008) Closing the barn door: The effect of parental supervision on Canadian children's online privacy. *Bulletin of Science, Technology and Society* 28(1), 4-19.
Steeves, V. and Regan, P. (2014) Young people online and the social value of privacy. *Journal of Information, Communication & Ethics in Society* 12(4), 298-313.
Steijn, W.M.P. and Vedder, A. (2015) Privacy under construction: a developmental perspective on privacy perception. *Science Technology & Human Values* 40(4), 615-37.
Steijn, W.M.P., Schouten, A.P. and Vedder, A.H. (2016) Why concern regarding privacy differs: The influence of age and (non-)participation on Facebook. *Cyberpsychology-Journal of Psychosocial Research on Cyberspace* 10(1), 1-12.
Third, A., Bellerose, D., Diniz de Oliveira, J., et al. (2017) Young and online: children's perspectives on life in the digital age. *The State of the World's Children 2017 Companion Report.* Sydney: Western Sydney University. Available at: www.westernsydney.edu.au/__data/assets/pdf_file/0006/1334805/Young_and_Online_Report.pdf.
Tirumala, S.S., Sarrafzadeh, A. and Pang, P. (2016) A survey on internet usage and cybersecurity awareness in students. *2016 14th Annual Conference on Privacy, Security and Trust (PST).* 223-8.
UNICEF. (2018) Children's online privacy and freedom of expression: Industry toolkit. New York: UNICEF.
Utz, S. and Krämer, N.C. (2015) The privacy paradox on social network sites revisited: the role of individual characteristics and group norms. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace* 3(2), article 2.
van der Hof, S. (2016) I agree, or do I? A rights-based analysis of the law on children's consent in the digital world. *Wisconsin International Law Journal* 34(2), 409-45.
van Gool, E., van Ouytsel, J., Ponnet, K., et al. (2015) To share or not to share? Adolescents' self-disclosure about peer relationships on Facebook: An application of the Prototype Willingness Model. *Computers in Human Behavior* 44, 230-9.
van Reijmersdal, E.A., Rozendaal, E., Smink, N., et al. (2017) Processes and effects of targeted online advertising among children. *International Journal of Advertising* 36(3), 396-414.
Velki, T., Solic, K., Gorjanac, V., et al. (2017) Empirical study on the risky behavior and security awareness among secondary school pupils - validation and preliminary results. *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics.*
Vickery, J.R. (2015) 'I don't have anything to hide, but…': the challenges and negotiations of social and mobile media privacy for non-dominant youth. *Information, Communication & Society* 18(3), 281-94.
Vickery, J.R. (2017) *Worried about the wrong things: youth, risk, and opportunity in the digital world.* Cambridge, MA: MIT Press.
Walker, K.L., Kiesler, T. and Malone, S. (2016) Youth-driven information privacy education campaign 2015-16: Digital Trust Foundation final grant report. Digital Trust Foundation.
Walrave, M. and Heirman, W. (2013) Adolescents, online marketing and privacy: predicting

adolescents' willingness to disclose personal information for marketing purposes. *Children and Society* 27(6), 434-47.
Weeden, S., Cooke, B. and McVey, M. (2013) Underage children and social networking. *Journal of Research on Technology in Education* 45(3), 249-62.
Weinstein, E.C. (2014) The personal is political on social media: online civic expression patterns and pathways among civically engaged youth. *International Journal of Communication (19328036)* 8, 210-33.
Westin, A.F. (1967) *Privacy and freedom.* New York: Atheneum.
Williams, A. and Merten, M. (2008) A review of online social networking profiles by adolescents: Implications for future research and intervention. *Adolescence* 43(170), 253-74.
Williamson, B. (2017) Learning in the 'platform society': Disassembling an educational data assemblage. *Research in Education* 98(1), 59-82.
Winterberry Group. (2018) Know your audience: The evolution of identity in a consumer-centric marketplace.
Wisniewski, P. (2018) The privacy paradox of adolescent online safety: a matter of risk prevention or risk resilience? *IEEE Security and Privacy* 16(2), 86-90.
Wisniewski, P., Jia, H., Xu, H., et al. (2015) 'Preventative' vs. 'reactive': how parental mediation influences teens' social media privacy behaviors. Association for Computing Machinery, Inc, 302-16.
Xie, W.J. and Kang, C.Y. (2015) See you, see me: teenagers' self-disclosure and regret of posting on social network site. *Computers in Human Behavior* 52, 398-407.
Xu, H., Irani, N., Zhu, S., et al. (2008) Alleviating parental concerns for children's online privacy: a value sensitive design investigation. ICIS 2008 Proceedings.
Youn, S. (2008) Parental influence and teens' attitude toward online privacy protection. *The Journal of Consumer Affairs* 42(3), 362-88.
Youn, S. (2009) Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. *Journal of Consumer Affairs* 43(3), 389-418.
Youn, S. and Hall, K. (2008) Gender and online privacy among teens: risk perception, privacy concerns, and protection behaviors. *Cyberpsychology and Behavior* 11(6), 763-5.
Young, A.L. and Quan-Haase, A. (2013) Privacy protection strategies on Facebook: the internet privacy paradox revisited. *Information, communication and society* 16(4), 479-500.
Yu, J., Hu, P.J.H. and Cheng, T.H. (2015) Role of affect in self-disclosure on social network websites: a test of two competing models. *Journal of Management Information Systems* 32(2), 239-77.
Zarouali, B., Ponnet, K., Walrave, M., et al. (2017) 'Do you like cookies?' Adolescents' skeptical processing of retargeted Facebook-ads and the moderating role of privacy concern and a textual debriefing. *Computers in Human Behavior* 69, 157-65.
Zhang-Kennedy, L. and Chiasson, S. (2016) Teaching with an interactive e-book to improve children's online privacy knowledge. *Proceedings of the 15th International Conference on Interaction Design and Children.* Manchester, UK.
Zhang-Kennedy, L., Abdelaziz, Y. and Chiasson, S. (2017) Cyberheroes: The design and evaluation of an interactive ebook to educate children about online privacy. *International Journal of Child-Computer Interaction* 13, 10-8.
Zhang, Y. (2012) College students' uses and perceptions of social networking sites for health and wellness information. *Information Research-an International Electronic Journal* 17(3).
Zizek, B. (2017) Digital socialization? An exploratory sequential analysis of anonymous adolescent internet-social interaction. *Human Development* 60(5), 203-32.